CHECKLIST

Security and Compliance Evidence Collection Checklist

What separates a policy from proof that a control operated, the quality tests that decide whether evidence is accepted, and a checklist of acceptable evidence and common rejection reasons for twelve control areas.

WHO IT IS FOR

The person assembling evidence for an audit, a certification, a customer security review or an insurance application — often for the first time, and often for more than one of them at once.

LAST REVIEWED

14 September 2026

READING TIME

15 minutes

ON THIS PAGE

An auditor, a certification body, an underwriter and a customer's security team are all asking versions of the same question: show me that this control operated, on the systems in scope, over the period that matters. A policy cannot answer that. It says what should happen. Evidence shows what did.

Most evidence problems are not missing controls. The control works; the proof is undated, unattributed, taken from the wrong system, or a year old. This checklist sets out the evidence types that usually work, the quality tests every item has to pass and — for twelve control areas that recur across frameworks and questionnaires — examples of acceptable evidence and the reasons evidence is commonly sent back.

The freshness guidance describes common practice, not a requirement of any standard. The framework you are working to, your auditor, your contracts and your own policies decide what applies to you.

PART 1 OF 7

A policy is not proof

A policy, standard or procedure is evidence of design. It shows the organisation decided what should happen, and an assessor will usually want to see it. On its own it proves nothing about whether the control operated.

Operating evidence shows the control happening: the access review with its reviewer, date and outcomes; the restore test with its result; the ticket showing a leaver's account was disabled on their last day. Most assessments need both. A period-of-time assessment, such as a SOC 2 Type 2 examination, needs operating evidence from across the whole period rather than a single good day.

A useful test for any item: if the person who produced it left tomorrow, could someone else show from this item alone what was checked, on which system,

when, by whom, and what the result was? If not, it is probably an assertion with a file attached.

PART 2 OF 7

Evidence types, and what each is good for

COMMON EVIDENCE TYPES

TYPE	WHAT IT IS	GOOD FOR	WATCH FOR
Configuration export or screenshot	A setting captured from the system that enforces it.	Showing a technical control is configured: MFA policies, password settings, encryption, firewall rules.	It must show the system or tenant name and the date. Crops that hide exclusions or scope are commonly rejected. It shows one point in time only.
System-generated report	A report produced by the tool itself, such as patch compliance, endpoint coverage, training completion or backup job history.	Showing coverage and operation across a whole population, often over time.	Keep the report parameters — date range, filters, scope — with the output. A report filtered to show only compliant devices proves very little.
Ticket or change record	A record in a service desk, change or HR system showing something was requested, approved and completed.	Joiners, movers and leavers, change approvals, incident handling, vulnerability remediation.	Timestamps and the approver's identity must be visible. Tickets closed with no record of what was done are weak.
Sign-off record	A recorded approval or review by a named person with the authority to give it.	Showing a decision or review happened and who was accountable: an approved policy, a risk acceptance, a completed access review.	A name typed at the bottom of an unsigned document is not a sign-off. Keep the approval trail, not just the final file.
Sampled records	A selection from a larger population, such as a sample of leavers checked against account disablement dates.	Testing whether a recurring control operated consistently over a period.	Keep the full population list so the sample can be seen to be fair. Choosing only the cases that went well defeats the purpose.

TYPE	WHAT IT IS	GOOD FOR	WATCH FOR
Log extract	Entries from system or audit logs showing that events happened.	Administrative activity, enforcement at sign-in, alert handling, retention.	Include the query, the time range and the source. Raw logs with no explanation are hard to assess, and may contain personal data that should be minimised.

PART 3 OF 7

Quality tests every item should pass

01

Dated

WHY IT MATTERS

An assessor needs to place the evidence inside the period being assessed. The date should come from the system where possible, not from a filename someone typed later.

WHERE IT USUALLY FALLS SHORT

Screenshots with no visible date, or a date added to the filename weeks after capture.

02

Attributable to a system and a person

WHY IT MATTERS

The item should show which system, tenant or environment it came from, and who produced or approved it. Evidence that could have come from any environment, including a test one, is weak.

WHERE IT USUALLY FALLS SHORT

A setting captured from an administrator’s browser with the tenant name cropped out.

03

Complete population, or a clearly drawn sample

WHY IT MATTERS

Say whether the item covers everything in scope or a sample, and if a sample, how it was chosen and from what list. A report covering one office when the scope is three is incomplete, however clean it looks.

WHERE IT USUALLY FALLS SHORT

Coverage reports filtered to one device group, with unmanaged devices outside the view.

