



INDEPENDENT EVIDENCE ASSURANCE | WORKED FICTIONAL EXAMPLE

Technology Vendor Security Evidence Review

Illustrative matter: Greystone Payroll Services LLC

Review subject: AtlasCloud Hosted Platform

THE BUYER DECISION

What does the submitted assurance actually cover, what must the customer implement and which security claims remain unsubstantiated?

ILLUSTRATIVE EVIDENCE POSITION

Request scope and bridge-period evidence before accepting “fully independently audited” as a description of all services.

DEMO REFERENCE

DEMO-06-2026-001

EVIDENCE DATE

11 OCT 2026

STATUS

ILLUSTRATIVE ONLY

Prepared for prospective US clients. No real client, counterparty or evidence packet.



Document control and limits of reliance

Aperture Research Works | Technology Vendor Security Evidence Review | Demonstration Edition, 11 October 2026.

Control	Record
Matter reference	DEMO-06-2026-001
Scenario	Wholly fictional; invented organisations, documents, persons, dates and figures
Prepared for	SaaS purchasers, financial-services vendors and small institutional buying teams
Evidence cut-off	11 October 2026 for public methodological references only; no target-specific sources retrieved
Approval status	Demonstration document. Human approval required before public release.
Professional boundary	No SOC audit opinion, penetration test, control attestation, regulator examination or security certification.

READ THIS FIRST: All MOCK exhibit labels and findings describe invented records created to show the investigation method. They are not allegations about, or findings concerning, any real person or entity.

The decision this work supports

A fictitious vendor offers a SOC 2 Type II report and security questionnaire. The report’s period does not cover a recently launched service, and a critical cloud subprocessor is outside the stated examination boundary.

Central evidence question: What does the submitted assurance actually cover, what must the customer implement and which security claims remain unsubstantiated?

Commercial moment: Before onboarding a technology vendor that will handle sensitive business information

Economic context in the fictional case: A \$96,000 annual SaaS contract handling payroll data



Executive position: what should change now?

Request scope and bridge-period evidence before accepting “fully independently audited” as a description of all services.

The scenario illustrates why a clean-looking presentation is not a complete evidence basis. The purpose is to identify source-attributed decision issues early, distinguish conflicting explanations and direct additional work only where it changes the decision.

Three practical buyer benefits

- Understand precisely what an assurance document covers.
- Spot missing service modules, vendor responsibilities and period gaps.
- Turn a glossy questionnaire into a documented procurement decision.

From a claim to decision-ready evidence

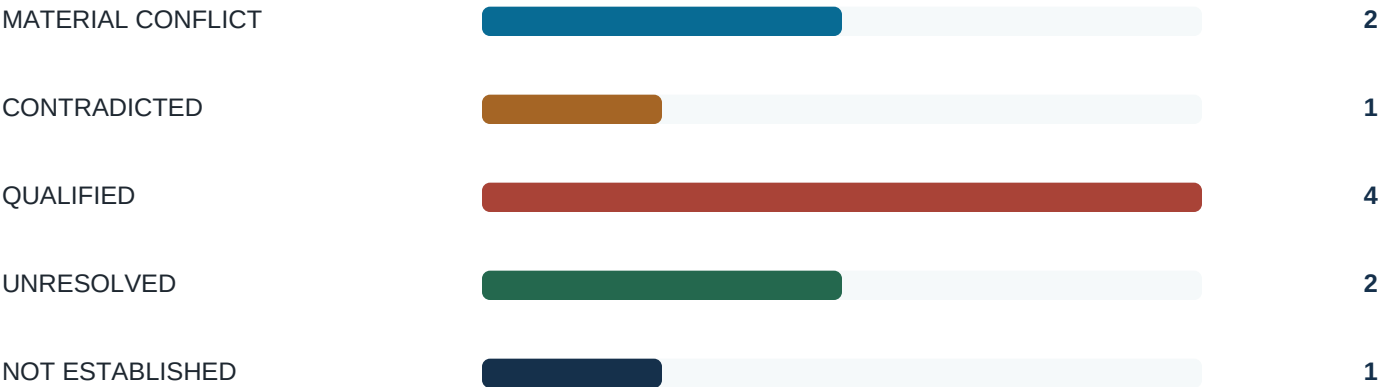


The evidence trail is part of the deliverable, not an invisible step.

