

A risk and control matrix

Sample requirements for an invented organisation. Each risk is linked to a control, supporting evidence and a test approach.

Fictional work sample. Created for this portfolio; no client deliverables or completed tests are reproduced.

Area	Risk	Sample control	Evidence	Test approach
Leaver access	Accounts remain usable after departure.	Remove access by the end of the departure date.	HR effective date; account disable event; exceptions register.	Compare the complete leaver population with account status and disable dates.
Privileged access	Elevated permissions are retained without a current need.	Approve privileged access and review it periodically.	Approval; role membership; review record; removal evidence.	Check a sample against approvals and evidence of review.
Repository changes	Code changes bypass an agreed review.	Require authorised review before protected changes are merged.	Repository rules; change sample; reviewer and merge records.	Compare configuration with evidence from actual changes.

Read the requirement first

The deadline in this matrix is a fictional policy assumption. A real engagement would establish its applicable requirements, scope, full population and sampling approach.

A configured control and evidence that it operated are different things. Testing should support the actual conclusion being made.

A documented access finding

Fictional finding AC-01. This example assumes that the invented HR, directory and event records have been validated.

Fictional work sample. Created for this portfolio; no client deliverables or completed tests are reproduced.

Finding element	Illustrative content
Requirement	The sample policy requires access to be revoked by the end of the departure date.
Condition	DEMO-A and DEMO-C remain enabled after departure. DEMO-E was disabled eight days after departure.
Evidence	Invented HR list, directory snapshot and disable-event records, reviewed as at 2 October 2026.
Risk	Former staff may retain access beyond the intended period. DEMO-C has privileged access, increasing the potential impact. This does not establish misuse.
Cause	Not yet established. Review departure notification, access-removal workflow and ownership before concluding on cause.
Proposed action	Confirm current access and follow the agreed removal/escalation process. Reconcile the full leaver population, investigate delays and verify closure with evidence.
Owner / due date	To be agreed with the responsible owner. No management acceptance or closure is claimed.

Candidate exceptions need investigation. The walkthrough explains the questions that come before this fictional finding.

An automation review output

A reconstructed illustration of PII screening. Filenames are invented; values are masked and no personal data is included.

Fictional work sample. Created for this portfolio; no client deliverables or completed tests are reproduced.

File	Candidate match	Reviewer disposition	Reason / next action
sample-log.txt	Masked email pattern	Needs context review	Confirm purpose, access and retention before deciding whether the presence is inappropriate.
sample-report.pdf	Identifier-like number	False positive in this example	The invented value is a report reference, not a personal identifier.
sample-export.xlsx	Masked contact pattern	Confirmed presence in this example	Presence alone is not a policy breach. Review necessity, access and handling requirements.

What this output can and cannot tell us

Pattern screening helps identify records to review. It can miss data and produce false positives. A candidate match needs context before it becomes a confirmed observation.

This newly created sample is not the original scanner output. It reports no accuracy, coverage or performance benchmark.

The project case study describes the actual Python screening initiative from my resume.

An AI use-case review

Fictional use case: an internal knowledge assistant retrieving answers from approved policy documents. These are proposed review questions, with no completed testing or deployment claimed.

Fictional work sample. Created for this portfolio; no client deliverables or completed tests are reproduced.

Review area	Question / evidence request
Data and purpose	Map documents, prompts, provider, retention and output audience. Establish whether personal or confidential data can enter the system.
Access	Check that retrieval respects the user’s permissions. Request evidence of denied access as well as successful access.
Prompt injection	Treat retrieved content as untrusted. Propose tests with instructions embedded in documents; check behaviour and restricted-information exposure.
Accuracy and oversight	Define representative questions, expected sources, uncertainty handling and decisions that need human review.
Action permissions	Identify integrations that can change records or act. Establish limits and approval requirements.
Change and monitoring	Identify owner, change process, evaluation evidence and response to reported failures. Revisit the review when the use case changes.

References

NIST AI Risk Management Framework
OWASP LLM01:2025 Prompt Injection

This sample does not assert conformity to a standard. A test plan is not evidence that a control passed.