04

Retained

WHY IT MATTERS

Evidence must still exist when someone asks, including for the whole of an audit period that may end long after the event. Decide where it lives and how long it is kept before you need it.

WHERE IT USUALLY FALLS SHORT

Evidence held in a personal mailbox or a departed employee’s drive, or in a tool that overwrites its history after a short period.

05

Reviewed

WHY IT MATTERS

Someone other than the person who produced the item should confirm it shows what it claims, for the control it is attached to. Review catches the wrong system, the wrong period and the missing exclusion list.

WHERE IT USUALLY FALLS SHORT

Items uploaded in bulk the week before an audit and attached to controls by guesswork.

06

Fresh enough for the question being asked

WHY IT MATTERS

Every item has a useful life. Set an expiry or review date when you file it, based on how often the control operates and what the person asking needs, so stale evidence is visible to you before anyone else notices it.

WHERE IT USUALLY FALLS SHORT

A penetration test or access review from a previous year still being sent with current questionnaires.

PART 4 OF 7

Checklist by control area

For each area: why the evidence matters, examples of evidence that is usually acceptable, and the reasons evidence is commonly rejected. The examples are illustrative; the right evidence depends on your systems and on exactly what the assessor has asked for.

01

Access reviews

WHY IT MATTERS

Shows that someone with the right knowledge periodically checks who can reach important systems and removes what is no longer needed. Access accumulates quietly; reviews are the control that reverses it.

EVIDENCE THAT HOLDS UP

- The account and permission list that was reviewed, exported from the system and dated.
- The reviewer’s decision for each account — keep, change or remove — with their name and sign-off date.
- Tickets or change records showing the removals and changes were carried out.

WHERE IT USUALLY FALLS SHORT

Rejected when the review is an email saying “looks fine” with no account list, when reviewers approved their own access, or when removals were decided but never actioned.

02

Joiners, movers and leavers

WHY IT MATTERS

Shows access is granted when approved, changed when roles change, and removed promptly when people leave. Leavers are tested most, because an active account for someone who has gone is an obvious risk.

EVIDENCE THAT HOLDS UP

- The period’s leavers from the HR system, matched against account disablement dates in the identity platform.
- Joiner tickets showing a manager approved access before it was granted.
- Mover tickets showing old access removed, not only new access added.

WHERE IT USUALLY FALLS SHORT

Rejected when the HR list and the account list cannot be reconciled, when accounts were disabled well after the leaving date without explanation, or when contractors sit outside the process.

03

Multi-factor authentication

WHY IT MATTERS

Shows that signing in to important systems takes more than a password, and where exceptions exist and why. Reach is the question: email, remote access, administrative accounts, cloud consoles and backup systems.

EVIDENCE THAT HOLDS UP

- A dated export of the MFA or conditional access policy, showing the users and applications in scope.
- The exclusion list, with a reason and compensating restriction for each account.
- A sign-in report showing MFA required in practice, and configuration blocking legacy authentication.

WHERE IT USUALLY FALLS SHORT

Rejected when the policy is in report-only mode, when exclusions are cropped out, or when the evidence covers email but the request also asked about remote access or administrators.

04

Backups and restore tests

WHY IT MATTERS

Shows data can be recovered, not only that copies are taken. A job success report proves the backup ran; a restore test proves recovery works.

EVIDENCE THAT HOLDS UP

- Backup job history for the period, with failures and how they were resolved.
- A restore test record: date, system restored, backup used, result, time taken and who performed it.
- Configuration or a provider statement describing the immutable or offline copy and how it is separated.

WHERE IT USUALLY FALLS SHORT

Rejected when there is no restore test at all, when the test restored a single file rather than a system that matters, or when failed jobs appear with no record of follow-up.

05

Vulnerability and patch management

WHY IT MATTERS

Shows known weaknesses are found and fixed within the timeframes your own policy sets, and that exceptions are tracked rather than forgotten.

EVIDENCE THAT HOLDS UP

- Dated vulnerability scan reports for internal and internet-facing systems in scope.
- Patch compliance reports showing coverage and outliers, and remediation tickets for critical findings with dates found and fixed.
- An exceptions register for end-of-life or unpatchable systems, with approver, compensating control and review date.

WHERE IT USUALLY FALLS SHORT

Rejected when scans leave out servers or network devices, when critical findings stay open beyond policy with no exception recorded, or when scanning is shown but remediation is not.

06

Endpoint protection

WHY IT MATTERS

Shows devices and servers run protection, that coverage is known against the inventory, and that alerts are dealt with.

