



HOUSEBLEND / RESEARCH & PRACTICAL GUIDANCE

NetSuite Audit Logs for Audit Evidence: A Source Map

Make NetSuite work better for your finance and operations teams with Houseblend. We help design, implement, integrate and improve ERP systems, with practical support for the people who use them every day.

Published by Houseblend · 2026-10-15 · netsuite audit logs · netsuite audit evidence · netsuite audit trail · system notes · login audit trail · transaction audit trail · deleted records · itgc · audit readiness

Original article: <https://www.houseblend.io/articles/netsuite-audit-evidence-map>



In this article

1. Executive Summary
 2. Introduction and Background
 3. Evidence Taxonomy: Match the Event to the Source
 4. Question-to-Evidence Decision Map
 5. Build a Reproducible Evidence Packet
 6. Data Analysis and Evidence
 7. Failure Modes and Quarterly Verification
 8. Implications and Future Directions
 9. Frequently Asked Questions (FAQs)
 10. Conclusion
-

Executive Summary

An audit request should start with a **question**, a population, and a period. “Who changed a vendor bank field?” asks for record change history. “Who approved the resulting payment?” asks for an approval record and a test of its design and operation. A NetSuite change log may answer the first question while leaving the second open. The distinction matters because audit evidence must be relevant, accurate, and complete for its intended use, and a control conclusion needs more than an inquiry or a log entry. (pcaobus.org) (pcaobus.org) (www.aicpa-cima.com) (www.isaca.org)

NetSuite audit logs for audit evidence are a family of sources. The Transaction Audit Trail reports transaction history; a record-type Audit Trail searches System Notes for one record type; a general System Note search spans supported record types. System Notes v2 is a separate system with its own coverage and search path. Login Audit Trail concerns authentication, the Transaction Numbering Audit Log concerns assigned numbers, and deletion evidence depends on the analytics data source and record type. The matrix below routes eight common questions to these sources. Oracle explicitly distinguishes the transaction report from general System Note searches. (docs.oracle.com) (docs.oracle.com)

The practical output is a **reproducible evidence packet**: request wording, source, filters, period and time basis, exporting role, raw export, population tie-out, exceptions, reviewer, and a conclusion limited to what the data show. The Public Company Accounting Oversight Board (PCAOB) directs auditors to test the accuracy and completeness of company-produced information and to document the purpose, source, and conclusion of audit work. The Institute of Internal Auditors (IIA) emphasizes work that another competent person could repeat. These sources inform the packet design; an auditor decides what evidence is sufficient for the engagement. (www.theiia.org) (www.aicpa-cima.com)

There are specific traps as of **September 2026**. A System Notes v2 view can default to the last **30 days**, which is a display filter rather than a stated retention period. Workflow execution logs are deleted every **60 days**; script-log availability depends on the retrieval surface. The Script Execution Logs page shows **30 days** of logs, while Execution Log subtab and Server Script Log search results can be purged earlier under shared storage limits. ([Oracle: Script Execution Logs](#)) A missing row can reflect source coverage, permissions, filter settings,

or elapsed time. These periods should not be generalized to other NetSuite logs. The export and review procedure should therefore be checked in a non-production account and refreshed after each release. (docs.oracle.com) (docs.oracle.com) (docs.oracle.com) (nvlpubs.nist.gov) (www.cyber.gov.au)

Introduction and Background

A controller receiving an audit request often sees the word “audit trail” without an object or assertion. That wording can send an administrator to a familiar report even when the auditor needs a different population. The useful first step is to rewrite the request as a testable question: **which object, which event, which people, which period, and which assertion?** A purchase order edit, an employee role assignment, and a login are different events. Their records do not have interchangeable fields. Oracle describes the transaction audit trail as a transaction history report, while the record-type trail is a search over System Notes for a selected record type. (www.aicpa-cima.com)

