Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

# SEC Rule 17a-4: WORM and the Audit-Trail Alternative

> Reliable Context is a kernel of truth: a system of record for organizations that fuse private and public information and must defend every value they act on. One canonical record per real thing, a cited source and an observation date behind every value, unknowns declared rather than left blank, and any past state of the record reproducible.

Published by Reliable Context · 2026-10-29 · sec rule 17a-4 · 17a-4 worm · 17a-4 audit trail alternative · broker dealer electronic records · sec 17a-4(f) requirements

Original article: https://reliablecontext.com/articles/sec-rule-17a-4-electronic-records-worm-and-audit-trail-alternative



### In this article

1. Scope and a caution
2. Who the rule covers
3. Retention periods
4. Definitions that shape the architecture
5. The two preservation paths
6. Requirements that apply to either path
7. The undertaking: executive officer or third party
8. Timeline of the 2022 amendments
9. Recreating the original record: a worked example
10. Architecture patterns
11. Pitfalls
12. Summary
13. Sources

## Scope and a caution

Rule 17a-4 under the US Securities Exchange Act of 1934, codified at 17 CFR 240.17a-4, sets how long broker-dealers must keep the records the SEC requires and in what form they may keep them. Paragraph (f) governs electronic records. Since amendments adopted in October 2022, paragraph (f) offers two ways to preserve electronic records: a non-rewriteable, non-erasable format, widely called WORM ("write once, read many"), or a system that "maintains a complete time-stamped audit trail".

This article explains both paths as a records architecture problem. It is educational, describes the rule text as published on eCFR on 28 October 2026, and is not legal advice. Firms should take advice on how the rule applies to their records.

## Who the rule covers

Rule 17a-4 applies to "every member, broker or dealer subject to § 240.17a-3", the companion rule that lists the records broker-dealers must make (17 CFR 240.17a-4(a)). Security-based swap dealers and major security-based swap participants that are not also broker-dealers are covered by a parallel rule, 17 CFR 240.18a-6, which the SEC describes as "modeled on Rule 17a-4" (SEC Release No. 34-96034). The same 2022 release amended both rules.

## Retention periods

Retention depends on the record type. The rule's main tiers are:

| Paragraph | Records (abbreviated) | Minimum period | Accessibility |
|---|---|---|---|
| 17a-4(a) | Records under 17a-3(a)(1)-(3), (5), (21), (22), e.g. blotters and ledgers | Not less than 6 years | First two years in an easily accessible place |
| 17a-4(b) | Records under 17a-3(a)(4), (6)-(11) and others; bank records; bills; "originals of all communications received and copies of all communications sent ... relating to its business as such"; trial balances and net capital computations | Not less than 3 years | First two years in an easily accessible place |
| 17a-4(c) | Account cards or records on opening and maintenance of customer accounts | Not less than 6 years after the account closes | |
| 17a-4(e) | Various records kept "in an easily accessible place" for periods specified per item | As specified | |

Source: 17 CFR 240.17a-4(a)-(e). A records team typically turns this into a retention schedule keyed by record class, because the same system often holds records from several tiers.

## Definitions that shape the architecture

Paragraph (f)(1) defines the terms the rest of the paragraph relies on:

- **Electronic recordkeeping system:** "a system that preserves records in a digital format in a manner that permits the records to be viewed and downloaded" (f)(1)(ii).
- **Designated executive officer:** "a member of senior management ... who has access to and the ability to provide records maintained and preserved on the electronic recordkeeping system", directly or through a designated specialist (f)(1)(iii).
- **Designated third party:** "a person that is not affiliated with the member, broker, or dealer" with the same access and ability (f)(1)(vi).

The definition of an electronic recordkeeping system was itself changed in 2022 from a media-oriented one. The SEC's stated aim was to make the rule "more technology neutral" (Release 34-96034).

