HOUSEBLEND

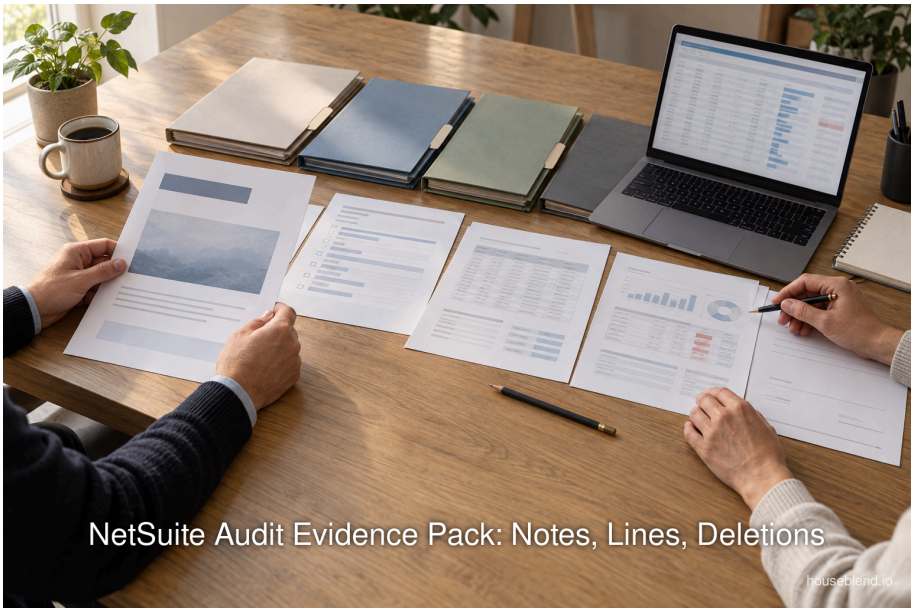
HOUSEBLEND / RESEARCH & PRACTICAL GUIDANCE

NetSuite Audit Evidence Pack: Notes, Lines, Deletions

> 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 · 2026-09-27 · netsuite audit evidence pack · netsuite system notes · netsuite audit trail · deleted records · line level audit trail · system notes v2 · saved search audit · audit evidence · netsuite integrations

Original article: https://www.houseblend.io/articles/netsuite-audit-evidence-pack



In this article

Executive Summary

A **NetSuite audit evidence pack** should begin with the auditor's question: which object changed, which event matters, who acted, and what period is in scope. Transaction Audit Trail and transaction System Notes address header activity and field changes; line History addresses updates to existing lines; Deleted Record searches address deletion events; Analytics Audit Trail and workflow History address configuration edits; execution logs help establish what scripts or integrations ran. Oracle's line History documentation expressly excludes line creation and deletion, while its v2 documentation distinguishes a supported record's surviving notes from original System Notes that disappear with a deleted parent. The pack must state those boundaries rather than treat every native history view as complete. (pcaobus.org) (www.gao.gov)

As of September 2026, collection timing is a material part of the decision. Oracle documents a **30-day** default display interval in the System Notes v2 viewer and a **60-day** rolling saved-search Execution Log. Other runtime and export views also have short, source-specific windows, as Table 3 details. None establishes a universal NetSuite retention term. (docs.oracle.com) (docs.oracle.com) (nvlpubs.nist.gov) (www.cisa.gov) (csrc.nist.gov)

For each request, retain the approved population, search definition or navigation path, scoped export, stable record identifiers, relevant configuration snapshot, count reconciliation, exceptions, and reviewer sign-off. A screenshot may document a setting, but a repeatable extract and the method used to test it are needed to evaluate the information. PCAOB AS 1105 requires testing the accuracy and completeness of company-produced information or relevant controls and evaluating whether the output is precise enough for the audit purpose. GAO likewise uses accuracy, completeness, and applicability to assess audit data. (pcaobus.org) (pcaobus.org) (www.gao.gov) (www.theiia.org) (www.aicpa-cima.com)

The choice of native source is only the beginning. A restricted role can produce a misleadingly empty result; a timestamp can use company or Pacific time depending on the view; a deletion event may lack former field values. The controller should own the question and population, the administrator or integration owner should document collection, and an independent reviewer should test the handoff against source records. NIST's

chain-of-custody definition and the Institute of Internal Auditors' repeatability criterion support retaining who handled each file, when, and how another reviewer can reproduce the work. (csrc.nist.gov) (www.theiia.org) (www.cisa.gov)

