

Build an evidence pack that can be inspected.

Organise technical evidence against agreed requirements without treating a checklist as a certification.

Assurance evidence index

Requirement area	Evidence example
Identity and access	Role definitions, access reviews and revocation checks
Change control	Reviewed source, release records and verification results
Data handling	Data flows, retention implementation and deletion checks
Recovery	Restore exercises and verified business workflows

State the scope of the evidence

Record the system version, environment and time period examined. A successful test in one environment does not automatically demonstrate the same control elsewhere.

Keep claims proportionate

Distinguish implemented controls, tested behaviour and formally assessed compliance. Do not use the presence of a document as proof that a control operates.

Connect a requirement to observable evidence

Begin with the specific requirement and its source. It may come from an internal policy, a contract, a procurement process or an applicable external obligation. Record who interprets the requirement and which systems or workflows are in scope. Avoid treating a generic checklist as proof that every relevant obligation has been identified.

Map the requirement to a control and then to evidence that the control works. For a release-approval requirement, useful evidence might connect a change, reviewer, test result and deployment. For access management, evidence may include an approved role change and a check that the resulting permissions match it. The mapping should be understandable to the person reviewing the assurance claim.

Explain what the evidence does and does not prove

Record the environment, version, date and method behind a result. A test performed against a demonstration environment may establish part of a control but not its production configuration. A screenshot can show a setting at one moment without proving that it remained in effect or that access to change it is controlled.

Keep the original evidence where authorised reviewers can inspect it. Summaries should link back to that record and identify exceptions. Distinguish evidence of design from evidence of operation. A documented backup procedure and a successful restoration exercise answer different questions. Combining them provides a clearer account than presenting either as complete assurance on its own.

Maintain an honest assurance statement

State the scope examined, the findings and any unresolved conditions. Assign owners to gaps and record how corrective work will be verified. If a finding is accepted temporarily, preserve the reasoning and review date. Do not let a limitation disappear when the document is reformatted for another audience.

Review the evidence after meaningful changes to the system or its operating model. Keep superseded records for the agreed retention period while making the current status clear. Formal certification or legal compliance claims require the relevant assessment and authority. Cobnex resource material can support preparation and engineering discussions, but downloading or completing it does not itself certify a business or system.

Does this page claim a Cobnex certification?

No. It describes how technical evidence can be organised. Any certification or contractual compliance requirement must be verified separately.

Read the current resource online

<https://cobnex-review.rgcsekaraa.workers.dev/trust-hub/compliance-resources/>