This report is for controllers, Sarbanes-Oxley (SOX) and information technology general control (ITGC) owners, internal auditors, external-audit coordinators, and NetSuite administrators. It treats a log as **observational evidence**. A row can identify an event and actor in the source system, subject to scope and access checks. It does not alone show that an independent person approved the event, that the population is complete, or that a control operated consistently. PCAOB guidance separates the reliability of company-produced information from conclusions about operating effectiveness. (pcaobus.org) (www.isaca.org)

Houseblend describes NetSuite compliance work that includes roles, approval logic, audit trails, and internal controls. That perspective is relevant to designing repeatable searches and review procedures, but the native evidence sources discussed here are Oracle NetSuite features. The consultancy also describes saved searches and role reviews as part of ongoing monitoring. (www.houseblend.io) (www.houseblend.io)

The product paths below are **documentation paths, not account-tested instructions**. Menus, available fields, permissions, record coverage, and exports must be confirmed in a current non-production account using the same role that will produce the packet. The report avoids an assumed universal retention period. The Australian Cyber Security Centre ties log retention to risk assessment, and NIST ties it to the applicable records-retention policy in its scoped guidance. Neither statement establishes a NetSuite-wide duration. (www.cyber.gov.au) (nvlpubs.nist.gov) (csrc.nist.gov)

Evidence Taxonomy: Match the Event to the Source

Transaction history and record changes

The **Transaction Audit Trail** is the transaction-centered report. Oracle describes a history of transactions entered in NetSuite, with the actor and creation or modification time. It is a useful starting point for a journal, bill, invoice, payment, or similar transaction question. The **record-type Audit Trail** narrows a System Note search to a selected record type. A **general System Note search** is appropriate when the question spans a record class or requires filters such as user, role, date and time, change type, field, old or new value, or context. Oracle's general search is at Reports > New Search > System Note.

System Notes v2 deserves a separate decision. Oracle says NetSuite has two change-tracking systems. The v2 record view offers date and text filters and exposes headings such as user, role, context, action, object, and values, but Oracle says v2 tracks significant changes only and does not currently log general company setting changes. The supplied v2 workbook has specific supported records and a default date criterion. It should not be treated as a universal replacement for original System Notes. **Attribution caveat:** In the v2 User field, an inactive user is represented by the oldest active administrator-user; managed-bundle activity identifies the user who installed the bundle. Corroborate identity before concluding who performed a historical change from the displayed User value alone. (Oracle: [Viewing System Notes v2](#))

Authentication, numbering, deletion, and automation

The **Login Audit Trail** answers a session or authentication question. Oracle locates it at Setup > Users/Roles > View Login Audit Trail and says it captures the IP address at the beginning of a session. An advanced search can expose status, address, role, request URI, and related fields, depending on the selected result columns. It does not identify who changed a bill merely because the actor logged in. (cheatsheetseries.owasp.org)

The **Transaction Numbering Audit Log** is for sequence questions. Oracle says it includes numbers associated with standard and custom transactions that were deleted or never created. A gap in displayed transaction numbers is therefore a prompt to inspect the numbering log, not proof that a transaction was deleted. Conversely, the numbering log is not a substitute for a record-change trail or an approval record. (pcaobus.org)

Deleted-record evidence follows a branching path. Oracle lists record types for which deletion instances create a log. For records using the old data source, a **Deleted Record search** is available at Reports > New Search. For the new analytics data source, Oracle describes a SuiteQL query of `deletedRecordInConnect` and a NetSuite Analytics Warehouse feature dependency. An administrator should establish the record type and data source before promising a deletion export.

Workflow history and execution logs answer different automation questions. The workflow definition History subtab records revisions; an execution log tracks actions and transitions for a state visit when logging is configured. Oracle states that workflow execution logs are deleted every 60 days. Script Execution Logs have their own page and purge behavior. These troubleshooting records can help explain automation context, but an event recorded by a workflow or script is not itself evidence that the business approval rule was appropriate.