EVIDENCE THAT HOLDS UP

- A coverage report from the endpoint console, reconciled against the asset inventory.
- The devices without protection, and the reason for each.
- A sample of alerts showing investigation and closure, with dates.

WHERE IT USUALLY FALLS SHORT

Rejected when the console and inventory disagree without explanation, when servers are missing, or when alerts are shown with nothing to show anyone acted on them.

07

Logging and monitoring

WHY IT MATTERS

Shows security-relevant events are recorded, kept long enough to investigate, and reviewed by someone.

EVIDENCE THAT HOLDS UP

- The log sources sent to central collection, and the important systems that are not included.
- Retention settings shown in configuration.
- Review records for the period — alert tickets, review sign-offs or a monitoring provider's reports — with one investigation followed from alert to closure.

WHERE IT USUALLY FALLS SHORT

Rejected when logging is enabled but nothing shows review, when retention is shorter than the policy states, or when the evidence is a vendor's service description rather than your own configuration.

08

Incident response plan and exercises

WHY IT MATTERS

Shows there is a current plan, and that the people named in it have rehearsed it and turned lessons into actions.

EVIDENCE THAT HOLDS UP

- The plan, with version, approval date and owner.
- An exercise record: date, scenario, participants, observations and agreed actions.
- Evidence the exercise actions were completed, and post-incident reviews for any real incidents.

WHERE IT USUALLY FALLS SHORT

Rejected when the plan has no approval or is clearly out of date, when the exercise record has no participants or outcomes, or when actions from the last exercise are still open with no owner.

09

Vendor and third-party reviews

WHY IT MATTERS

Shows suppliers with access to systems or data are known, assessed in proportion to their risk, and reviewed again over time.

EVIDENCE THAT HOLDS UP

- A supplier register showing criticality, the access or data involved, and review dates.
- For critical suppliers, the review record: questionnaire responses, independent assurance reports with scope and period checked, and the reviewer's conclusion.
- Contract extracts covering security and incident notification terms.

WHERE IT USUALLY FALLS SHORT

Rejected when an assurance report on file has expired or covers a different service from the one you use, when there is no reviewer conclusion, or when suppliers with remote access are missing from the register.

10

Security awareness

WHY IT MATTERS

Shows staff receive training, that completion is tracked by person, and that the organisation checks whether it is working.

EVIDENCE THAT HOLDS UP

- Completion records by person and date from the training platform, reconciled against the HR list.
- Phishing simulation results with dates, scope and follow-up.
- Evidence that new starters complete training within the period your policy sets.

WHERE IT USUALLY FALLS SHORT

Rejected when completion is shown only as a percentage with no underlying list, when the HR and training populations do not match, or when the records predate the current cycle.

11

Change management

WHY IT MATTERS

Shows changes to important systems are requested, assessed, approved and tested before going live, and that emergency changes are reviewed afterwards.

EVIDENCE THAT HOLDS UP

- The period’s list of changes from the change or ticketing system.
- Sampled change records showing request, approval by someone other than the implementer, testing and completion.
- Emergency changes with retrospective approval, and for software, pull request records showing review before deployment.

WHERE IT USUALLY FALLS SHORT

Rejected when implementers approved their own changes, when approvals were recorded after go-live without the change being marked as an emergency, or when changes made directly in production appear nowhere.

12

Business continuity

WHY IT MATTERS

Shows the organisation has worked out which activities matter most and how long it can manage without them, and has tested its arrangements.

EVIDENCE THAT HOLDS UP

- The continuity plan, with approval date and owner, covering the activities identified as critical.
- A business impact analysis or equivalent record of priorities and tolerable downtime.
- A test or exercise record with date, scope, result and actions.

WHERE IT USUALLY FALLS SHORT

Rejected when the plan has never been tested, when the test left out the systems identified as critical, or when recovery targets in the plan contradict what restore tests actually achieved.

PART 5 OF 7

How fresh evidence usually needs to be

These windows describe common practice across audits, certifications and questionnaires. They are not requirements of any standard. Your framework, your auditor, a customer contract or your own policy may set a different period, and where one does, that period applies.

TYPICAL FRESHNESS WINDOWS — COMMON PRACTICE, NOT A REQUIREMENT OF ANY STANDARD

CONTROL AREA	COMMONLY TREATED AS CURRENT	WHAT TENDS TO SHORTEN IT
Access reviews	Within the review cycle your policy sets, often quarterly or six-monthly.	Privileged access, systems holding sensitive data, a recent reorganisation.