## The two preservation paths

Paragraph (f)(2)(i) gives the choice. An electronic recordkeeping system must either:

**(A)** "Preserve a record for the duration of its applicable retention period in a manner that maintains a complete time-stamped audit trail that includes: (1) All modifications to and deletions of the record or any part thereof; (2) The date and time of actions that create, modify, or delete the record; (3) If applicable, the identity of the individual creating, modifying, or deleting the record; and (4) Any other information needed to maintain an audit trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted"; or

**(B)** "Preserve the records exclusively in a non-rewriteable, non-erasable format".

(17 CFR 240.17a-4(f)(2)(i))

### Why WORM stopped being the only option

Before 2022, Rule 17a-4 required electronic records to be kept "exclusively in a non-rewriteable, non-erasable format". The adopting release explains the practical problem: broker-dealers told SEC staff that the systems they use for business "are dynamic and updated constantly (e.g., with each new transaction or position) and easily accessible", whereas WORM-compliant systems "are more akin to static 'snapshots' of the records at a point in time and less accessible" (Release 34-96034, section II.D.2). Firms were running two systems: one to work in and one to comply with.

The SEC considered and rejected a looser alternative proposed by commenters, a general standard of "appropriate systems and controls". Its reasoning was that such a standard, "unlike the audit-trail or WORM requirement does not require a specific and testable outcome that the system must achieve". The audit-trail alternative was adopted because, like WORM, it sets a testable outcome: the original record can be re-created.

### What the audit trail must be able to do

Three points in the release narrow what the audit-trail path requires.

1. **The outcome is re-creation.** Under the audit-trail alternative, the system must preserve records "in a manner that permits the recreation of an original record if it is modified or deleted" (Release 34-96034, section I.B).
2. **Not every intermediate state.** The proposed text required re-creation of "the original record and interim iterations of the record". After commenters noted that systems may not be able "to reproduce every version of a record that has undergone changes at multiple points in time", the final rule eliminated "the phrase 'and interim iterations of the record'". The release explains that the requirement applies to the regulatory record, for example the daily record of transactions, and "was not intended to create new recordkeeping requirements".
3. **Identity "if applicable".** A commenter noted that systems "don't always record names" and that "in many instances an automated system or process rather than a natural person will be the actor". The final text records the individual "if applicable".

The difference from WORM is therefore not that the audit-trail path is weaker, but that it locates integrity in a different place. WORM makes the stored bytes unchangeable. The audit-trail path permits change but requires that every change, its time and, where applicable, its author be captured so completely that the original can always be reproduced.

## Requirements that apply to either path

Paragraph (f)(2) continues with requirements that apply whichever option is chosen. The system must:

| Paragraph | Requirement | Architectural implication |
|---|---|---|
| (f)(2)(ii) | "Verify automatically the completeness and accuracy of the processes for storing and retaining records electronically" | Automated reconciliation between source systems and the archive, with results retained |
| (f)(2)(iii) | "If applicable, serialize the original and duplicate units of the storage media, and time-date the required period of retention" | Applies to media-based storage |
| (f)(2)(iv) | Have the capacity to "readily download and transfer copies of a record and its audit trail (if applicable) in both a human readable format and in a reasonably usable electronic format", plus the information needed to locate it | Export must include the audit trail, not just the current value |
| (f)(2)(v) | A backup electronic recordkeeping system that meets the same requirements, or "other redundancy capabilities" designed to ensure access | Redundancy that preserves the audit trail too |

And a firm using an electronic recordkeeping system must, under (f)(3): have facilities "for immediately producing the records" for SEC, self-regulatory organisation and state examiners (i); "immediately provide" any requested record (ii); and "organize, maintain, keep current, and provide promptly ... all information necessary to access and locate records" (iv). For firms on the WORM path only, (f)(3)(iii) adds "an audit system providing for accountability regarding inputting of records ... and inputting of any changes made to every original and duplicate record", with audit results preserved for as long as the audited records.

## The undertaking: executive officer or third party

Before 2022, a firm had to engage a third party able to download its records, who filed undertakings with the firm's designated examining authority. The amended rule keeps the undertaking but allows it to be signed "by either a designated executive officer or designated third party" (17 CFR 240.17a-4(f)(3)(v)(A)). The undersigned undertakes to furnish information on reasonable request and, if the firm fails to do so, "to download copies of a record and its audit trail (if applicable)" into human-readable and reasonably usable electronic formats.