Question-to-Evidence Decision Map

Begin by classifying the request: a **record mutation** goes to the relevant System Notes route; a **transaction lifecycle** question goes to Transaction Audit Trail; a **session** question goes to Login Audit Trail; a **sequence** question goes to Transaction Numbering Audit Log; and an **automation** question needs workflow or script evidence plus the resulting record trail. If a question asks whether a control worked, add the control definition, population and sample method, reviewer record, and exception disposition. PCAOB AS 2201 distinguishes testing operation from observing the existence of a control. (pcaobus.org) (pcaobus.org) (www.aicpa-cima.com)

Table 1 is an intake form to complete before running a search. A signed request and stable criteria make later reproduction easier. PCAOB documentation guidance identifies purpose, source, preparer, reviewer, and conclusion; IIA guidance similarly expects another competent person to be able to repeat the work. (www.theiia.org) (www.isaca.org)

Intake field	Example entry	Why it matters
Auditor question	Who changed vendor bank details during the quarter?	Separates a field edit from payment approval.
Population and assertion	Active vendors with relevant field changes; completeness and authorization	States what the export must cover.
Period and time basis	Quarter start through quarter end, inclusive; account time zone recorded	Makes boundaries reproducible.
Object and identifiers	Vendor internal ID and selected bank-field identifier	Supports a tie-out to the record population.
Candidate source and role	System Note search; documented export role	Prevents a partial view caused by access.
Delivery and reviewer	CSV plus criteria capture; controller review	Preserves data and signoff separately.

The form is deliberately specific about **time basis**. OWASP distinguishes event time from logging time, and the Australian Cyber Security Centre recommends consistent date-time formatting across systems. A date-only export that silently crosses a time-zone boundary can misstate the population. (cheatsheetseries.owasp.org) (www.cyber.gov.au) (cloudsecurityalliance.org)

Table 2 maps frequent requests to a first source. “Available fields” lists fields to validate for the account and record, not a guarantee that every record exposes them. “Unknown” means Oracle's cited page did not establish the item. The citation in the Oracle source column is the product basis for that row.

Auditor question	Process	NetSuite evidence source	Navigation or search	Key filters	Available fields to validate	What it proves	What it does not prove	Known limitation	Export format	Required permission to validate	Reviewer	Oracle source	Last verified
Who edited a vendor bank field?	P2P, vendor master	Record-type trail or System Note search	Vendor list Audit Trail or Reports > New Search > System Note	Vendor ID, field, actor, period	Date/time, user, role, old/new value, context	Logged field change	Payment approval	Record/field coverage varies	CSV/XLS X/PDF for accessible search	Record access, Notes Tab and export rights; test scope	AP manager	(docs.oracle.com)	2016-09-29

Auditor question	Processes	NetSuite evidence source	Naviga tion or search	Key filter s	Availa ble fields to valida te	What it prov es	Wh at it doe s not pro ve	Known limitation	Exp ort form at	Requi red permission to valida te	Re vi ewer	Or acl e source	L a st v er ifi e d
Who created or changed a bill, invoice, or journal?	P2P , O2 C, GL	Transa ction Audit Trail	Transa ctions > Manag ement > View Audit Trail	Type , action, user, date, amo unt	Trans action , actor, time; inspec t detail and GL impac t	Repo rted trans action activi ty	Auth oriz atio n or com plet ene ss	Original System Notes route	Acco unt-teste d expo rt	Audit Trail permis sion for custo m role	Co ntr oll er	(do cs. ora cle .co m)	2026-09-29
Which item-master field changed?	Item mas ter	Record -type Audit Trail or genera l Syste m Note search	Item list Audit Trail; System Note search	Item, field, date, actor	Chan ge type, before /after value, conte xt	Logg ed item chan ge	Busi nes s reas on for cha nge	Validate item type and field	CSV/ XLS X/PD F for acce ssibl e sear ch	Reco rd/sear ch and export rights	Item ow ne r	(do cs. ora cle .co m)	2026-09-29
Who gained or changed a role?	Access ad mini stration	Emplo yee Access > History ; role search ; suppor ted v2 view	Emplo yee record or role search	Emp loyee, role, per mission, perio d	Role- chang e action /date, permi ssion level	Reco rded assign men t or level chan ge	Acc ess-revi ew appro val	Legacy notes omit some role-tab changes	Sear ch expo rt where supported	Role and search acces s, test	IT G C ow ne r	(do cs. ora cle .co m)	2026-09-29
Who logged in from an address?	Aut hen ticat ion	Login Audit Trail	Setup > Users/ Roles > View Login Audit Trail	Ema il, role, statu s, date, IP	Login time, status , IP, role	Reco rded sessi on event	A sub sequ ent reco rd edit	Logout entries depend on behavior	CSV	View Login Audit Trail	Se cu rity ow ne r	(do cs. ora cle .co m)	2026-09-29

