AI Sovereignty Quarterly Review Checklist

amazee.ai

Quarter	
Review Owner	
Participants	
Systems & Teams in Scope	
Previous Actions Reviewed	
Next Review Date	

1 | Confirm the Scope

- [ ] List every active AI use case, application, agent, API integration, embedded feature, & approved
- [ ] Identify the business & technical owner for each use case.
- [ ] Record the teams & user groups with access.
- [ ] Confirm which models, providers, regions, & environments each workload uses.
- [ ] Compare the inventory with procurement records, API key records, expense data, & security findings.
- [ ] Investigate new or unapproved tools that may indicate shadow AI.
- [ ] Retire duplicate, abandoned, or ownerless workloads.

Keep as evidence: Updated AI register, owner list, data-flow diagrams, & retirement records.

2 | Recheck Data & Purpose

- [ ] Confirm that the documented purpose for every use case is still accurate.
- [ ] Identify the data used in prompts, files, retrieved context, metadata, logs, & outputs.
- [ ] Check whether personal, confidential, privileged, regulated, or contractually restricted data has been introduced.
- [ ] Confirm teams use only the data needed for the stated purpose.
- [ ] Reassess the lawful basis & notices where personal data is involved.
- [ ] Verify that retention & deletion rules cover prompts, outputs, logs, backups, & connected stores.
- [ ] Check that memory, history, fine-tuning, file storage, & external connectors have received separate approval where needed.

Keep as evidence: Data classification, processing purpose, retention decision, privacy review, and approved exceptions.

3 | Verify Residency & Jurisdiction

- [ ] Confirm where prompts, outputs, logs, backups, & support data are processed & stored.
- [ ] Verify that the selected region still matches customer contracts, internal policy, & sector requirements.
- [ ] Review providers, subprocessors, infrastructure operators, & relevant legal jurisdictions.
- [ ] Check whether remote support or administrative access can occur from another region.
- [ ] Confirm that international transfers have the required legal mechanism & assessment.
- [ ] Review changes to provider ownership, subprocessor lists, & government-access exposure.
- [ ] Document exceptions, why they remain acceptable, and who approved them.

Keep as evidence: Region configuration, subprocessor list, transfer assessment, data-processing agreement, & exception approvals.

4 | Review Providers, Models, & Contracts

- [ ] Confirm that every active provider & model remains approved for its current use.
- [ ] Review changes to data use, training, retention, deletion, intellectual property, incident support, & liability terms.
- [ ] Check whether the provider has introduced features that store or reuse data.
- [ ] Confirm that security & compliance documentation remains current.
- [ ] Identify models approaching deprecation & assign a migration owner.
- [ ] Test a replacement before changing a production model.
- [ ] Record why each model remains suitable, including quality, risk, region availability, & cost.

Keep as evidence: Approved provider & model list, contract review, security documents, model decisions, & migration plans.

5 | Reconcile Access & Credentials

- [ ] Match active users, workspaces, service accounts, & API keys to current owners.
- [ ] Revoke access for people who have changed roles or left the organization.
- [ ] Remove unused, duplicate, or ownerless keys.
- [ ] Separate individual user keys from service-account keys.
- [ ] Confirm each key is scoped to the intended team, service, & environment.
- [ ] Rotate credentials according to policy & after suspected exposure.
- [ ] Review workspace & team isolation against the current organizational boundaries.
- [ ] Test the joiner, mover, & leaver process using a recent example.

Keep as evidence: Access review, revoked credentials, key-owner register, rotation record, & remediation tickets.

6 | Test Gateway and Application Controls

- [ ] Confirm production applications send requests through the approved gateway or access path.
- [ ] Verify API key controls, workspace isolation, rate limits, request validation, & schema enforcement where applicable.
- [ ] Check spend limits & budget controls by key, user, or team.
- [ ] Confirm zero data retention remains the default for workloads that require it.
- [ ] Verify that customer prompts & files are not used for model training.
- [ ] Check that content logging is explicit, approved, & stored in a customer-controlled location.
- [ ] Test error handling so failures don't route data to an unapproved provider or region.
- [ ] Confirm sensitive workloads use the required enterprise deployment & infrastructure configuration.

Keep as evidence: Configuration records, test results, approved logging design, & control changes.