Each claim is matched to an invented source object and tested for entity attribution, date, origin, contrary evidence, plausible alternatives and the specific document that would close the gap.

Finding classification used in this example

SUPPORTED means adequate evidence for the narrow stated point. QUALIFIED means partial support with a material limitation. MATERIAL CONFLICT or CONTRADICTED means the invented record contains an explicit inconsistency. UNRESOLVED and NOT ESTABLISHED are evidence insufficiency classifications, not findings of misconduct.



Claim-to-evidence matrix

All rows below are constructed data, not actual research results. Exhibit references identify simulated document objects, not attachments or verified public records.

# / claim	Illustrative record outcome	Evidence state
1. All offered services are SOC 2 audited	The evaluated system description excludes the new analytics module.	MATERIAL CONFLICT
2. The report is current	The report ends six months before the proposed go-live date.	QUALIFIED
3. No significant exceptions exist	Management response references one exception not in marketing summary.	UNRESOLVED
4. Data is encrypted everywhere	Encryption-at-rest scope omits a temporary export bucket.	QUALIFIED
5. Subprocessors inherit the same controls	A data analytics subprocessor is unlisted in service diagram.	UNRESOLVED
6. Vendor backups meet 4-hour RPO	One tabletop exercise is not equivalent to a recovery test.	NOT ESTABLISHED
7. Penetration testing covered the production stack	New module's assets are absent from the scoped asset list.	QUALIFIED



# / claim	Illustrative record outcome	Evidence state
8. Customer responsibilities are minor	Customer must configure MFA, roles and audit exports.	MATERIAL CONFLICT
9. Incident notification is within 24 hours	Notification begins after vendor determination, not awareness.	QUALIFIED
10. Hosting region cannot change	Vendor may add regions with notice.	CONTRADICTED

Material findings with original-document tests

01. All offered services are SOC 2 audited

Constructed record: MOCK-01 SOC summary. State: MATERIAL CONFLICT.

Worked observation: The evaluated system description excludes the new analytics module.

Counter-evidence test: look for independently attributable, contemporaneous records, confirm the relevant entity and effective dates, and actively search for a reasonable alternative before describing the discrepancy as adverse.

Release gate for the buyer: Obtain applicable report and module-specific evidence.

02. The report is current

Constructed record: MOCK-02 audit-period cover. State: QUALIFIED.

Worked observation: The report ends six months before the proposed go-live date.

Counter-evidence test: look for independently attributable, contemporaneous records, confirm the relevant entity and effective dates, and actively search for a reasonable alternative before describing the discrepancy as adverse.

Release gate for the buyer: Request signed bridge letter and current exception log.

03. No significant exceptions exist

Constructed record: MOCK-03 excerpt. State: UNRESOLVED.

Worked observation: Management response references one exception not in marketing summary.

Alternative explanations to test: the stated discrepancy could reflect a recording delay, a superseded document, an affiliated entity or a legitimately scoped exception. These are candidate explanations only; none is proven by this illustration.



Release gate for the buyer: Review full report and tested control statement.

04. Data is encrypted everywhere

Constructed record: MOCK-04 security questionnaire. State: QUALIFIED.

Worked observation: Encryption-at-rest scope omits a temporary export bucket.

Counter-evidence test: look for independently attributable, contemporaneous records, confirm the relevant entity and effective dates, and actively search for a reasonable alternative before describing the discrepancy as adverse.

Release gate for the buyer: Confirm system design and evidence of export safeguards.

05. Subprocessors inherit the same controls

Constructed record: MOCK-05 subprocessor appendix. State: UNRESOLVED.

Worked observation: A data analytics subprocessor is unlisted in service diagram.

Counter-evidence test: look for independently attributable, contemporaneous records, confirm the relevant entity and effective dates, and actively search for a reasonable alternative before describing the discrepancy as adverse.

Release gate for the buyer: Request complete subprocessors and dataflow inventory.

06. Vendor backups meet 4-hour RPO

Constructed record: MOCK-06 BC/DR presentation. State: NOT ESTABLISHED.

Worked observation: One tabletop exercise is not equivalent to a recovery test.