Auditor question	Processes	NetSuite evidence source	Navigational or search	Key filters	Available fields to validate	What it proves	What it does not prove	Known limitation	Export format	Required permission to validate	Reviewer	Oracle source	Last verified
Was a record deleted?	Master or transaction data	Deleted Record search or SuiteQL deletion table	Old source search; new source SuiteQL	Type, ID, date, actor	Deletion entry per supported type	Logged deletion	Full pre-deletion content	New-source deletion time displays in Pacific Time; document conversion before period-boundary tests; type/source and Warehouse dependency	Account-tested export	Deleted Record Search or query access	Data owner	(docs.oracle.com)	2026-09-29
Why is a number absent?	Transaction numbering	Transaction Numbering Audit Log	Transactions > Management > Transaction Numbering Audit Log	Number range, type, period	Number and status details to validate	Sequence disposition	Approval or financial impact	Export method unknown	Unknown; capture method tested	Numbering-log access	Controller	(docs.oracle.com)	2026-09-29
What automation ran or changed?	Workflow/s script	Workflow History and execution log; script log	Workflow record; Script Execution Logs	Workflow, state, script, time	Revision, action/transition, error/log	Recorded execution or definition revision	Control design or approval	Logging setting; finite log life	Account-tested export	Workflow permission, SuiteFlow	Processes owner	(docs.oracle.com)	2026-09-29

The table is a **routing aid**, not a completeness certification. A search should be repeated with a permitted role and cross-checked against the underlying transaction, master-data, or workflow population. For a journal question, a general ledger tie-out may be necessary; for a vendor question, the vendor population may need an independent listing. PCAOB guidance explicitly calls for testing company-produced information for accuracy and completeness and for sufficient precision and detail. (www.aicpa-cima.com)

Build a Reproducible Evidence Packet

Preserve the query, the population, and the export

A usable packet begins with the **auditor's exact request** and the preparer's interpretation of it. Record the business process, the event, the field or transaction type, entity and subsidiary scope, inclusive dates, and the requested assertion. Purchase-to-pay (P2P), order-to-cash (O2C), and general ledger (GL) requests should not be grouped into a single export merely because they share a period. Keep an intake record for questions that need the auditor to define whether the target is a change, approval, completeness, or access assertion. The PCAOB's information-produced-by-the-company guidance explains why a technically correct query still needs a completeness and accuracy assessment. (pcaobus.org) (www.aicpa-cima.com)

Capture the **source configuration**: exact report or saved-search name, criteria, result columns, role, account/subsidiary, time zone, run time, and any visible record-type or feature setting. Save the raw export and, when criteria do not travel with it, a screenshot of the filter screen. A screenshot is a supplement because it does not contain the row population needed for sorting, recounting, and exception testing.