Introduction and Background

An auditor asks who changed a transaction, what changed on a line, or whether a record disappeared. These sound like one request for an "audit trail," but they identify different objects and therefore different NetSuite evidence sources. **Transaction Audit Trail** summarizes transaction activity, **System Notes** records field changes on supported records, the line History view addresses edits to existing transaction lines, and the Deleted Record search addresses deletion events. Oracle expressly treats the transaction trail as a System Notes feature; it is not a universal interface to every log. (www.gao.gov)

The practical unit of work is an **evidence request**, not a screen. For each request, the controller and auditor should agree on the object, field or event, actor, legal entity or subsidiary, period, time zone, and assertion being tested. A list of matching rows is only the start: the team must demonstrate that the query included the intended population, that the exported fields identify the source records, and that a reviewer can repeat the extraction. Public Company Accounting Oversight Board (PCAOB) AS 1105 explicitly calls for testing the accuracy and completeness of company-produced information or the controls over those qualities; it also asks whether the information is sufficiently precise for the audit purpose. (pcaobus.org) (pcaobus.org) (www.theiia.org)

This guide describes a **native-source evidence pack** as a controlled bundle of a request sheet, search or report definition, source export, population reconciliation, configuration snapshot where needed, and reviewer record. It does not assume that the presence of a log satisfies any particular auditor. The Government Accountability Office (GAO) frames data reliability around accuracy, completeness, and applicability, a useful discipline for deciding whether a NetSuite extract actually answers the question. (www.gao.gov) For teams that need assistance producing this bundle, Houseblend identifies NetSuite compliance, managed support, and integrations among its services; the relevant decision remains which account-specific source and control the auditor accepts. (www.houseblend.io) (www.iso.org)

Audit Questions and the Source Map

Intake: define the object before the search

Write the request in four parts. **Object** is the transaction header, transaction line, master record, saved search, workflow, or integration request. **Event** is create, edit, execute, export, or delete. **Actor** is a named user, role, script, or integration identity. **Period** is a bounded timestamp range with an explicit time-zone convention. Add the field name or transaction internal ID when available. This intake is an editorial control: it reduces the chance that a plausible but unrelated log is handed over. BDO's 2026 guidance on information produced by an entity recommends identifying relevant fields, totals, status codes, dates, and entity scope before testing a report. (www.bdo.com) (www.gao.gov) (www.isaca.org) (www.aicpa-cima.com)

Table 1 maps five common requests to the native starting point and the evidence needed around it. Each row is a retrieval hypothesis to validate in the client's account, since feature coverage and permissions vary by record and role.

Auditor question	Native source and filter	Known boundary	Owner and retained evidence
Who changed a transaction header?	Transaction Audit Trail for transaction activity; transaction System Notes or System Note search for the specific field, actor, and period.	Confirm whether creation notes were generated and whether the requested value is a header field.	Controller defines the population; administrator exports the note results, filter definition, transaction IDs, and review record.
Who changed a transaction line?	Line History on the line, or transaction saved search with Line System Notes fields.	The documented line trail covers edits to existing lines, not their creation or deletion.	Transaction owner identifies the line and retains the line-level export plus a current transaction snapshot.
What record was deleted?	Deleted Record search for the relevant data source and record type; System Notes v2 only where that record is supported.	A deletion log may identify an event without preserving the deleted record's full prior contents.	Administrator scopes deletion period and type; reviewer matches IDs to source population and other retained records.
Who edited a saved search or workflow?	Analytics Audit Trail for saved-search definition; workflow History for definition edits; execution logs for runs.	Definition history and execution history answer different questions.	Search or workflow owner retains definition snapshot, change history, and reviewer conclusion.
What integration executed?	Changed record's System Notes context plus the applicable script, SOAP, REST, or RESTlet execution log.	A context label does not by itself prove which payload or business event ran.	Integration owner retains request correlation, deployment or integration identity, log extract, and mapping snapshot.

