



FREE PROGRAM-IN-A-BOX

The AI Identity & Attestation Program Blueprint

Launch a credible enterprise program in 30 days—with the operating model, templates, technical patterns, and executive materials already created for you.

Discover → Register → Verify → Attest → Resolve → Report

Use with Keypass or adapt to your existing environment. Version 1.0 • August 2026

Start here

You do not need a perfect inventory, a large transformation budget, or a new governance bureaucracy.

THE PROMISE Within 30 days, establish a persistent identity, accountable owner, and recurring attestation for a meaningful pilot population of enterprise AI.

This blueprint is for the person who has been asked to “get control of AI” but has inherited fragmented spreadsheets, overlapping tools, uncertain ownership, and no reliable way to tell whether yesterday’s inventory is still true.

What you will leave with

- An executive-ready program narrative and charter.
- A scored readiness assessment that exposes precise operating gaps.
- A 30-day launch plan and 60-day scale plan.
- A minimum AI identity standard, role model, and lifecycle.
- Registration and attestation playbooks with escalation rules.
- Integration patterns for catalogs, GRC, CI/CD, gateways, and AI factories.
- Program KPIs and a monthly executive report format.
- Editable companion assets you can brand and reuse.

The important boundary

AI identity establishes which AI is being discussed, which organization recognizes it, who owns it, why it exists, and whether its registration is current. It does not independently prove that the AI is secure, compliant, accurate, safe, or cryptographically authentic. Those disciplines can reference the persistent Key ID and attach their own evidence and decisions.

How to use the package

If you need to...	Open...
Get leadership approval	Executive Pitch deck + Section 2
Diagnose your current state	Readiness Assessment workbook + Section 3
Launch the pilot	30-60-90 Roadmap + Sections 4–7
Run the recurring program	Operating Toolkit + Sections 8–10
Integrate technically	Section 9 + Developer Community patterns

1 The Executive Blueprint

AI governance cannot reliably govern an AI it cannot consistently identify.

The entire program on one page

Step	Operating action	Outcome
01	DISCOVER	Identify AI systems, applications, models, agents, copilots, automations, and embedded vendor AI.
02	REGISTER	Issue a persistent identity and capture minimum organizational facts.
03	VERIFY	Make registration status and organizational ownership independently checkable.
04	ATTEST	Ask the accountable owner to periodically affirm that the identity record remains accurate.
05	RESOLVE	Escalate missing ownership, overdue attestations, duplicates, and lifecycle exceptions.
06	REPORT	Measure coverage, currency, response performance, and exceptions—not paperwork volume.

Minimum viable program

- One executive sponsor and one named program owner.
- A written definition of which AI must be registered.
- A persistent, globally unique identifier for every recognized AI.
- One accountable human owner per identity.
- A small required metadata set.
- A documented attestation cadence and escalation path.
- A visible status model and historical record.
- A monthly operating review based on exceptions and coverage.

Five decisions leadership must approve

1. Which AI is in scope?
2. Who is accountable for each identity record?

- 3. What facts must every record contain?
- 4. How often must owners attest, and what happens when they do not?
- 5. Which workflows must reference or verify the persistent identity?

Identity versus evaluation

Identity program establishes	Specialist disciplines evaluate
Which AI this is	Whether it is secure
Which organization recognizes it	Whether it meets policy or regulatory obligations
Who owns it	Whether risk is acceptable
Its intended business purpose	Whether outputs are accurate and appropriate
Whether registration is current	Whether runtime behavior is safe

2 Win Executive Support

Make the request small, concrete, and visibly connected to existing governance investments.

The 60-second pitch

SAY THIS We already have processes that assess security, privacy, risk, architecture, and compliance. The missing foundation is a persistent way to establish which AI is being evaluated, who owns it, and whether that registration remains current. I propose a 30-day pilot that assigns identity and accountability to a defined AI population, runs one owner-attestation cycle, and reports coverage and exceptions. It will complement—not replace—our existing systems.

The decision request

Ask	Recommended starting position
Scope	One business unit, AI platform, or 25–100 AI identities
Duration	30-day launch; 60 additional days to integrate and scale
Leadership	One sponsor and one empowered program owner
Participants	AI owners, architecture/platform, governance/risk, security, and one operations administrator
Success	Named ownership, complete required fields, first attestation completed, exceptions visible, and monthly reporting live

Objection handling

Leadership objection	Response
“We already have an inventory.”	An inventory is useful. The pilot tests whether every record has a persistent identity, accountable owner, explicit status, and repeatable confirmation that the record remains current.
“This sounds like another governance tool.”	It is a lightweight identity layer. Existing risk, security, architecture, and compliance systems can continue to own their specialist decisions.
“Can’t we use a spreadsheet?”	A spreadsheet can start discovery. The program requires stable identifiers, controlled ownership, status, history,

recurring attestations, verification, and integration.