(www.archives.gov) AICPA audit data standards emphasize accurate data in a usable format through a repeatable process; PCAOB documentation guidance calls for purpose and source to be clear. (www.aicpa-cima.com) (pcaobus.org) (www.archives.gov)

Use a **stable file name**, for example 2026Q3_VendorBankChange_SystemNote.UTC_20261001_v01.csv. Its components identify period, object, source, time basis, extraction date, and version. The period and extraction date are not interchangeable: a file produced after quarter end can still report quarter activity. Store the query definition beside the export, not only inside a personal saved-search folder. OWASP notes that event and logging timestamps can differ; Cloud Security Alliance calls for a reliable time source across relevant systems. (cheatsheetseries.owasp.org) (cloudsecurityalliance.org) (www.cyber.gov.au)

Validate a **population tie-out** before sampling. Record the row count, filter boundaries, selected columns, distinct record count, and totals where a financial amount is relevant. Reconcile to an independent source appropriate to the question, such as a transaction listing or master-record listing. Investigate unexplained differences instead of deleting rows for a cleaner file. The Financial Reporting Council's ISA (UK) 500 requires consideration of the accuracy and completeness of entity-produced information; the U.S. PCAOB adds whether it is sufficiently precise and detailed. These are scoped auditing standards, not product guarantees. (media.frc.org.uk) (pcaobus.org) (www.aicpa-cima.com)

Finally, document **review and disposition**. Preserve who prepared the packet, who reviewed it, what exceptions were identified, how they were resolved, and the conclusion's limit. For a public-company audit, PCAOB documentation guidance identifies preparers and reviewers; IIA standards require internal auditors to document information and evidence supporting engagement results. The same design is a practical internal packet convention even when those standards do not directly govern the organization. (www.theiia.org) (www.isaca.org)

Worked example: a change is not an approval

Consider a **hypothetical example** in which an auditor asks, “Who changed vendor bank details and who approved the next payment?” The first clause points to a vendor record audit trail or System Note search filtered to the vendor, field, and period. Capture actor, role, date/time, context, and available before/after values. The second clause requires the payment and its approval evidence under the configured process, plus evidence that the approval was performed by the intended reviewer. The System Note row can support a statement about a recorded field edit. It cannot by itself establish the approval of a separate payment. Oracle documents the change-search filters; PCAOB AS 2201 describes operating effectiveness as a question of how a control operated. (www.aicpa-cima.com)

If the field was populated by an integration or script, retain the **context** reported in the change history and then inspect the relevant automation record or log. This is an investigative branch, not a reason to infer that the automation authorized itself. If a workflow execution log is needed, confirm logging was enabled and preserve it promptly because Oracle says those logs are deleted every 60 days. If the approval occurs outside NetSuite, label the external record and its custodian in the intake; do not silently treat the NetSuite mutation as a substitute.

Data Analysis and Evidence

There is no reliable public benchmark for the percentage of audit questions answered by a given NetSuite log, and this report does not extrapolate one. The useful quantitative analysis is a **source-coverage inventory** derived from Oracle's documented features. Table 2 has **eight** question rows, but they route to multiple source families, and several rows need a second approval, population, or external record. That count describes this editorial map, not the coverage of a customer's configured account. The relevant statistical claim is therefore narrower: one export is not a measured substitute for eight tested assertions. (pcaobus.org) (www.isaca.org)

Table 3 gathers product-specific numbers that affect evidence timing or extraction. Each applies only to the named feature. The right column states what should be checked before the number is used operationally.

Documented number	Source and scope	Evidence implication	Account check
30 days	Default System Notes v2 record-view time interval (docs.oracle.com)	A short initial view can omit older events from the screen.	Expand the date filter; do not call this retention.
60 days	Workflow execution logs deleted after this period (docs.oracle.com)	Preserve a relevant troubleshooting log promptly.	Confirm logging and the workflow setting.
30 days	User-generated script logs are purged after 30 days, but availability depends on the retrieval surface (docs.oracle.com).	Execution Log subtab and Server Script Log search results can disappear earlier when shared storage limits trigger purges. The Script Execution Logs page retains logs for 30 days regardless of volume (docs.oracle.com).	Use Customization > Scripting > Script Execution Logs for the documented 30-day repository. Record the retrieval surface used in the evidence packet, along with the script, selected log level, and date filters.