The crosswalk deliberately separates **event evidence** from **state evidence**. A change row can identify the actor and old and new values, while a contemporaneous configuration or transaction snapshot establishes how the item stood when the test was performed. An auditor may also ask for a source-to-report trace: BDO recommends tracing selected source transactions into the report for completeness and vouching report items back to source records for accuracy. (www.bdo.com) (www.bdo.com) The two directions test different failure modes and should be recorded separately. (www.theiia.org)

Audit evidence checklist: minimum intake record

- **Question and assertion:** Copy the auditor's wording and state whether the test concerns occurrence, authorization, completeness, or accuracy. (pcaobus.org)
- **Population:** Name subsidiaries, transaction types, records, and boundary dates; note exclusions and why they are outside scope. (www.gao.gov)
- **Source and identifiers:** Confirm the native source covers the record type and event, test the extracting role, and collect internal ID, document number, line identity, and search or workflow ID before extracting.
- **Time basis:** Record the displayed time zone and any company-time or Pacific-time convention present in the chosen log.
- **Review path:** Record preparer, reviewer, extraction date, source version, the test that reconciles the output to the agreed population, and the auditor's required corroboration. (pcaobus.org)

Transaction and Record Change Evidence

Transaction header: summary first, field detail second

The **Transaction Audit Trail** is a fast way to narrow transaction activity. Oracle places it under Transactions > Management > View Audit Trail and describes a one-line summary per transaction with links to detail. The page offers filters for transaction activity, but Oracle directs users to a System Note search for advanced filters, selectable result columns, exports, and saved searches. Therefore, a defensible header-change pack often begins with the trail to identify candidate transactions and then uses field-level System Notes as its retained extract. (docs.oracle.com) (docs.oracle.com) (www.gao.gov)

For a request such as "who changed the memo on journal J-104 during the close," the administrator should search the journal's internal ID and memo field within the approved period, retain old and new values, actor, role if displayed, context, and change timestamp, and then compare the extract to the journal's current state. Oracle says transaction System Notes display timestamps in the **company time zone**; the role column may require a customized view. A current state snapshot matters because a later edit can supersede the value visible in the selected event. (docs.oracle.com) The auditor should decide whether this is sufficient for the assertion, using the precision and detail criterion in AS 1105. (pcaobus.org) (www.aicpa-cima.com)

Creation coverage needs a specific check. Oracle documents a "Log System Notes on Updates Only" preference that determines whether notes are generated when a transaction is created. An absence of a creation row should therefore trigger an account-setting check and corroboration with transaction history, not an inference that no creation occurred. (docs.oracle.com) The same logic applies when the requested field is calculated or system populated: define what the log captures before interpreting an empty result. AICPA guidance emphasizes evaluating accuracy, completeness, authenticity, and possible bias in audit information regardless of source. (www.aicpa-cima.com) (www.gao.gov)

Other records: record-type audit trail and System Notes

A **record-type Audit Trail** is a preset search of System Notes for a selected type, such as a customer or employee. It is useful when the question concerns a population of one record type. Oracle's general System Note search crosses supported record types and offers broader filtering and export options. For a sampled master-data change, the record's own System Notes subtab can establish the exact event, while a saved System Note search makes the population reproducible. (docs.oracle.com) (www.gao.gov)

Access is part of the evidence design. Oracle says a viewer needs record access plus the Notes Tab permission, and that the Notes Tab permission alone can limit visibility to changes the viewer made. Querying all System Notes through the analytics data source requires an Administrator or System Notes for Analytics and REST permission. An empty extract produced by a restricted role cannot be treated as proof of no activity until access is checked. (docs.oracle.com) The controller should sign off on the intended population; the administrator should document the extracting role; the independent reviewer should compare counts and sample rows to source records. GAO's risk-based reliability framework supports scaling that work to the decision at hand. (www.gao.gov) (www.cisa.gov)

- **Header field:** Pair the transaction trail with a field-level note.
- **Creation event:** Check the account preference before relying on creation notes.

- **Master record:** Use the type-specific trail or general System Note search.
- **Actor visibility:** Confirm that the role can see other users' changes.
- **Record key:** Preserve an internal ID alongside displayed document numbers.
- **Reperformance:** Save filters and a sampled source-record check.