A designated executive officer may appoint in writing "up to two designated officers" and "up to three designated specialists", but the appointment "does not relieve the designated executive officer of the obligations set forth in the undertaking" (f)(3)(v)(B)-(C).

Separately, where records are held by an outside service bureau or "a recordkeeping service that owns and operates the servers or other storage devices", that outside entity must file a written undertaking that the records are the firm's property and "will be surrendered promptly on request" (17a-4(i)). Cloud storage of regulatory records falls naturally into this paragraph.

## Timeline of the 2022 amendments

The SEC adopted the amendments in Release No. 34-96034, dated 12 October 2022, published at 87 FR 66412 on 3 November 2022 (Federal Register citation). The release set the compliance date for the Rule 17a-4 amendments at six months after Federal Register publication, and for Rule 18a-6 at twelve months (Release 34-96034, DATES), which places them in May 2023 and November 2023 respectively.

## Recreating the original record: a worked example

The firm in this example is fictional. Its trade blotter is kept in an operational database that is the system of record for the daily record of transactions. The firm chooses the audit-trail path.

On 14 March 2026 at 15:02:11 UTC, trade T-90113 is booked: buy 500 shares at 41.20. At 15:40:03 an operations analyst corrects the price to 41.02, a keying error. At 16:10:47 an automated allocation process splits the trade across two accounts.

| Seq | Time (UTC) | Actor | Action | Field | Before | After |
|---|---|---|---|---|---|---|
| 1 | 2026-03-14 15:02:11 | user: trader-117 | create | price, qty | (none) | 41.20, 500 |
| 2 | 2026-03-14 15:40:03 | user: ops-042 | modify | price | 41.20 | 41.02 |
| 3 | 2026-03-14 16:10:47 | process: alloc-svc v5.2 | modify | allocation | (none) | A-1: 300; A-2: 200 |

Each element of (f)(2)(i)(A) maps to the log: modifications (1), date and time (2), identity where applicable (3); the process in row 3 is identified as a process, which is what "if applicable" allows. The fourth element, "any other information needed ... to ensure the authenticity and reliability of the record and ... permit re-creation", is where most designs succeed or fail. Re-creating the record as originally booked requires that the log hold before-values for every changed field, that it be complete (no change bypasses it), and that it be protected from alteration.

The test an examiner can apply is direct: ask for T-90113 as originally created, and compare. If the system can only show the current state and a list of "price changed" events without prior values, it cannot re-create the original. If database administrators can update rows without generating log entries, the trail is not complete.

## Architecture patterns

**Event-sourced or append-only ledger.** The record is the sequence of events; the current state is derived. Re-creation of the original is trivial. The log itself must be held in an append-only log that ordinary users and administrators cannot rewrite.

**Operational database with change capture.** A conventional database with triggers or change data capture writes before and after images to a protected history store. The completeness question is whether any path, such as bulk loads, administrative fixes or schema migrations, bypasses capture. The (f)(2)(ii) duty to "verify automatically the completeness and accuracy" of storage processes is the control that detects such bypasses.

**WORM archive fed from operational systems.** The original pattern: the business system remains mutable, and snapshots or journals are written to object storage with retention locks. The archive satisfies (f)(2)(i)(B), but the firm must still meet (f)(3)(iii) on accountability for inputs and changes.

**Tamper evidence.** None of these patterns is required by name, but each benefits from making alteration detectable. Hash-chaining or Merkle-tree structures let an auditor check that a log has not been rewritten; Crosby and Wallach describe a tree-based structure that proves an event is present and that "the log, as seen

now, is consistent with how it was seen in the past". External time-stamping, as defined in RFC 3161 for requests to a Time Stamping Authority, can anchor the time of a log state outside the firm's control.

