



4. Security, Privacy and Legal: define specialist review routes and decision limits for applicable uses.
5. Sponsor: assign one accountable person per process, backups, funding and escalation authority.
6. ITAM lead: publish the approved charter, cadence, scope and authority matrix in the controlled evidence store.

Decision and exception rules

An executive may approve funding but cannot waive another authority's mandatory approval. Record the delegation, backup and expiry for each authority. Use the Seven Gates as checkpoints: Request purpose; Procure rights; Receive access and evidence; Deploy accepted configuration; Maintain controls; Recover identities and capacity; Dispose data and obligations.

Unowned services remain visible and cannot receive routine production approval.

Evidence record

Service boundary; legal entities; sponsor; accountable human; specialist approvals; delegation expiry; gate evidence; exception expiry. Preserve the source and effective date for each material fact; record decisions and approvals separately from observations.

Acceptance test

Give the team an unowned embedded assistant inside an already approved SaaS product. Expected: create a candidate service, establish an owner and assess changed data/actions before enabling the feature. Existing SaaS approval alone does not pass.

Completion: Sponsor-approved scope, ownership, funding and escalation exist.

Measurement

In-scope services with named accountable owner / total in-scope services. State the denominator, time window, exclusions and owner before reporting. Track unknown and overdue exceptions separately.

AI02 Discover AI adoption and reconcile coverage

Accountable role: ITAM lead. Trigger: Scheduled discovery, new supplier or shadow-use signal.

Inputs: Procurement, expense, SSO, cloud billing, approved endpoint and gateway sources. Core connections: C01 G03 G04 C04.

Operating design

Define the population for each discovery source. SSO covers federated access, expense data covers reimbursed purchases, cloud billing covers charges and gateway records cover routed requests; none individually describes the whole estate. Capture source coverage dates, collection permissions, expected totals and gaps. Reconcile aliases using supplier account and tenant identifiers. Treat unmatched records as candidates with an owner, never as automatically approved services.

Procedure

1. Analyst: obtain authorized, minimized exports and record source time, period, entity and expected count.



2. Integration owner: reconcile fetched, accepted and rejected populations; investigate pagination and missing scope.
3. Analyst: match supplier/service/account identifiers, preserving uncertain matches instead of merging by name alone.
4. Business owner: explain the work performed by unapproved services and why the sanctioned route was insufficient.
5. Security owner: triage unsafe use and approve containment without deleting needed investigation evidence.
6. ITAM lead: reconcile findings into AI03 with an owned exception queue and coverage limitations.

Decision and exception rules

Do not scrape personal accounts or collect prompt contents merely to discover an application. Use authorized metadata and route suspected sensitive activity to the incident owner. Stop declaring coverage when the source population or last successful complete extraction is unknown.

Do not claim no shadow AI merely because an SSO source is clean.

Evidence record

Source ID; authorization; extraction time UTC; covered period; expected records; fetched records; rejected records; identity match basis; investigation owner. Preserve the source and effective date for each material fact; record decisions and approvals separately from observations.

Acceptance test

Synthetic source: 120 billed accounts, 105 SSO accounts, 15 non-SSO accounts and 5 overlapping aliases. Expected: preserve provenance, resolve overlaps by stable IDs, investigate the non-SSO population and report source coverage separately from service approval.

Completion: Every discovered candidate is matched or assigned for investigation; coverage limits are explicit.

Measurement

Reconciled source populations and aged unowned candidates, reported separately. State the denominator, time window, exclusions and owner before reporting. Track unknown and overdue exceptions separately.

AI03 Maintain the AI estate and dependency register

Accountable role: Asset data owner. Trigger: New service, changed dependency or periodic reconciliation.

Inputs: Discovery candidates, service owners, identities, models, agreements and meters. Core connections: G03 C03 C04 S02.

Operating design

Separate service, use case, model, deployment, agent, identity, tool, dataset, contract and meter records. A model may serve multiple deployments; one service may route to several models. Store