Documented number	Source and scope	Evidence implication	Account check
60 days	System error script logs purged after this period (docs.oracle.com)	This purge statement does not establish 60-day availability through the Script Execution Log page; Oracle says that page shows log details for 30 days (docs.oracle.com).	Verify the accessible source and its period before relying on an error log.
10,000 entries	Script Execution Logs download may be limited to this many entries (docs.oracle.com)	Large extracts may need partitioned requests and reconciliation.	Compare exported count with the search result.

The numbers should **not** be read as a NetSuite-wide retention schedule. Oracle's documentation presents separate behaviors for v2 display, workflow logs, and script logs. NIST's controlled-unclassified-information requirements tie record retention to a policy, while the Australian Cyber Security Centre recommends setting periods from risk. These are general design references with defined scopes. For a customer, the correct policy and any external preservation process must be established independently. (nvlpubs.nist.gov) (www.cyber.gov.au) (csrc.nist.gov)

The map also reveals a structural evidence gap: **event evidence** and **control evidence** are separate. A login entry can support that a session event was recorded; it does not show a subsequent transaction action. A numbered-transaction entry can explain a sequence number; it does not demonstrate approval. A workflow execution log can report a state visit; it does not establish whether the rule was designed appropriately. This is a synthesis of the documented fields and PCAOB's distinction between observing events and testing operation. (pcaobus.org) (www.aicpa-cima.com)

Failure Modes and Quarterly Verification

Wrong time basis. An extract with a date range can exclude boundary events if the preparer and reviewer use different time zones. Record the account display zone, selected filter zone, and export timestamp. For deleted records using the new analytics data source, Oracle says deletion date and time display in Pacific Time Zone; document the conversion before testing period boundaries. Convert only in a documented working copy and retain the original. OWASP differentiates event time from logging time; the Australian Cyber Security Centre recommends a consistent format across systems. (cheatsheetseries.owasp.org) (www.cyber.gov.au) (cloudsecurityalliance.org)

Missing context or partial access. A role may see only a subset of System Notes, and original System Notes and v2 do not have identical scope. Oracle says users with Notes Tab permission see only notes for their own changes unless additional access applies; it separately documents administrator or specific analytics permissions for wider queries. Test the producing role against a known event before treating an empty result as absence of activity.

Over-broad exports. Pulling every field and every entity can produce an impressive but hard-to-review file. Set a narrow question, then keep enough identifiers and context to test completeness. PCAOB AS 1105 asks whether company information is precise and detailed enough for the purpose. AICPA guidance also calls

attention to authenticity and management bias when assessing audit evidence. (pcaobus.org) (www.aicpa-cima.com) (www.isaca.org)

Screenshot without criteria. A cropped screen can show an event while hiding the period, role, or filter. Preserve the raw file and search definition. NARA describes electronic-record integrity in terms of a record being complete and unaltered; NIST calls for protecting audit information and logging tools from unauthorized access. These are useful preservation principles, not assertions that a NetSuite export is immutable after download. (www.archives.gov) (nvlpubs.nist.gov) (cloudsecurityalliance.org)

Assumed permanence. Oracle gives finite periods for workflow and script logs, but those statements do not define the life of every System Note, login event, or deleted-record entry. Assign retention and capture procedures by evidence source and applicable policy. The Australian Cyber Security Centre's risk-based approach and NIST's policy language both support making the rule explicit. (www.cyber.gov.au) (nvlpubs.nist.gov) (csrc.nist.gov)

A **quarterly verification checklist** is practical because account configuration and product behavior can change. The owner should test a known record change and its old/new fields, a transaction modification, a login result, a deletion in the relevant data source, a numbering example, and a workflow execution event. Verify permissions and export buttons using the actual evidence role. Re-run boundary-date tests and reconcile sample row counts to independent populations. Record Oracle page links and the account release at the time of testing. The IIA's repeatability criterion and PCAOB's company-data reliability criterion provide a reason to keep this test record. (www.theiia.org)