“Will this slow delivery?”

Begin with registration and ownership. Add automated verification only to workflows where the control value exceeds the delivery friction.

“Does active mean safe?”

No. Active means the organization recognizes the identity and its registration is current. Safety and compliance decisions remain separate.

Pilot business case

- Reduce time spent reconciling competing inventories and ambiguous names.
- Create a join key across governance, security, cost, architecture, procurement, and delivery records.
- Expose orphaned AI and stale ownership before an incident, audit, or executive question.
- Demonstrate control without claiming that identity equals safety or compliance.
- Give leadership a measurable coverage and attestation program rather than a one-time inventory exercise.

3 Score Your Readiness

Use the companion workbook for automatic scoring; use this page to interpret the result.

Dimension	Diagnostic question
Identity	Can two systems and two teams unambiguously refer to the same AI?
Ownership	Is one accountable person clearly responsible for each identity record?
Lifecycle	Can teams distinguish proposed, active, expiring, expired, and revoked records?
Attestation	Can the organization prove who confirmed which identity facts, and when?
Integration	Do relevant workflows reference or verify the same persistent identity?

Score	Level	What it means	First move
0–15	Unknown	Identity depends on individual knowledge.	Define scope and pilot population.
16–30	Documented	Inventory exists, but ownership or currency is unreliable.	Standardize identity, owner, status, and cadence.
31–45	Managed	Repeatable registration and ownership practices exist.	Automate reminders and connect key systems.
46–60	Verifiable	Identity and attestation operate across workflows.	Improve enforcement, exceptions, and assurance.

Do not wait for a perfect score

The assessment is a prioritization tool, not a gate. A useful pilot deliberately exposes missing ownership, duplicate identities, unclear scope, and stale records. Those discoveries are early wins because they convert invisible ambiguity into work the organization can assign and resolve.

4 The 30-60-90 Day Roadmap

Launch in 30 days. Integrate and institutionalize during days 31–90.

Window	Objective	Milestones	Proof
Days 1–10	Design	Sponsor, charter, scope, roles, minimum metadata, status definitions, cadence, pilot selected.	Approved one-page charter and owner list.
Days 11–20	Populate	Discover pilot AI, remove obvious duplicates, register identities, assign owners, resolve missing fields.	Pilot registry populated and quality-reviewed.
Days 21–30	Operate	Notify owners, run first attestation, escalate non-response, publish baseline dashboard, hold review.	First cycle completed; exceptions and next actions visible.
Days 31–60	Connect	Map Key IDs into catalogs/GRC/CMDB/procurement; refine reminders; pilot verification in one workflow.	One integration live; coverage and response improving.
Days 61–90	Scale	Expand population, add lifecycle triggers, consider CI/CD or gateway checks, establish monthly executive review.	Repeatable service with accountable backlog.

30-day launch checklist

- ☐ Sponsor approves scope and success criteria.
- ☐ Program owner has authority to request and escalate owner responses.
- ☐ In-scope definition and exclusions are published.
- ☐ Required fields, statuses, and attestation cadence are configured.
- ☐ Pilot population is imported or registered.
- ☐ Every identity has one accountable owner.
- ☐ Owner communications and FAQs are ready.
- ☐ First attestation cycle is completed.
- ☐ Exceptions are assigned and aged.
- ☐ Baseline dashboard and executive update are delivered.

5 Adopt an AI Identity Standard

Keep the identity record small enough to maintain and useful enough to connect.

Recommended in-scope definition

COPY-PASTE STANDARD Register any AI system, application, model, agent, copilot, automation, or embedded vendor capability that performs or materially influences a business process, decision, customer or employee interaction, production workflow, regulated activity, or access to organizational data.

Minimum identity record

Import field	Purpose	Example / rule
name	Human-readable identity name	Claims Assistant
type	AI classification	Use the current Keypass type values; e.g., Agent.
purpose	Concise business outcome	Automates first-pass claims triage.
owner_name	Accountable human owner	Priya Patel; do not use a team mailbox.
environment	Deployment context	Production, Development, Test, or approved vocabulary.
business_unit	Organizational placement	Claims
provider	External/internal provider	OpenAI
model	Model reference when applicable	gpt-4o
repository_url	Source or configuration repository	Full HTTPS URL.
application_url	Application/service location	Full HTTPS URL.
internal_reference	Existing join/reference value	CLAIMS-001
data_classification	Organizational data classification	Internal
description	Operational context	Customer-facing claims triage agent.
tags	Searchable labels	Semicolon separated: claims;prod

Keypass assigns the persistent Key ID and manages registry status, attestation dates, version, and history. They are program outputs rather than fields in the current CSV import template.

