

COMPLIANCE WORKING RECORD

Backup restore outcome comparator

FICTIONAL evidence sample. Requires tailoring.

Document control

Field	Value
Document type	Evidence workpaper
Document reference	CASE-FICTIONAL
Jurisdiction	United States
Version	2026-10-09.assurance-resilience.1
Status	FICTIONAL sample. Requires tailoring.
Classification	Private
Prepared by	Fictional responsible reviewer
Prepared on	October 9, 2026
Sources reviewed	October 9, 2026
Generated	October 9, 2026

Document control and frozen case

Compare each customer-run restored part against an approved baseline manifest, exact count, retained hash and data-age tolerance.

Field	Value
Case reference	CASE-FICTIONAL
Organization	Fictional Example Company
Subject	Fictional customer case
Responsible reviewer	Fictional responsible reviewer
Preparation date	October 9, 2026

Field	Value
Scope	Fictional customer-approved scope. Replace all example records before real use.
Customer policy	POLICY-FICTIONAL
Customer policy version	fictional-v1
Declared approver	Fictional approver
Declared approval date	October 2, 2026
Decision boundary	No substantive decision or external filing made.

Named method and supported scope

Match frozen baseline version, restore ID and part identity. Compare absolute record-count differences, exact SHA-256 and recovered-data age with one approved tolerance. Missing or duplicated whole parts remain unresolved.

No live restore, recovery execution or independent functional validation. Hash identity only covers supplied bytes and annotations. Up to 100 rows per table, 20 originals and 25,000,000 combined original bytes.

Original contents, annotations, approvals, reported events and applicability remain customer declarations. File hashes establish retained byte identity only.

No SOC assurance, live restore, actual failover, legal service, legal classification, contract negotiation, transaction approval or external communication occurs.

All accepted records remain complete. Recovery preserves original bytes and frozen results without creating fresh payment, source authentication, consent or approval authority.

Complete result counts

Measure	Value
Manifest parts	1
Parts outside approved tolerance	0
Unresolved parts	0

1. Original evidence source (S1)

State. Customer verification linked

Customer-declared original identity and verification only. Content is not extracted or independently authenticated.

Field	Value
id	S1
fileId	F1
locator	Fictional section one
sourceDate	October 1, 2026
custodian	Fictional customer custodian
description	Fictional source declaration. Does not establish actual evidence.
verification	Customer verified
verifiedBy	Fictional reviewer
verifiedOn	October 2, 2026
Exact evidence source references	S1

2. Original byte manifest (F1)

State. Indexed

Complete export requires these exact original bytes.

Field	Value
id	F1
name	FICTIONAL-assurance-resilience-evidence.txt
mimeType	text/plain
bytes	197
sha256	06569f98e8a6ebac8b1f9470fd3bdbefd8d3c577e4bc765ee106601022f85c71
Exact evidence source references	S1

3. Frozen customer policy (POLICY-FICTIONAL)

State. Documented

Exact approved customer scope. No automatic legal applicability.

Field	Value
reference	POLICY-FICTIONAL
version	fictional-v1
approvedBy	Fictional approver
approvedOn	October 2, 2026
sourceIds	["S1"]
Exact evidence source references	S1

4. Restore manifest part comparison (PART1)

State. Within approved tolerance

Only customer-run restore observations are compared. No live restore or recovery validation is performed.

[illegible]

Field	Value
Baseline hash matches	Yes
Gaps	
Exact evidence source references	S1

Complete accepted task inputs

The following exact accepted fields preserve every supplied task record, including orphan records and contradictions. They are customer annotations, not independently extracted or authenticated evidence.

Field	Value
baselineVersion	fictional-v1
restoreReference	RESTORE1
baselines 1. reference	PART1
baselines 1. sourceIds	S1
baselines 1. part	Fictional records
baselines 1. version	fictional-v1
baselines 1. recordCount	1000
baselines 1. sha256	1111111111111111111111111111111111111111111111111111111111111111 11111111111111111111
baselines 1. dataAt	2026-10-01T08:00:00.000Z
observations 1. reference	OBS1
observations 1. sourceIds	S1
observations 1. restoreReference	RESTORE1
observations 1. baselineReference	PART1
observations 1. baselineVersion	fictional-v1
observations 1. part	Fictional records
observations 1. recordCount	998

Field	Value
observations 1. sha256	1111111111111111111111111111111111111111111111111111111111111111 11111111111111111111
observations 1. dataAt	2026-10-01T08:00:00.000Z
observations 1. restoredAt	2026-10-01T10:00:00.000Z
tolerances 1. reference	TOL1
tolerances 1. sourceIds	S1
tolerances 1. baselineReference	PART1
tolerances 1. baselineVersion	fictional-v1
tolerances 1. maximumCountDifference	2
tolerances 1. maximumAgeMinutes	120
tolerances 1. hashRequired	Yes
tolerances 1. approvedBy	Fictional approver
tolerances 1. approvedOn	October 2, 2026

Recovery and original attachment boundary

The complete local ZIP includes every original file listed in the retained manifest. A structured JSON or cloud record alone preserves the descriptor and annotation, not the original file bytes. Attach matching bytes before producing a complete original-attachment pack.

Customer recovery restores neither source authentication, approval authority nor paid export access. Payment ownership is checked before each commercial export.

Official sources

Source	Provision	Date	Link
National Institute of Standards and Technology: Contingency Planning Guide for Federal Information Systems. SP 800-34 Revision 1	Sections 3.2 and 3.5.1 and Appendix B support impact analysis, distinct RTO/RPO/maximum disruption, testing, after-action findings and corrective actions. Federal guidance is a voluntary method reference for private customers. No current control baseline or legal obligation is inferred.	October 9, 2026	https://csrc.nist.gov/pubs/sp/800/34/r1/updates/final