

THE AI GOVERNANCE CHECKLIST

How to audit your Zapier and AI stack for data exposure.

15 practical controls for the systems your team already uses.

Bring this checklist to a review with the people who own your operations, technology, and data. For each control, record the evidence, the owner, and the next action. An unknown answer is a reason to investigate.

ORGANIZATION

REVIEWER / ROLE

WORKFLOW / SYSTEMS

REVIEW DATE

Use evidence, not assumptions.

1. Map the workflow and include connected vendors and tools.
2. Mark each control as reviewed, a gap, or not yet checked.
3. Assign follow-up work and agree when it will be reviewed.

This is a working checklist, not a certification or a completed security audit. Provider policies, model eligibility, and your contractual requirements must be checked for the actual deployment.



01 / Ownership and data use

Establish who is responsible and what information the workflow can use.

01 Assign an accountable owner

Name the business owner, technical owner, and approver for each AI workflow.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action:

02 Inventory AI vendors and integrations

Record the provider, model, subscription or API tier, connected tools, and purpose.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action:

03 Map the data flow

Identify what leaves each system, every processor it reaches, and where copies are stored.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action:

04 Classify and minimize sensitive data

Identify customer PII, financial records, and confidential material. Remove or redact fields the workflow does not need.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action:

05 Verify training-use terms

Check the terms for the exact product and account. Record whether prompts, files, or outputs can be used for model training.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action:

Need help closing the gaps? Discuss an Operational Discovery Audit.



02 / Retention and access

Verify where information goes and who or what can reach it.

06 Verify retention and deletion

Document provider logs, application state, backups, and deletion schedules. Confirm zero-data-retention eligibility and activation where required.

☐ Evidence reviewed☐ Gap found☐ Not yet checked

Owner / evidence / next action: _____

07 Confirm processing locations

Check processing, storage, support access, and subprocessors against your organization's residency requirements.

☐ Evidence reviewed☐ Gap found☐ Not yet checked

Owner / evidence / next action: _____

08 Review vendor evidence

Collect current contractual terms and relevant independent assurance reports. Check the services and controls actually covered.

☐ Evidence reviewed☐ Gap found☐ Not yet checked

Owner / evidence / next action: _____

09 Limit identities and permissions

Use named service identities with the smallest access needed. Review who can add tools or expand permissions.

☐ Evidence reviewed☐ Gap found☐ Not yet checked

Owner / evidence / next action: _____

10 Protect and rotate credentials

Keep production keys in a secrets store. Assign an owner for rotation and revocation when access changes.

☐ Evidence reviewed☐ Gap found☐ Not yet checked

Owner / evidence / next action: _____

Need help closing the gaps? Discuss an Operational Discovery Audit.



03 / Approvals and operation

Define how actions are approved, monitored, and recovered.

11 Define approval boundaries

Document which actions require a person, including payments, access changes, external messages, and deletion.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action: _____

12 Test untrusted content and outputs

Test prompt injection, malformed inputs, and unsupported answers. Validate extracted fields before they change a record.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action: _____

13 Keep useful, limited audit records

Capture actions, approvals, and failures with appropriate access and retention. Avoid unnecessary sensitive payloads in logs.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action: _____

14 Plan failure response and shutdown

Name the responder, define alerts and recovery, and test a way to stop or roll back the workflow.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action: _____

15 Set a baseline and review cadence

Record operating costs, cycle times, and error rates. Recheck performance and controls when models, vendors, or workflows change.

☐ Evidence reviewed

☐ Gap found

☐ Not yet checked

Owner / evidence / next action: _____

Need help closing the gaps? Discuss an Operational Discovery Audit.