Line Changes, Deletions, and System Notes v2

A line edit is not every line event

The **line-level History** link and its export answer a focused question: what was changed on an existing line. Oracle explicitly states that the line-level audit trail tracks updates to existing line items and excludes line creation and deletion. The History window can export CSV or XLS; Line System Notes fields can also filter a transaction saved search. Capture the transaction internal ID, line identity, field, old and new values, actor, and timestamp, and retain a transaction snapshot so the reviewer can locate the line later. (docs.oracle.com) (www.theiia.org)

A zero-row result is especially ambiguous when a line was added, removed, or regenerated through a business process. The pack should state which line events the selected source covers and use the transaction's other history and business documents to resolve the specific request. It should never describe the line History export as a complete list of all lines that ever existed. A source-to-report trace and a report-to-source vouch remain useful checks when the line extract is used to support a broader population claim. (www.gao.gov)

Deleted records: event log versus former content

A deletion request requires the record type and data source before selecting the search. Oracle documents a Deleted Record search for the older data source and a SuiteQL approach for records using the newer analytics data source. Before choosing the newer-source workflow, confirm that NetSuite Analytics Warehouse is enabled in the account. The old-data-source search can expose records across types to a role with Deleted Record Search permission, so the administrator should limit distribution of the export. On the newer source, Oracle says the **Date Deleted** display uses **Pacific Time**, which should be recorded before comparing it to a company-time-zone System Note. (docs.oracle.com) (docs.oracle.com) (www.canada.ca)

A deletion row can show that a record was deleted, but it is not a full reconstruction of the deleted record. Oracle says original System Notes are removed when their parent record is deleted, while **System Notes v2** persist after deletion. This difference makes record-type coverage decisive: the v2 supported-record list must be checked for the record under review, and the team should not infer that every standard transaction has a v2 reconstruction. (docs.oracle.com) (docs.oracle.com) If the auditor needs the former field values, ask what pre-deletion exports, attachments, approvals, or external records exist, and document the remaining gap without inventing a value. ISO's records guidance frames authenticity, integrity, and usability as properties to protect through the record lifecycle. (www.iso.org) (www.iso.org)

System Notes versus System Notes v2

Oracle describes **System Notes and System Notes v2 as different systems**. V2 can capture supported sublist changes and its viewer initially filters to a recent interval. That default is a display interval, not a retention promise. A search that stops at the default window may omit valid events in an older audit period even if those events still exist. Oracle also says v2 tracks significant changes only; it should not be read as a complete snapshot of every original default or every record type. (nvlpubs.nist.gov)

For each sampled object, record whether its page presents System Notes, v2, both, or another history view. Save the supported-record reference and the account's configuration state with the pack. This is a practical safeguard against using an attractive v2 screen for a record that belongs in another source. The Institute of Internal Auditors (IIA) says documentation should be relevant, reliable, and sufficient, and that another competent person should be able to repeat the steps. (www.theiia.org)

Configuration, Search, and Integration Evidence

Saved searches, reports, and workflows

A request to identify who **edited a saved search** differs from one asking who **ran or exported it**. Oracle's Analytics Audit Trail covers definition changes to saved searches, custom reports, report schedules, and financial report layouts. A saved search also has an Audit Trail subtab for changes and a separate Execution Log; Oracle describes the latter as a rolling usage history, quantified in Table 3, with no equivalent execution log for reports. The search owner should preserve the current definition, criteria, results columns, and change history before interpreting an output generated from that search. (docs.oracle.com) (technologyblog.rsmus.com)

A workflow similarly has a definition history distinct from runtime logs. Oracle documents a workflow History subtab for changes to the workflow, and notes that a System Notes search may show only a revision number. Runtime execution logs answer whether a workflow ran and can be short lived. If the audit request concerns an approval path, the pack should specify whether the claim is about a **configuration edit**, a **workflow execution**, or the **record's resulting status**. Those are three different evidentiary objects and may require three exports. (docs.oracle.com) BDO advises checking whether a report or query changed during the period in which it was used, an analogous reason to retain the relevant definition snapshot. (www.bdo.com) (technologyblog.rsmus.com)

Integration-origin changes

A changed record's System Notes **Context** helps identify whether a change came through a user interface, web services, SuiteScript, or another route, but it does not establish the full request payload or all transformations. Oracle documents script execution context in a script log and in the record's System Notes. An integration evidence request should therefore correlate the record change with the deployment or integration identity, request time, transaction ID, response status, and any external batch identifier. The integration owner should also retain the mapping version that translated the source system's fields. (docs.oracle.com) ISACA describes data traceability as understanding interfaces and transformations between systems. (www.isaca.org) (www.isaca.org)