## Pitfalls

1. **Exporting the value but not the trail.** (f)(2)(iv) requires the record "and its audit trail (if applicable)". An export of current rows does not satisfy it.
2. **Privileged bypass.** A trail that records application changes but not direct database updates is incomplete.
3. **Identity collapsed to a service account.** "If applicable" excuses recording an individual when a process acts; it does not excuse hiding the individual behind a shared account when a person acts.
4. **Backup without history.** A backup that restores current state but not the audit trail does not meet the same requirements, which (f)(2)(v)(A) expects of the backup system.
5. **Locate information treated as an afterthought.** (f)(3)(iv) requires the information "necessary to access and locate records". Indexes, schemas and record-class mappings are part of compliance, not documentation.
6. **Unclear record boundaries.** The audit trail applies to the regulatory records. A firm needs a precise definition of which tables, fields and messages constitute each required record, or it cannot show that the trail covers them.

The general concept of an audit trail, meaning who changed what, when and why, is shared with other regulated sectors; Rule 17a-4 is distinctive in tying it to an explicit outcome, re-creation of the original. The site's financial services note discusses the broader requirement to defend values a firm acts on.

## Summary

Rule 17a-4(f) now lets broker-dealers choose between making stored records unchangeable and making every change reconstructable. Both paths share the same surrounding duties: automatic verification of storage, export of records with their trails, redundancy, immediate production, information to locate records, and a signed undertaking by an executive officer or third party. The audit-trail path fits modern operational systems, but it puts the burden of proof on completeness: if any change escapes the trail, the original cannot be re-created.

## Sources

1. Electronic Code of Federal Regulations, 17 CFR 240.17a-4, Records to be preserved by certain exchange members, brokers and dealers. https://www.ecfr.gov/current/title-17/chapter-II/part-240/subject-group-ECFR2fdf0ba1d7c7f55/section-240.17a-4
2. U.S. Securities and Exchange Commission, *Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants*, Release No. 34-96034, 12 October 2022. https://www.sec.gov/rules/final/2022/34-96034.pdf

3. Federal Register, SEC notice of 4 December 2025 citing Release No. 34-96034 at 87 FR 66412 (3 November 2022). https://www.federalregister.gov/documents/2025/12/04/2025-21924/agency-information-collection-activities-submission-for-omb-review-comment-request-extension-rule
4. Crosby and Wallach, *Efficient Data Structures for Tamper-Evident Logging*, USENIX Security 2009. https://www.usenix.org/legacy/event/sec09/tech/full_papers/crosby.pdf
5. IETF, RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. https://www.rfc-editor.org/rfc/rfc3161

## Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.ecfr.gov/current/title-17/chapter-II/part-240/subject-group-ECFR2fdf0ba1d7c7f55/section-240.17a-4
2. https://www.sec.gov/rules/final/2022/34-96034.pdf
3. https://www.federalregister.gov/documents/2025/12/04/2025-21924/agency-information-collection-activities-submission-for-omb-review-comment-request-extension-rule
4. https://www.usenix.org/legacy/event/sec09/tech/full_papers/crosby.pdf
5. https://www.rfc-editor.org/rfc/rfc3161

THE PUBLISHER

# About Reliable Context

Reliable Context is a system of record for organizations that fuse private and public information and must defend every value they act on.

### The guarantees

One canonical record per real thing: duplicates resolve by rule, ambiguity is shown rather than hidden, and related organizations relate without ever being merged. A verbatim, cited source and an observation date sit behind every value. Unknowns are declared as not found, blocked or not applicable with a reason, never left as an empty cell. Any past state of the record is reproducible, together with what changed since.

### Where it runs

It runs inside the customer's perimeter, one database per organization. Permitted sources, model routing, reader clearance and retention are set as the customer's own policies, and every value is exportable with its chain of custody for an auditor or regulator.

### What it is not

It is not a vector database or a RAG framework, not a data catalog, MDM or data-quality suite, not a CRM or data-enrichment vendor, and not a chatbot or AI assistant. Where a reader needs one of those, the honest answer is to say so and point them there.

### Visit

See Reliable Context.

Reliable Context is in production use in two sectors; more than six thousand of its identity decisions were made by rule and none has been reversed. Articles published here explain general practice, cite their primary and academic sources, and name the jurisdiction of any regulatory rule they describe. They are not legal, regulatory or compliance advice for a specific organization, and requirements change.

**Website:** https://reliablecontext.com

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.