

AI Sovereignty Evidence Checklist

Define the system boundary and required period of independent operation before reviewing controls. Use synthetic data and an isolated environment for failure, revocation, and restoration exercises. Record observed results against the agreed requirement. Untested claims remain Unverified. Status options: Unverified, Demonstrated, Gap, Accepted dependency, or Not applicable (with rationale). An accepted dependency needs a named approver and review date. Results apply to the recorded version, scope, and test period.

System / version: _____ Reviewer / date: _____

Boundary / approved external services: _____ Required offline period: _____

01 Data location

Where are documents, prompts, embeddings, and backups?

Include extracted text, temporary files, conversation history, replicas, support bundles, retention, and deletion.

Evidence to request Data-flow map; storage inventory; replication and backup settings; retention rules; relevant service commitments.

How would you verify this? Trace a synthetic document through ingestion, retrieval, logs, and backup. Compare actual destinations and retention settings with the approved geographic boundary. Record each copy and any unexplained destination.

Suggested roles Data owner + storage or platform lead

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date

02 Inference

Where does processing happen, including fallback requests?

Include parsing or OCR, embedding, reranking, generation, overload routing, retries, and fallback providers.

Evidence to request Endpoint inventory; routing and fallback configuration; request traces; DNS, proxy, or firewall records.

How would you verify this? Observe representative requests and outbound connections. Make local inference unavailable in a test environment. Confirm whether requests stop, queue, or use an approved fallback; identify the processor and location for every stage.

Suggested roles AI application owner + network lead

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date

AI Sovereignty Evidence Checklist

Continue the same review. Record evidence, observed results, gaps, and accountable owners. Status: Unverified / Demonstrated / Gap / Accepted dependency / Not applicable (explain).

System / version: _____ Reviewer / date: _____

Boundary / approved external services: _____ Required offline period: _____

03 Administrative access

Who can access the system, and who approves it?

Include supplier support, subcontractors, service accounts, infrastructure privileges, operator locations, and emergency access.

Evidence to request Privileged-role export; support-access terms; approval records; access logs; emergency-access procedure.

How would you verify this? Match a recent privileged session to its approver, identity, location, and actions. Test time-limited support access in a sandbox. Confirm it expires, cannot be reused, and leaves an audit record.

Suggested roles Identity and access lead + service owner

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date

04 Logs and telemetry

What leaves the environment?

Include prompts, retrieved passages, filenames, user identifiers, traces, crash reports, monitoring, and support uploads.

Evidence to request Telemetry configuration; sample application payloads; destination and retention inventory; support-bundle contents; egress records.

How would you verify this? Inspect sample payloads and outbound traffic during normal use, errors, and support collection. Reconcile destinations with the allowlist. Inspect contents at the application layer because encrypted traffic alone cannot show the payload.

Suggested roles Observability lead + security or privacy owner

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date

AI Sovereignty Evidence Checklist

Continue the same review. Record evidence, observed results, gaps, and accountable owners. Status: Unverified / Demonstrated / Gap / Accepted dependency / Not applicable (explain).

System / version: _____ Reviewer / date: _____

Boundary / approved external services: _____ Required offline period: _____

05 Encryption keys

Who controls the keys, and who can revoke them?

Include key administration, decrypt permissions, supplier access, policy changes, recovery keys, cached keys, and plaintext copies.

Evidence to request Key ownership and policy records; decrypt grants; key audit events; rotation, revocation, and recovery procedures.

How would you verify this? Revoke a test key in an isolated environment and attempt fresh decrypt operations. Check cached-key and plaintext behaviour, then test recovery. Record who could reverse revocation; revocation cannot recall plaintext already copied.

Suggested roles Key-management owner + security lead

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date

06 Software and model updates

Who approves changes, and can versions be retained?

Include weights, tokenizers, runtimes, drivers, prompts, retrieval settings, registry credentials, model access rights, and security maintenance.

Evidence to request Approved release manifest with versions and hashes; artifact inventory; model access and licence terms; change approvals; rollback records.

How would you verify this? Match deployed artifacts to the approved manifest. Rebuild from retained copies with external registries blocked and demonstrate rollback. Confirm retention and use rights, access-token dependencies, and an owner for security fixes.

Suggested roles Release or MLOps lead + procurement owner

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date

AI Sovereignty Evidence Checklist

Continue the same review. Record evidence, observed results, gaps, and accountable owners. Status: Unverified / Demonstrated / Gap / Accepted dependency / Not applicable (explain).

System / version: _____ Reviewer / date: _____

Boundary / approved external services: _____ Required offline period: _____

07 Continuity

What works if external services become unavailable?

Include identity, DNS, time, certificates, registries, model access, licence checks, monitoring, backups, restart, and operator availability.

Evidence to request Dependency inventory; recovery runbook; local artifact and backup inventories; continuity objectives; exercise logs and timings.

How would you verify this? In a controlled test, disconnect external services and try login, ingestion, inference, restart, and restoration. Exercise relevant credential or licence expiry. Record duration, lost functions, recovery time, and staffing; do not infer indefinite independence.

Suggested roles Platform operations lead + continuity owner

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date

08 Exit and portability

Can the organisation export its data and replace components?

Include documents, chunks, permissions, metadata, configurations, evaluation cases, audit records, export rights, and replacement effort.

Evidence to request Export formats and samples; schemas; component interfaces; exit terms; migration runbook; alternative-component evaluation results.

How would you verify this? Import a representative export into an alternative component. Check retrieval quality, citations, and access restrictions. Account for re-embedding if the model changes; measure time, lost features, cost, and required supplier assistance.

Suggested roles Application architect + data and procurement owners

Evidence reference / capture date / system version

Observed result / test duration / status

Gap or accepted dependency

Named owner / next action / due date

Approver / acceptance rationale / next review date