Collection must be timely. The script and SOAP usage windows in Table 3 are short enough that a late request can miss useful runtime detail. Those are source-specific statements, not a single retention rule for every NetSuite integration log. The SOAP Usage Log does not save lengthy requests or responses, so preserve external run records when payload corroboration is needed. For asynchronous SOAP jobs, check SOAP Web Services Process Status. Use the log relevant to the integration protocol, record its documented gaps, and corroborate with the changed record and the external platform's own run ID where available. NIST's log-management guidance treats log collection and maintenance as an enterprise process, which supports scheduling capture before short-lived views disappear. (csrc.nist.gov) (csrc.nist.gov)

Login and permission evidence

Login Audit Trail can help establish when an account entered NetSuite and from what initial IP address, but a successful login is not proof that the person made a particular field change. Oracle documents filters including user, role, IP address, and date range. When a change source is ambiguous, retain the login result as corroboration and keep the System Note or execution log as the event source. (docs.oracle.com) CISA advises restricting and monitoring log access and secure storage; those controls also help protect exports that contain user identifiers or customer details. (www.cisa.gov)

- **Definition edit:** Retrieve the change history for the saved search or report.
- **Execution:** Retrieve the run log separately where the source offers one.
- **Workflow revision:** Match the revision to the period under review.
- **Script deployment:** Retain the deployment identity and execution context.
- **Interface request:** Correlate protocol log, record change, and external batch.
- **Login:** Use login history as corroboration of access, not the field event.
- **Configuration:** Preserve the mapping or workflow definition used in the test.

Building and Reviewing the Evidence Pack

Extraction sequence and control record

Begin with an agreed **population definition** and a named preparer. Capture the search criteria before running it, including date range, timezone, subsidiary, record type, status, and permissions of the extracting role. Execute the search, export the results in a usable format, and record the export time and file name. Oracle says most search results can be exported as CSV, PDF, or spreadsheet files when the role has Export Lists and Perform Search permissions. Add **Internal ID** to the results so the reviewer can reconnect rows to records after sorting. (docs.oracle.com) (docs.oracle.com) (pcaobus.org)

Next, test whether the export is complete for its purpose. Compare row counts with the NetSuite result screen, split by date or entity if a result set is too large, and document any partial export, error, or rerun. Trace a sample of source records into the export and vouch a sample of export rows back to their source records. The first direction addresses omission; the second addresses whether extracted rows accurately represent the source. BDO recommends both procedures for information produced by an entity, while PCAOB AS 1105 requires accuracy and completeness testing or evaluation of relevant controls. (pcaobus.org) (www.gao.gov)

Table 2 is a field dictionary for a reusable pack. Some fields are **pack metadata**, created by the team, rather than columns native to every NetSuite log. That distinction prevents a blank column from being misread as a missing system event. (pcaobus.org)

Field	Purpose and source	Review check
Request ID, assertion, population	Pack cover sheet records the auditor's question, entities, dates, and exclusions.	Reviewer approves the scope before extraction. (www.gao.gov)
Record type and internal ID	Native result or joined transaction record identifies the object.	Reopen a sampled ID and verify the record type.
Field, old value, new value, action	System Note, line History, configuration trail, or deletion result where offered.	Compare sample rows to the native record or history view.
Actor, role, context, integration ID	Native change result plus integration correlation and role evidence.	Distinguish a user from a script or interface account. (www.isaca.org)
Source timestamp and time basis	Native log value plus pack note on company or Pacific time.	Reconcile a sampled event after normalizing time.
Search definition, extraction time, row count	Saved search criteria and results; pack cover sheet records run and export details.	Repeat the query and reconcile count or explain a change. (www.bdo.com)
File hash, custodian, review sign-off	Pack metadata added after export, not a NetSuite System Note field.	Check the received file matches the recorded digest and handoff. (www.nist.gov)

The dictionary is intentionally broader than a single CSV. If a source lacks role, payload, old value, or a stable line identifier, mark that field **unavailable in this source** and cite the companion artifact used to answer it. Do not backfill it from memory. NIST defines chain of custody in terms of who handled evidence and when it was collected or transferred; a digest can help show that a retained file matches the reviewed version. These are pack controls, not native NetSuite guarantees. (csrc.nist.gov) (www.nist.gov)