7 | Review Usage & Cost

- [ ] Compare usage with the previous quarter by team, application, model, & key.
- [ ] Investigate unexplained spikes, dormant integrations, & unusual activity.
- [ ] Review spend against budgets & expected business value.
- [ ] Confirm that rate limits and cost caps still fit production demand.
- [ ] Identify workloads that need a different model based on quality, latency, region availability, or cost.
- [ ] Check whether growth requires a dedicated enterprise deployment or additional regional capacity.
- [ ] Assign follow-up actions for teams ready to move from a pilot to governed production.

Keep as evidence: Usage summary, cost review, anomaly investigation, capacity decision, & expansion plan.

8 | Confirm Human Oversight

- [ ] Reclassify each use case if its audience, automation, data, or consequences have changed.
- [ ] Confirm where a person must review, challenge, or override an AI-supported result.
- [ ] Check that reviewers have enough context, expertise, time, & authority.
- [ ] Sample outputs for factual errors, bias, unsafe recommendations, insecure code, copyright concerns, & policy breaches.
- [ ] Verify that public-facing and consequential outputs receive the required specialist approval.
- [ ] Record the human rationale for high-impact decisions rather than relying on a simple approval click.
- [ ] Confirm that affected people have an escalation or appeal route where required.

Keep as evidence: Risk classification, test sample, reviewer guidance, approval records, & escalation procedure.

9 | Check Audit & Incident Readiness

- [ ] Confirm that retained audit metadata meets investigation & assurance needs.
- [ ] Test access to available evidence before an incident or audit requires it.
- [ ] Check that logging does not capture prompt content unless this is intentional, approved, & protected.
- [ ] Run a tabletop exercise for an exposed key, prohibited data submission, harmful output, or provider incident.
- [ ] Verify escalation paths across security, privacy, legal, engineering, communications, & the business owner.
- [ ] Review incidents, complaints, near misses, & data-subject requests from the quarter.
- [ ] Confirm corrective actions were completed & reflected in policy, training, or configuration.

Keep as evidence: Evidence map, tabletop results, incident records, corrective actions, & current contact list.

10 | Review Policy, Training, & the Approved Route

- [ ] Update acceptable-use policy for material changes in tools, risk, or regulation.
- [ ] Confirm employees know which AI services are approved and where to request access.
- [ ] Give teams clear examples of restricted data & prohibited uses.
- [ ] Keep approval paths proportionate, with faster handling for routine low-risk uses.
- [ ] Review training completion & provide role-specific refreshers.
- [ ] Ask users where the approved route creates friction or fails to meet a legitimate need.
- [ ] Turn recurring questions into guidance, templates, or platform improvements.

Keep as evidence: Current policy, training records, employee communications, feedback themes, & improvement backlog.

11 | Close the Quarter with Clear Decisions

- [ ] Mark each control as effective, needs improvement, or not applicable.
- [ ] Give every gap an owner, priority, due date, & required evidence.
- [ ] Escalate high-risk findings rather than carrying them into the next quarter.
- [ ] Record accepted risks with a named approver & review date.
- [ ] Approve, restrict, pause, or retire each use case where a decision is required.
- [ ] Summarize changes in AI adoption, risk, cost, & control effectiveness.
- [ ] Share relevant findings with leadership & remediation owners.
- [ ] Schedule the next review and any interim checks needed for higher-risk systems.

Quarterly Decision Summary

Area	Status	Owner	Evidence	Follow-up Date
AI Inventory & Ownership				
Data Classification & Purpose				
Residency & Jurisdiction				
Providers, Models, & Contracts				
Access & Credentials				
Technical Controls				
Usage & Cost				
Human Oversight				
Audit & Incident Readiness				
Policy & Training				

Notes

Reduce Your Workload with a Private AI Gateway

A private AI gateway can reduce that workload by bringing many of the technical controls into one approved access path. You can review regional routing, model access, API keys, workspace boundaries, usage, and spending centrally.

The amazee.ai AI Gateway gives enterprises a controlled, region-selectable, OpenAI-compatible route to leading AI models. Its privacy-first pure-proxy model provides zero data retention by default, and customer prompts and files aren't used to train models. Teams can create, scope, and revoke API keys, isolate workspaces, apply spend limits, and choose dedicated deployments for enterprise requirements.

Check out amazee.ai's Private AI Gateway