

Credential-Handoff Evidence Starter

A practical companion for security and SOC 2 reviews. Build a small packet that explains one credential handoff: why it was authorized, how it was handled, what was observed and what remains unverified. This is not an audit report, control certification or assessment of your organization.

Write the question before collecting the records "For the selected contractor task, can we support approval of bounded access, use of the agreed transfer procedure, and verified closure in the issuing system?" That is a reviewable question. "Can we prove credentials never leak?" is not a conclusion this packet can establish.

One packet, five evidence groups

Group	Include	Do not substitute
Scope and authorization	Case reference, relevant procedure/version, authorized recipient, task, privileges, duration and approval reference.	A familiar name or possession of a link for approval.
Selected controls	The actual context and transfer settings, with who checked them and when.	A template name for proof that controls were applied.
Observed handling	Available transfer records, their coverage, and any separate receipt acknowledgment.	A screenshot of a settings page for evidence of successful use.
Source access closure	Issuing-system change and verification, or an approved continuing-access review date.	An expired handoff for proof of a revoked token.
Review and limitations	A scoped conclusion, unresolved gaps, next owner and date.	A blank checklist, expected outcome or invented test result.

Separate the kinds of evidence

Label information as **approved design**, **directly observed**, **reported by a participant**, or **not verified**. A customer's statement that the task ended can be useful; it is not the same as the issuing system recording a token revocation.

Use existing authorized records. Keep source originals in their restricted repository and place safe references in the packet. Do not include passwords, tokens, private keys, recovery material, access-bearing URLs or unneeded personal data.

Agree scope with the reviewer

Specify the workflow, period and selection method. A convenience sample is not automatically representative. One completed case does not establish operation across an entire audit period.

AICPA's Trust Services Criteria are used to evaluate and report on controls. The responsible reviewer determines how your evidence relates to your own controls; this starter supplies no universal control-number mapping or independent assurance. [S1]

A completed fictional packet

Teaching example only. Every identifier, event and time below is illustrative. Do not submit this page as your organization's evidence.

A contractor needs read-only access to a staging service for a two-hour diagnostic. The system owner approves a temporary scoped token. The review covers that one task, not production access or all contractors.

Time (UTC)	Safe reference and completed record	Supported interpretation
09:00	AP-204: source owner approves the named contractor, staging diagnostics, read-only scope and an 11:00 end time.	The task and bounded access were authorized.
09:05	CFG-204: operator records the actual transfer profile, intended recipient and a fixed one-hour delivery window.	The stated transfer configuration was selected.
09:08	OBS-204: reviewer sees a recorded successful retrieval within the available history; recipient separately confirms receipt.	Retrieval was observed and receipt was reported within the stated scope.
10:35	DONE-204: contractor reports the diagnostic complete using only the case reference.	The participant reported task completion.
10:40	CLOSE-204: source owner revokes the temporary token; the approved verification records that the token is rejected.	The reviewed token's source access was ended. Sessions/dependencies are assessed separately where relevant.
10:45	REVIEW-204: reviewer links the five references and records the limitations below.	The evidence and interpretation are connected.

Completed reviewer conclusion

For case H-204, the referenced records support authorization of a bounded staging task, selection of the recorded transfer controls, observed retrieval, participant-reported completion and verified revocation of the temporary token in the issuing system.

This review covers one case. It did not inspect every communication channel or device, establish the absence of recipient copies, or assess organization-wide control effectiveness. Applicable session or dependent-system closure must be supported separately where required.

Why this packet is useful

It connects the approval to the actual task and separates a one-hour delivery window from a two-hour access authorization. It does not rely on link expiry to establish source closure. It also states what was not inspected rather than hiding the gap behind a label such as "secure" or "compliant."

Never fabricate the missing row. If CLOSE-204 did not exist, the conclusion would say source-access closure was not verified and assign a follow-up. The packet would still explain what is known.

Interpret the evidence without overstating it

Artifact	It can support	It does not establish by itself
Approved policy	The practice the organization defined at that version/date.	That everyone followed it during the period.
Settings capture	The options shown in a particular context at a particular time.	Enforcement on every existing or future handoff.
Access-history extract	The events actually returned within the disclosed scope and window.	Every denied attempt, every member's activity or verified business authorization.
Disposable rehearsal	The operator completed the tested exercise under those conditions.	Successful handling of all live customer cases.
Recipient acknowledgment	The participant reported receipt or task completion.	Destruction of copies or termination of source access.
Source revocation record	The issuing system recorded the stated access change.	Closure of every derivative session or dependency unless checked separately.
Reviewer note	Someone evaluated the referenced evidence and explained a conclusion.	An independent examination or certification.

A precise note for CredenShare access history

CredenShare's current documentation describes creator-scoped access history, not an organization-wide record every administrator can read. It does not record every refusal. Keep the actual query period, returned coverage and known omissions with any extract. Do not use a list of shares as though it were complete access evidence. [C2]

Use these wording repairs

Instead of "All credential transfers are audited": "For the reviewed cases, we retained the available transfer records and documented their scope and coverage limits."

Instead of "No plaintext remains": "The reviewed procedure carries values outside the ordinary ticket body. This review did not inspect every external channel or recipient device."

Instead of "The contractor's access expired with the link": "The handoff ended separately. The source owner [verified revocation / has not yet verified closure] of the underlying access."

What to do when evidence is missing

Record the gap and its effect on the conclusion. Ask the relevant owner for an existing authorized record or a bounded verification. Do not backdate an approval or recreate a past successful test that was never performed. A new rehearsal can test the current process, but it cannot manufacture last month's operating history.

If a mandatory requirement cannot be supported, flag it for the responsible reviewer and owner. Additional polished wording is not a substitute for missing controls or records.

Prepare your own packet and share it safely

A compact record you can adapt

Use the following structure in an approved internal note or evidence repository. The separate editable template supplied with this resource has the same fields.

Review question: [specific control/workflow question]
Scope: [workflow, case references, period and selection method]
Approved design: [procedure version and approval references]
Observed records: [safe references, observation times and coverage]
Participant reports: [what was reported, by whom and when]
Access closure or continuation: [source verification or approved continuation/review date]
Conclusion: [only what the records support]
Limitations: [missing records, uninspected systems and sampling limits]
Next action: [actual action, accountable owner and due date, or none agreed]
Reviewer / version / review date: [actual values]

A useful delivery message

Here is the evidence summary for [workflow and period]. It links the approved procedure, selected case records and our scoped conclusion. The limitations section identifies what was not verified. Access is restricted to the agreed reviewers; the packet contains no credential values or live reading links. Please identify any additional control question or coverage requirement before we collect more material.

Before releasing the packet

Check each reference opens for the authorized reviewer but not for an unintended recipient. Remove credentials, access-bearing URLs, unnecessary personal details and unrelated customer material from the shared copy. Have the owner approve the conclusion and store the version actually released.

Retain records according to your approved requirements, not the expiry of a sharing link or an assumed product default. Keep a safe distribution reference so later questions concern the same scope and version.

References and limitations

[S1] [AICPA & CIMA: 2017 Trust Services Criteria, revised points of focus 2022](#). Consulted for the role of control criteria, not a prescribed packet or promise of compliance.

[C2] [CredenShare: Policy and Audit](#). Product history scope checked 29 September 2026. Confirm the current documented behavior and the actual extract before using product-specific wording.

All worksheets, examples and conclusions here are instructional. The fictional packet is not evidence about CredenShare, your company or any customer. A completed packet remains scoped evidence; it does not replace an independent examination or required vendor-assurance documentation.