- **Scope:** Confirm the object, assertion, subsidiaries, record type, and available field history.
- **Access:** Test the production evidence role, not only an administrator role.
- **Time:** Record the display zone, filter boundaries, and export time.
- **Coverage:** Check System Notes versus v2 and the deletion data source.
- **Automation:** Confirm workflow logging and script log collection before the request is urgent.
- **Export:** Compare search results with exported rows and preserve the query definition.
- **Review:** Assign a business owner and document exception disposition.

Implications and Future Directions

The durable improvement is an **evidence catalog** maintained with the NetSuite configuration. It should list the question, native source, supported record types, field-level caveats, permissions, export method, owner, tie-out, and last account test. A catalog turns a late audit request into a controlled extraction and makes known gaps visible before the period closes. (www.cisa.gov) NIST's log-management guidance speaks to maintaining practices across an enterprise, while the IIA's documentation rule emphasizes enough detail for repeatable work. (csrc.nist.gov) (www.theiia.org) (www.archives.gov)

A second improvement is to separate **collection** from **assessment**. Administrators can produce a technically reproducible extract. Controllers and process owners can verify the population and explain business exceptions. Auditors decide whether the evidence supports the requested assertion. PCAOB guidance gives

more weight to evidence obtained directly by an auditor and calls for assessment of company-produced data; ISACA defines sufficient evidence in terms of whether another auditor could reach the same conclusion. (pcaobus.org) (www.isaca.org)

Where a record lacks an expected field, mark **unknown** and test it in the configured account. Where a log's finite life is shorter than the audit cycle, establish a scheduled capture or another documented control under the organization's policy. Where the required approval occurs outside NetSuite, identify that source rather than stretching a System Note into an approval certificate. Cloud Security Alliance recommends restricting log access and using reliable time sources; CISA recommends centralized review of logs. These are design references, not a claim that a particular NetSuite setup already implements them. (cloudsecurityalliance.org) (cloudsecurityalliance.org) (www.cisa.gov) (csrc.nist.gov)

Frequently Asked Questions (FAQs)

Which NetSuite audit trail report should answer a transaction request?

Start with **Transaction Audit Trail** when the request concerns transaction creation, change, or deletion history. A System Note search can add field-level filters or cover other record types. Validate the transaction type, role, period, and displayed columns in the account before export.

Are System Notes and System Notes v2 the same evidence source?

No. Oracle documents **two change-tracking systems** with different scope and access paths. The original record-type Audit Trail is a System Notes search, and v2 has a separate record view and workbook. Confirm support for the exact record and field rather than merging their results without a mapping.

Where is login evidence exported?

Oracle places the **Login Audit Trail** at Setup > Users/Roles > View Login Audit Trail and documents CSV export for its search. Capture the selected criteria and the role used to run it. A login row supports a session question, not an inference that the same user approved a transaction.

How can deleted records be found?

First identify the record type and analytics data source. Oracle describes a **Deleted Record search** for the old source and a `deletedRecordInConnect` SuiteQL path for the new source, with a Warehouse feature dependency. Do not assume every deleted record type is logged.

How are role changes and workflow runs evidenced?

For **role assignments**, inspect employee Access > History and supported role searches or v2 views. For a workflow run, examine execution logging and the resulting record history; for a workflow definition change, inspect revision history. Each path answers a different question, and execution logging has its own finite life.

Conclusion

The right NetSuite evidence source follows the **auditor's question**. Transaction Audit Trail addresses transaction history; System Notes and record-type trails address recorded changes; Login Audit Trail addresses session activity; deletion paths, numbering logs, and automation histories answer narrower questions. A route is only a starting point. The preparer must confirm account coverage, permissions, criteria, time basis, and export completeness before interpreting an empty or populated result.