Cover sheet, sign-off, and sensitive data

A concise cover sheet should show the request owner, extraction owner, reviewer, source screens or searches, roles used, as-of date, period and time zone, result count, file names and hashes, reconciliation method, exceptions, and date of approval. PCAOB AS 1215 expects audit documentation to make its purpose, source, and conclusion clear and to identify preparer and reviewer. The client's pack need not mimic an auditor's workpaper format, but these fields make handoff and reperformance more practical. (pcaobus.org) (pcaobus.org) (csrc.nist.gov)

Keep the **minimum data** needed for the request. A deleted-record search or integration payload can expose information outside the tested entity or period; Oracle's Deleted Record Search permission may reach records beyond a role's usual record access. Canada's Treasury Board guidance recommends sharing only the minimum personal information needed and using secure transfer and storage; the UK Information Commissioner's Office similarly advises holding no more personal data than the purpose requires. Apply the organization's own policy and engagement instructions to decide redaction and retention. (www.canada.ca) (ico.org.uk) (www.canada.ca) (ico.org.uk)

A reviewer should sign off only after checking the source selection, permission scope, filters, row counts, sampled IDs, and exception log. The IIA's standards call for review of engagement documentation by the appropriate audit personnel. A screenshot may help establish the navigation path or screen setting, but the searchable export, saved definition, and reconciliation record carry the repeatable test. (www.theiia.org) (www.theiia.org)

- **Cover sheet:** State the question, assertion, scope, and source owner.
- **Native output:** Preserve the unmodified export with stable identifiers.
- **Search definition:** Save criteria, columns, role, and extraction timestamp.
- **Population test:** Reconcile counts and record sampled traces in both directions.
- **Exception record:** Describe missing rows, ambiguous actors, and unavailable fields.
- **Reviewer sign-off:** Record the decision and the evidence reviewed.

Data Analysis and Evidence

Native sources have **different windows and output constraints**. Table 3 compares documented figures that change collection timing or completeness testing. The figures are as described in Oracle's help pages accessed in September 2026; the team should check the account and the exact feature before planning an extraction.

Source or output	Documented figure	Planning implication
System Notes v2 viewer	Default filter covers the most recent **30 days**. (docs.oracle.com)	Set the full audit period explicitly; the filter is not a retention period.
Saved-search Execution Log	Rolling **60-day** usage history. (docs.oracle.com)	Capture execution and export evidence promptly when relevant.
Script Execution Logs page	Up to **10,000** displayed results at a time and storage up to **30 days**. (docs.oracle.com)	Narrow filters and preserve the relevant interval.
SOAP Web Services Usage Log (synchronous requests only)	Request and response data may be accessible for **21 days or less** with heavy activity. (docs.oracle.com)	Correlate and retain a scoped extract before it ages out. Lengthy request and response bodies are not saved; retain other corroborating evidence for those payloads.
Persisted saved-search result	Can run up to **3 hours**; CSV remains available for **7 days**. (docs.oracle.com)	Download and archive promptly; record the job and file count.
On-demand versus background reports	Dedicated report-limit page lists **100,000** versus **1,000,000** retrieved rows. (docs.oracle.com)	Segment reports or use an appropriate search, then reconcile segments.

These are **different denominators**. A short default view does not establish v2 retention; an execution log is not the definition-change history; a report row ceiling does not automatically govern a System Note search. Oracle says saved searches do not have the same row limitations as reports, although very large result sets may be difficult to export. A reviewer should record actual result and export behavior rather than assume a

single global limit. Oracle's separate FAQ says most reports are limited to **25,000 rows**, a different figure from the dedicated report-limit page; the documents do not reconcile the scope. Confirm the actual report path in the account. (docs.oracle.com) (www.gao.gov) (www.gao.gov)

The analysis also shows why no universal **seven-year NetSuite retention rule** can be inferred from audit-documentation standards. PCAOB AS 1215 sets a seven-year audit-documentation retention period for auditors in its scope, while NIST advises organizations to retain audit records in line with their records policy. Those statements concern different holders and purposes. They do not establish how long each NetSuite event source remains visible in a given account. (pcaobus.org) (nvlpubs.nist.gov) (nvlpubs.nist.gov) (www.cisa.gov)