Suggested type taxonomy

- AI-enabled application
- Autonomous or semi-autonomous agent
- Foundation or general-purpose model
- Fine-tuned or organization-specific model
- Copilot or assistant
- AI workflow or automation
- Embedded vendor AI
- AI development or orchestration platform
- Evaluation, monitoring, or guardrail service

Status meanings

Status	Meaning	Required action
Registered	Identity exists but activation requirements are not complete.	Complete ownership and minimum fields.
Active	Organization recognizes the identity and registration is current.	Continue normal cadence.
Expiring	Attestation due date is approaching.	Owner confirms or updates record.
Expired	Required attestation was not completed by policy deadline.	Escalate and determine continued recognition.
Revoked	Organization no longer recognizes the registration as valid.	Stop relying on active status; retain history.

6 Establish Roles and Accountability

The central team operates the program. AI owners remain accountable for their records.

Role	Accountability	Typical responsibilities
Executive sponsor	Authority and prioritization	Approve scope, remove barriers, review material exceptions.
Program owner	Program outcome	Own standard, cadence, KPIs, escalation, and improvement backlog.
AI owner	Identity-record accuracy	Confirm purpose, ownership, status, and current applicability.
Registry administrator	Process operation	Onboard records, run cycles, support owners, maintain quality.
Technical lead	Integration	Propagate Key IDs and implement verification patterns.
Governance/risk	Policy alignment	Connect identity to assessments and specialist decisions.
Security/platform	Control integration	Use identity in delivery, access, or runtime workflows where justified.
Audit/assurance	Independent observation	Review evidence, history, coverage, and exception treatment.

Simple RACI

Activity	Sponsor	Program	AI owner	Technical	Risk
Approve standard	A	R	C	C	C
Register identity	I	A/R	R	C	C
Attest record	I	A	R	I	C
Escalate overdue	A	R	C	I	C
Integrate Key ID	I	A	C	R	C
Report program health	I	A/R	I	C	C

7 Run Registration

Registration creates the durable identity that other evidence and workflows can reference.

6. Confirm the AI meets the inclusion criteria.
7. Search for an existing identity using name, purpose, owner, system, and vendor references.
8. Create the persistent identity only when no valid identity exists.
9. Capture the minimum identity fields and relevant external references.
10. Assign one accountable owner and confirm that the owner accepts responsibility.
11. Review the record for completeness, duplication, and appropriate status.
12. Activate the registration according to program rules.
13. Propagate the Key ID into related systems, repositories, and delivery artifacts.

Registration quality gates

- The record describes a specific AI—not a broad initiative or entire department.
- The purpose explains the business use, not merely “uses AI.”
- The owner is a named accountable person, not a shared mailbox or team name.
- The identity is not a duplicate of another environment, deployment, or vendor capability unless policy intentionally treats them separately.
- The active status is not presented as a security, safety, compliance, or performance approval.
- External assessment and system links remain owned by their source systems.

Identity granularity decision

Question	If yes...
Does the instance have a different accountable owner?	Usually create a separate identity.
Does it serve a materially different business purpose?	Usually create a separate identity.
Can it be independently deployed, revoked, or retired?	Usually create a separate identity.
Is it merely a new version under the same ownership and purpose?	Usually preserve the identity and record version/history.
Is it a shared model used by many applications?	Register the model and applications separately when each has distinct ownership or lifecycle.

8 Run Attestation

Attestation is a recurring owner affirmation of the identity record—not a substitute for reassessment.

The attestation question

ASK THE OWNER Is this AI identity record still accurate and applicable—including its name, business purpose, accountable ownership, organizational ownership, lifecycle status, and referenced systems?

Operating sequence

- 14. Generate the population due during the cycle.
- 15. Notify each accountable owner with the current record and due date.
- 16. Let the owner affirm the record or route changes through the normal update workflow.
- 17. Record the owner, timestamp, outcome, and applicable record version.
- 18. Send reminders according to policy.
- 19. Escalate non-response to the designated manager or program sponsor.
- 20. Update status only according to documented transition rules.
- 21. Review exceptions, complete remediation, and report cycle performance.