A useful packet lets another person reconstruct the query and understand its limits. It contains the request, search criteria, export, population tie-out, reviewer, and exception disposition. It also says plainly whether the artifact shows an event, a configuration revision, an approval, or a test of a control. This structure aligns with the IIA's repeatability principle and PCAOB's documentation and operating-effectiveness distinctions.

The final control decision belongs to the relevant auditor and process owner. For an operating team, the immediate action is to maintain a tested question-to-source map and refresh it each quarter. Unknown record coverage and feature dependencies should remain marked until verified in the actual NetSuite environment.

Source links

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

1. <https://pcaobus.org/oversight/standards/auditing-standards/details/AS1105>
2. <https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201>
3. <https://www.aicpa-cima.com/news/article/8-things-to-know-about-the-audit-evidence-standard>
4. <https://www.isaca.org/resources/glossary>
5. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N556825.html
6. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_4031815869.html
7. <https://houseblend.io/articles/netsuite-audit-evidence-pack>
8. https://www.theiia.org/globalassets/site/standards/editable-versions/globalinternalauditstandards_2024january9_editable.pdf
9. <https://www.aicpa-cima.com/resources/download/order-to-cash-subledger-standard-audit-data-standards>
10. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_4375937190.html
11. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_159499608205.html
12. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N2788150.html
13. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N3352137.html
14. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/800-171r3/NIST.SP.800-171r3.html>
15. <https://www.cyber.gov.au/business-government/detecting-responding-to-threats/event-logging/best-practices-for-event-logging-and-threat-detection>
16. <https://www.houseblend.io/services/netsuite-compliance>
17. <https://csrc.nist.gov/pubs/sp/800/92/final>
18. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/subsect_158108595525.html
19. https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html
20. <https://houseblend.io/articles/netsuite-deleted-record-sync-reconciliation>

21. <https://cloudsecurityalliance.org/blog/2025/07/28/implementing-ccm-cloud-security-monitoring-logging>
22. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N675070.html
23. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N673560.html
24. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/bridgehead_4591976451.html
25. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N324233.html
26. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_163584624721.html
27. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N253418.html
28. <https://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html>
29. <https://pcaobus.org/oversight/standards/auditing-standards/details/AS1215>
30. https://media.frc.org.uk/documents/ISA_UK_500_Updated_September_2025.pdf
31. https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf
32. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>
33. <https://houseblend.io/articles/netsuite-roles-permissions-sod-audit>

THE PUBLISHER

About Houseblend

Houseblend is a NetSuite consulting firm serving finance and operations teams. We help organizations implement ERP systems, connect business applications, improve existing configurations and maintain the systems that support everyday work. Our audience includes finance leaders, controllers, operations managers, NetSuite administrators and implementation teams.

Implementation and architecture

Houseblend provides NetSuite implementation, architecture and data migration services. We help teams evaluate how business processes, reporting requirements and existing data should fit together in an ERP environment. Training supports the people responsible for adopting and operating the resulting system.

Integrations, customization and AI

Our services include NetSuite integrations and customization, as well as AI integrations and AI transformation work. These engagements connect ERP data and workflows with the broader application landscape. The right design depends on the organization's systems, controls and operating needs.

Improve and support an existing system

Houseblend offers NetSuite health checks, optimization, managed support and project rescue services. We also provide expertise for analytics and specialist workflows, including NetSuite Analytics Warehouse, warehouse management and field service management. Published educational material helps teams investigate options and prepare informed questions for their implementation or support work.

Work with Houseblend

Explore [NetSuite implementation](#), [integrations](#), [managed support](#) and [AI integrations](#). [Contact Houseblend](#) to discuss your current system and priorities.

Article examples explain concepts rather than promising a particular license, product capability, delivery schedule or outcome. Engagement scope is confirmed with the Houseblend team.

Website: <https://www.houseblend.io>

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.