No public page reviewed here quantifies a universal probability that a native log is complete for every account, record type, and audit assertion. The measurable result for a particular engagement is local: defined population, extracted row count, reconciled count, sampled matches, unresolved exceptions, and reviewer decision. GAO's risk-based data-reliability approach and PCAOB's precision criterion support presenting those measured fields alongside the extract instead of a generic claim of completeness. (www.gao.gov) (pcaobus.org) (www.theiia.org)

Case Studies and Real-World Examples

Five worked requests (Hypothetical Examples)

These cases are **fictional test designs**, not findings from an actual NetSuite account. Each illustrates which evidence to request and which uncertainty to resolve before signing a cover sheet.

- **Header change (Hypothetical Example):** An auditor asks who changed a journal's department on the last close day. The controller records the journal internal ID and requested field; the administrator extracts its transaction System Notes, notes the company time zone, and saves the journal's current state. The reviewer checks the old and new values against the selected event and tests whether the requested period includes the boundary timestamp. (pcaobus.org)
- **Line edit (Hypothetical Example):** A purchase order line's quantity appears different from the approved order. The owner identifies the exact existing line and exports its History; the reviewer verifies whether the event was an edit rather than an added or removed line. The pack includes the approved order and current transaction as separate state evidence.
- **Deletion (Hypothetical Example):** A sampled vendor record cannot be opened. The administrator searches deleted records for the correct record type and data source, records the timestamp convention, and checks whether the type has System Notes v2 coverage. The reviewer reports which former values can be corroborated from retained documents and leaves unsupported values unresolved.
- **Workflow edit (Hypothetical Example):** An approval route differed during a week under test. The workflow owner exports definition History for the relevant revision and pairs it with available execution evidence and a dated definition snapshot. The reviewer separates who changed the workflow from whether a particular transaction followed it.

- **Integration-origin change (Hypothetical Example):** A customer field changed after an interface run. The integration owner correlates record System Notes context with a protocol-specific execution log and external batch ID; the reviewer inspects the mapping version and records any missing payload or aged-out log. (www.isaca.org)

The shared pattern is a **bounded claim**. Each case records what the native source establishes, what companion evidence provides context, and what remains outside coverage. That pattern accords with the IIA's repeatability criterion and the AICPA's emphasis on evidence quality, rather than assuming that more rows alone make a conclusion stronger. (www.theiia.org) (www.aicpa-cima.com) (www.aicpa-cima.com)

Implications and Future Directions

For controllers, the most useful next step is a **source register** maintained with the audit calendar: request type, source location, role required, export route, documented viewing window, owner, and capture cadence. The register should be updated when a workflow, saved search, integration, or role changes. A configuration snapshot is especially useful when the requested conclusion depends on the search definition or approval logic in effect during the period. BDO specifically advises checking whether a system-generated report or its query changed during the period. (www.coso.org) (www.aicpa-cima.com)

For internal auditors, the handoff should preserve the distinction between **native event history** and **company-produced evidence**. Even a vendor-maintained event row becomes company-produced information when management selects filters, runs the search, transforms columns, and exports a file. PCAOB AS 1105 calls for testing accuracy and completeness or relevant controls; the IIA calls for sufficient documentation that a competent person can repeat the work. This is why the saved criteria, row reconciliation, and reviewer sign-off belong next to the CSV. (pcaobus.org) (www.theiia.org) (www.theiia.org)

For administrators, the operational risk is timing and access. Some execution logs have short documented windows, while a restricted role can see only a subset of System Notes. Scheduling periodic capture for critical integrations and testing the extracting role before the audit period closes can avoid an unexplained empty result. CISA advises aligning log retention with policy and protecting logs from unauthorized access or deletion. (www.cisa.gov) (www.cisa.gov) (www.cisa.gov)

For Houseblend's NetSuite service audience, the practical work is account-specific source selection, integration correlation, and repeatable administration; its own site lists integrations and managed support as services. The client and auditor still set the assertion, materiality, and acceptance criteria. (www.houseblend.io) A future pack may automate counts, hashes, and filter capture, but any automation needs testing when searches, permissions, or record coverage change. ISACA's traceability guidance and ISO's integrity principles provide a basis for that review. (www.isaca.org) (www.iso.org)

Frequently Asked Questions (FAQs)

How do you export NetSuite System Notes for an audit?

