Control Evidence Review Worksheet

Organise a bounded control review around its criterion, evidence, limitations and follow-up.

How to use these four pages

1. State one criterion, its applicability and the question to answer.

2. Define the service, period, population, selection and approved methods.

3. Record observations separately from explanations and missing evidence.

4. Agree the supported conclusion, limitations, response and next action.

A practical working aid

Use the blank records for your own discussion. Examples are fictional, not client case studies. Print to complete by hand or adapt the prompts in your own document; this PDF is not a fillable form.

Keep completed records confidential. Use references to protected evidence rather than passwords, customer records or sensitive system details.

Online instructions and companion article

Read the guide

Read the article

Source guidance

NIST SP 800-53A Rev. 5: Assessing Security and Privacy Controls

Public guidance checked 16 November 2026. The source material informs the approach; no endorsement is implied. This worksheet supports planning and record-keeping. It does not authorise testing, certify compliance or replace an agreed specialist review.

Free to use and adapt within your business with the GRCPreneur acknowledgement retained.

A fictional worked example

Illustrative entries only. No real client, vendor result or completed implementation is claimed.

Record	Illustrative entry
Question	Do selected access changes have the approval evidence required by the procedure?
Boundary	One application and an agreed period; selection method recorded separately.
Observation	A selected completion ticket lacks approval evidence in the material provided.
Explanation	Administrator states that approval was given by telephone.
Current limit	The statement has not established the missing approval evidence.
Next action	Responsible owner provides further evidence; reviewer assesses the result.

Before using the blank pages

Agree who will review the record and what decision it supports. Mark assumptions, proposed actions and unverified claims clearly. Copy pages 3 and 4 when you need more space.

Your working record

Project / record ID: _____ Date: _____

Criterion and review question

Requirement reference, version, applicability and management decision.

Boundary and selection

Service, period, population, selection reason and completeness limitations.

Methods, owners and permissions

Approved review activities, evidence owners and handling arrangements.

Observations and evidence

What was examined? Separate records, explanations, gaps and assumptions.

Conclusion, limits and response

What is supported? What remains unresolved? Who owns the next decision?

Use protected evidence references. Do not enter credentials or confidential customer details.

Evidence and follow-up record

Related record / requirement: _____ Review date: _____

Criterion / observation	Evidence reference / limit	Owner / due date	Response / next check

Review before the next decision

- The criterion, service and review period are clear.
- The selection and evidence-completeness limits are recorded.
- Observed evidence is distinguished from explanations and assumptions.
- The conclusion, response and next action match the review scope.

Decision, authority and next checkpoint

Proceed / revise / defer / stop. State the decision scope, conditions, approver and date.

A completed record documents a review. Approval applies only to the stated scope and does not establish that untested work has succeeded.