Alternative explanations to test: the stated discrepancy could reflect a recording delay, a superseded document, an affiliated entity or a legitimately scoped exception. These are candidate explanations only; none is proven by this illustration.

Release gate for the buyer: Request timed recovery evidence and exceptions.

07. Penetration testing covered the production stack

Constructed record: MOCK-07 test executive summary. State: QUALIFIED.

Worked observation: New module's assets are absent from the scoped asset list.

Counter-evidence test: look for independently attributable, contemporaneous records, confirm the relevant entity and effective dates, and actively search for a reasonable alternative before describing the discrepancy as adverse.



Release gate for the buyer: Map tested assets to current production environment.

08. Customer responsibilities are minor

Constructed record: MOCK-08 complementary user controls. State: MATERIAL CONFLICT.

Worked observation: Customer must configure MFA, roles and audit exports.

Counter-evidence test: look for independently attributable, contemporaneous records, confirm the relevant entity and effective dates, and actively search for a reasonable alternative before describing the discrepancy as adverse.

Release gate for the buyer: Assign all CUECs to named client owners.

09. Incident notification is within 24 hours

Constructed record: MOCK-09 draft MSA. State: QUALIFIED.

Worked observation: Notification begins after vendor determination, not awareness.

Alternative explanations to test: the stated discrepancy could reflect a recording delay, a superseded document, an affiliated entity or a legitimately scoped exception. These are candidate explanations only; none is proven by this illustration.

Release gate for the buyer: Have counsel negotiate trigger and evidence-preservation terms.

10. Hosting region cannot change

Constructed record: MOCK-10 data processing addendum. State: CONTRADICTED.

Worked observation: Vendor may add regions with notice.

Counter-evidence test: look for independently attributable, contemporaneous records, confirm the relevant entity and effective dates, and actively search for a reasonable alternative before describing the discrepancy as adverse.

Release gate for the buyer: Agree geographic constraints and subprocess approval.

Reproducible quantitative check

The following values are fictional and their arithmetic is shown so a client can understand the checking method. No valuation, legal loss, statutory liability or security rating is inferred.



Assurance coverage timing illustration

Audit period end: months before go-live	6
Bridging evidence months supplied	1
Illustrative unbridged months	5

Assurance timing is not a scalar security score; a bridge letter cannot extend the original auditor opinion by itself.

Re-performance control: the calculations above are to be recomputed from the underlying constructed inputs. Where the third or fourth number is a derived value, test its inclusion and whether any value is already a subset of another amount. A buyer must never add an item twice merely because it appears under two risk headings.

Alternative hypotheses and challenge log

Hypothesis	What would support it	What would undermine it
Benign documentation gap	Time-stamped correction, matching independent counterparty confirmation	Conflicting identifiers or unexplained account changes
Scope or definition mismatch	Contemporaneous definitions and consistent signed annexes	Retroactive redefinition after the discrepancy was identified
Material misstatement / control weakness	Repeated exceptions, inconsistent original records, ineffective approvals	Authenticated correction, complete reconciled trail and credible independent corroboration

No adverse conclusion is reached in this hypothetical example. A real matter requires applicable fairness, right-of-reply considerations, lawful collection methods and jurisdiction-specific professional review.

Evidence provenance and chain of reliance

For every material source record, the production team should preserve: native filename and format; collector and lawful access method; capture timestamp and time zone; document hash where possible; issuing organisation; entity and period covered; reliability grading; amendments or superseded versions; contradiction trail; and reviewer approval.



Evidence object	Why it matters	Reliance boundary
MOCK-01 SOC summary	All offered services are SOC 2 audited	Obtain applicable report and module-specific evidence.
MOCK-02 audit-period cover	The report is current	Request signed bridge letter and current exception log.
MOCK-03 excerpt	No significant exceptions exist	Review full report and tested control statement.
MOCK-04 security questionnaire	Data is encrypted everywhere	Confirm system design and evidence of export safeguards.
MOCK-05 subprocessor appendix	Subprocessors inherit the same controls	Request complete subprocessors and dataflow inventory.
MOCK-06 BC	Vendor backups meet 4-hour RPO	Request timed recovery evidence and exceptions.