Define the target record type, field, actor, and period; run a System Note search or a record-type search with suitable result columns; include internal IDs; export in a format the reviewer can analyze; retain filters, counts, role, and time basis. Oracle identifies System Note search as the route with advanced filters and export options, and lists Export Lists and Perform Search as required permissions. Reconcile the exported population before making an audit conclusion. (pcaobus.org)

Are System Notes and System Notes v2 interchangeable?

No. Oracle calls them different systems. V2 has its own supported-record list and can preserve notes after a supported record is deleted; original System Notes are removed with the parent record. The v2 viewer's default interval is a filter, so set the audit interval explicitly. Confirm the record's actual source in the account.

Does a deleted-record result show every former field value?

Do not assume so. Use the Deleted Record result to establish the deletion event and identifiers, then determine whether supported v2 notes or retained source documents supply the former values the auditor asked for. Record the unresolved part of the request. (pcaobus.org)

Can transaction line history prove a line was added or removed?

Oracle says the System Notes line-level audit trail tracks updates to existing lines, not creation or deletion. A line History result therefore answers an edit question; addition or removal needs other transaction or business evidence.

Who should sign the pack?

The preparer should attest to the extraction steps and source files; a reviewer independent of the extraction should sign off on scope, counts, sample checks, and exceptions. The auditor decides whether the evidence is appropriate for the engagement. PCAOB documentation guidance identifies the work's performer and reviewer, and GAO emphasizes applicability to the audit purpose. (pcaobus.org) (www.gao.gov)

Conclusion

A **NetSuite audit evidence pack** should start with the auditor's object and assertion. Transaction Audit Trail and System Notes address transaction or record changes; line History addresses edits to existing lines; Deleted Record searches address deletion events; Analytics Audit Trail, workflow History, and execution logs answer configuration and run questions. Those sources must be chosen for the actual account, record type, period, and role.

The deliverable is a repeatable chain from request to conclusion: scoped question, saved query or navigation, export with stable identifiers, source and configuration snapshots, population reconciliation, exception log, and reviewer sign-off. Short-lived logs should be captured promptly, and time zones and permissions should be

documented before interpreting a blank or borderline result. The evidence standard is not the number of screenshots or rows; it is whether the information is accurate, complete, relevant, and sufficiently detailed for the specific audit purpose. (pcaobus.org) (www.gao.gov) (pcaobus.org) (www.theiia.org)

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://www.gao.gov/products/gao-20-283g
3. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_159499608205.html
4. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N688494.html
5. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/800-171r3/NIST.SP.800-171r3.html
6. https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems
7. https://csrc.nist.gov/pubs/sp/800/92/final
8. https://www.theiia.org/en/content/podcast/getting-started-with/2025/ep-0030/
9. https://www.aicpa-cima.com/news/article/8-things-to-know-about-the-audit-evidence-standard
10. https://csrc.nist.gov/glossary/term/chain_of_custody
11. https://www.houseblend.io/
12. https://www.iso.org/news/2016/04/Ref2072.html
13. https://www.bdo.com/insights/assurance/it-audit-considerations-for-information-produced-by-the-entity-ipe
14. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/is-audit-basics-the-domains-of-data-and-information-audits
15. https://pcaobus.org/oversight/standards/auditing-standards/details/AS1215
16. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N556825.html
17. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N673560.html
18. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N555355.html
19. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N675070.html
20. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/chapter_158644279544.html
21. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N557476.html
22. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_4031815869.html
23. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_163584617278.html
24. https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html
25. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/subsect_159499523675.html
26. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N688379.html
27. https://technologyblog.rsmus.com/technologies/netsuite/system-audit-functionality-in-netsuite/
28. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_4498532139.html
29. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_157927488310.html

30. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N324233.html
31. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N663983.html
32. https://www.nist.gov/glossary-term/38726
33. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/
34. https://www.theiia.org/globalassets/site/standards/condensedglobalinternalauditstandards_2024january9_printable.pdf
35. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/chapter_N3917921.html
36. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N3444819.html
37. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/article_1029112142.html
38. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_N719691.html
39. https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/article_1210033112.html
40. https://www.coso.org/monitoring-internal-control-system

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