CONTROL AREA	COMMONLY TREATED AS CURRENT	WHAT TENDS TO SHORTEN IT
Joiners, movers and leavers	Records from across the whole assessment period, not a single point.	A period-of-time audit that samples throughout the period.
Multi-factor authentication	A configuration captured shortly before it is submitted — weeks rather than months.	Any change to identity policies since the capture.
Backups and restore tests	Job history for the period, and a restore test within the last year as a common minimum; many organisations test more often.	An insurance application, or a significant change to the backup design.
Vulnerability and patch management	Scan and patch reports from roughly the last month.	Internet-facing systems, and newly published critical vulnerabilities.
Endpoint protection	A coverage report from roughly the last month.	Device refreshes, acquisitions, or a move to a new tool.
Logging and monitoring	Recently captured configuration, with review records across the period.	A change of log sources or monitoring provider.
Incident response exercises	An exercise within the last year.	Major changes to the people, systems or providers named in the plan.
Vendor reviews	Critical suppliers reviewed within the last year, with assurance reports covering a recent period.	A supplier incident, a change of service, or an expired report.
Security awareness	Completion within the current training cycle, often annual.	New starters, and roles targeted by payment fraud.
Change management	Records from across the whole assessment period.	A period-of-time audit.
Business continuity	A plan reviewed and tested within the last year.	Changes to critical activities, sites or suppliers.

PART 6 OF 7

Naming, storing and versioning evidence

- Use one naming pattern everywhere: capture date, control area, system, evidence type and version — for example, “2026-09-01 MFA policy export, identity platform, v1”. Anyone should be able to tell what an item is without opening it.

- Use the date of capture, not the date of upload. Where the system shows a date inside the item, the two should agree.
- Keep evidence in one controlled location with access limited to those who need it — not in personal drives, mailboxes or chat threads.
- Link each item to the control or requirement it supports, and record an owner and an expiry or review date when you file it.
- Never overwrite. When evidence is refreshed, file the new version and keep the old one, because an assessment of an earlier period still needs the item that covered it.
- Keep context with the item: the report parameters, the query behind a log extract, or the population a sample was drawn from.
- Minimise personal data. Redact what is not needed to show the control operated, and agree retention with whoever handles privacy in your organisation.
- Record what was sent to whom, and when. If a customer, auditor or insurer received an item, you will want to know which version they have.

PART 7 OF 7

Reusing evidence across frameworks without claiming equivalence

Frameworks and questionnaires overlap heavily. One restore test record can support a backup control in an ISO/IEC 27001 programme, an availability-related criterion in a SOC 2 examination, a data recovery safeguard in the CIS Controls, a recovery outcome under NIST CSF, and the backup question on an insurance application. Collecting it once and linking it to each is sensible, and it stops five copies of the same document drifting apart.

Reuse the evidence, not the conclusion. Each framework asks a slightly different question, sets its own scope, and may expect a different period or depth. A restore test of one system may satisfy a questionnaire and still fall short of what an auditor expects across the full scope. Before attaching an item to a second framework, check three things: it covers the systems in that

framework's scope, it falls within that assessment's period, and it answers what that requirement actually asks.

Avoid saying that a result under one framework stands in for another. Readiness for, or certification against, one framework does not mean another is met, and mappings between frameworks are aids to organising work rather than formal equivalences. Where a customer or insurer chooses to accept one as evidence for another, that is their decision to make.

CYBERWAVE SENTINEL

Where Sentinel fits

Sentinel's evidence library, included from the Essentials plan, holds each item against the control it supports, with an owner, an expiry date and one of seven statuses — Accepted, Approved, Under Review, Pending, Draft, Expired or Missing — and one item can be linked to requirements in more than one framework. Items past their date show as expired in the library.

Evidence is attached by the people who own each control. When you upload a document, Sentinel extracts its text, sorts it by document type and notes which common frameworks it names, but it does not pull evidence from your systems, and someone on your side decides whether an item is accepted.

See how the evidence library works →

Limitations

WHAT THIS CHECKLIST IS NOT

This checklist is general guidance on organising security and compliance evidence. Examples of acceptable evidence and freshness windows describe common practice; they are not requirements of any standard, and they do not predict what a particular auditor, certification body, customer or insurer will accept.

CyberWave does not certify compliance, issue audit opinions or verify your evidence, and does not replace independent auditors, certification bodies or legal counsel. Framework references here are informational. Nothing in this checklist is legal advice, including on retention periods or on handling personal data within evidence.

Related

How the evidence library works →

SOC 2 readiness →

ISO/IEC 27001:2022 readiness →

Governance and compliance →

All checklists and templates →