What the buyer can do with the result

Stage	Decision use	Appropriate next owner
Initial screening	Do not elevate unverified representations to confirmed facts.	Buyer / internal project lead
Before irreversible payment or contract	Resolve documentary release gates and obtain written conditions.	Buyer, finance leader and counsel
Negotiation or remediation	Send a focused discrepancy schedule rather than an unstructured accusation.	Authorised counterparty contact
Specialist escalation	Separate accounting, legal, technical or regulated determinations.	Qualified professional in relevant jurisdiction
Final record	Preserve traceable limitations and a source-backed decision note.	Buyer and nominated reviewer



Priority release gates for the illustrative engagement

PRIORITY / EVIDENCE RELEASE PATH

- Obtain applicable report and module-specific evidence.
- Request signed bridge letter and current exception log.
- Review full report and tested control statement.
- Confirm system design and evidence of export safeguards.
- Request complete subprocessors and dataflow inventory.
- Request timed recovery evidence and exceptions.

Illustrative evidence-object index

X-01 | MOCK-01 SOC summary | Purpose: All offered services are SOC 2 audited. Result: The evaluated system description excludes the new analytics module. | Constructed illustration only.

X-02 | MOCK-02 audit-period cover | Purpose: The report is current. Result: The report ends six months before the proposed go-live date. | Constructed illustration only.

X-03 | MOCK-03 excerpt | Purpose: No significant exceptions exist. Result: Management response references one exception not in marketing summary. | Constructed illustration only.

X-04 | MOCK-04 security questionnaire | Purpose: Data is encrypted everywhere. Result: Encryption-at-rest scope omits a temporary export bucket. | Constructed illustration only.

X-05 | MOCK-05 subprocessor appendix | Purpose: Subprocessors inherit the same controls. Result: A data analytics subprocessor is unlisted in service diagram. | Constructed illustration only.

X-06 | MOCK-06 BC/DR presentation | Purpose: Vendor backups meet 4-hour RPO. Result: One tabletop exercise is not equivalent to a recovery test. | Constructed illustration only.

X-07 | MOCK-07 test executive summary | Purpose: Penetration testing covered the production stack. Result: New module's assets are absent from the scoped asset list. | Constructed illustration only.

X-08 | MOCK-08 complementary user controls | Purpose: Customer responsibilities are minor. Result: Customer must configure MFA, roles and audit exports. | Constructed illustration only.

X-09 | MOCK-09 draft MSA | Purpose: Incident notification is within 24 hours. Result: Notification begins after vendor determination, not awareness. | Constructed illustration only.

X-10 | MOCK-10 data processing addendum | Purpose: Hosting region cannot change. Result: Vendor may add regions with notice. | Constructed illustration only.



Methodological source register

The links below identify real public reference material used to shape the methodology. They are NOT documents obtained about the fictional organisations or verification of any mock finding.

1. AICPA, SOC 2 Reporting guidance

<https://www.aicpa-cima.com/cpe-learning/publication/soc-2-reporting-on-an-examination-of-controls-at-a-service-organization-relevant-to-security-availability-processing-integrity-confidentiality-or-privacy>

2. NIST Cybersecurity Framework 2.0

<https://www.nist.gov/cyberframework>

3. NIST SP 800-161 supply-chain security guidance

<https://csrc.nist.gov/pubs/sp/800/161/final>

Scope, professional boundaries and limitations

No SOC audit opinion, penetration test, control attestation, regulator examination or security certification.

The proposed fee is an indicative quotation hypothesis for a bounded service: \$3,500. It is not evidence of prior completed sales or a guaranteed price. Actual scope, geographic coverage, legal authority, source costs, timing, conflict checks and responsible-review resources must be approved in writing before work begins.

This report is intentionally a constructed demonstration, not a certified assessment. No claims of actual source retrieval, customer success, audit assurance, regulated investigative licensing or market-leading accuracy are made.

What to send for a scope review

Start with a short written account of the decision to be made, the legal entities involved, the date by which the decision is needed, the approximate geography and the single most material unresolved claim. Do not send confidential or personal documents in an initial public enquiry.

Aperture Research Works can assess whether a narrowly defined evidence review would be useful and lawful. Every engagement is separately accepted and scoped. The buyer retains decision responsibility.

Visit: apertureforensic.com | [Discuss a Matter](#) | info@apertureforensic.com