Suggested cadence matrix

Population signal	Starting cadence	Adjust when...
High-change agentic or production AI	Monthly	Ownership, purpose, access, or deployment changes frequently.
Material business process AI	Quarterly	Risk and change cadence support less frequent confirmation.
Stable embedded/vendor AI	Semiannual	Contract, vendor, or business use is stable.
Low-change reference records	Annual	Policy permits and change triggers provide additional coverage.

Change-triggered review

Periodic cadence is the backstop. Require an update when ownership, purpose, deployment, vendor, major model, production status, data access, or organizational placement materially changes. Avoid

turning attestation into a detailed change log; use the identity update and audit history for the changed record.

Escalation example

Timing	Action
14 days before due	Initial owner notification
7 days before due	Reminder
Due date	Final owner reminder and program queue
5 days overdue	Manager escalation
15 days overdue	Program exception review
Policy threshold	Status transition or sponsor decision

9 Connect Identity to the Enterprise

Start manually. Connect systems next. Enforce only where it creates more control than friction.

Adoption track	Best for	Pattern	Evidence of success
START	Pilot	Manual registration, public/internal verification, periodic owner attestation.	Owners and status are visible; first cycle completes.
CONNECT	Established governance	Key ID referenced by CMDB, GRC, model catalog, procurement, repositories, and cost records.	Teams reconcile less and records point to the same AI.
ENFORCE	Mature operations	CI/CD, gateway, deployment, or orchestration checks verify recognized status.	Unknown or invalid identities follow a defined exception path.

Integration principles

- Treat the Key ID as the join key; do not duplicate every specialist field in the identity record.
- Design for explicit handling of unknown, active, expiring, expired, and revoked outcomes.
- Cache verification only as long as policy permits; define failure behavior when verification is unavailable.
- Do not claim that identity verification proves runtime cryptographic authenticity.
- Begin with advisory checks, observe false positives and operational friction, then decide whether to gate.
- Preserve the identity across versions when organizational meaning remains stable.

Workflow decision matrix

Workflow	Recommended use of identity	Initial response to invalid/unknown
Architecture review	Require Key ID in decision record.	Return for registration or documented exception.
Procurement	Register material embedded/vendor AI.	Flag for owner assignment before production use.
CI/CD	Verify identity and status before deployment.	Advisory warning during pilot; gate later if justified.
API/agent gateway	Verify recognized identity at interception point.	Deny, quarantine, or route to exception based on risk.

GRC/model risk	Use Key ID to link assessments and decisions.	Create or reconcile identity before closure.
Cost management	Tag usage/cost with persistent identity.	Route unattributed cost for ownership resolution.

10 Measure Program Health

Measure whether the organization can identify, reach, and obtain current accountability—not whether it created more forms.

Executive KPI	Definition	Decision it supports
Identity coverage	In-scope AI with a registered identity ÷ estimated in-scope AI.	Where discovery or adoption is incomplete.
Owner coverage	Active identities with one accountable owner ÷ active identities.	Where accountability is missing.
Current attestation	Active identities with valid attestation ÷ identities requiring attestation.	Whether records are being kept current.
Cycle completion	Attestations completed by due date ÷ attestations due.	Whether the operating model works.
Median time to attest	Median elapsed time from request to completion.	Whether workload and communications are reasonable.
Exception age	Age of unresolved identity and attestation exceptions.	Where leadership intervention is needed.
Verification outcomes	Volume and rate of active, unknown, expired, or revoked results.	Whether integrations expose unmanaged use.

Monthly executive report

- Overall health: Green / Amber / Red with a one-sentence rationale.
- Coverage: registered identities, owner coverage, and growth since last month.
- Attestation: due, completed, on-time rate, median completion time, and overdue count.
- Exceptions: orphaned, expired, revoked, duplicate, and aging items.
- Integration: verification volume, outcomes, and newly connected workflows.
- Progress: three accomplishments and three next priorities.
- Decisions needed: explicit sponsor actions, owners, and dates.

SLO starting points

Objective	Illustrative target
Owner coverage	≥ 98% of active identities have one accountable owner.
On-time attestation	≥ 90% completed by due date during pilot; improve toward ≥ 95%.
Registration quality	≥ 95% of required fields complete and valid.

Exception response	Material exceptions assigned within 2 business days.
Verification availability	Set only after architecture and dependency tolerance are understood.

11 Operate the Monthly Rhythm

A small recurring rhythm turns an inventory into an accountability program.

Week	Program activity	Output
Week 1	Review due population, ownership changes, and new registrations.	Clean cycle population.
Week 2	Send requests and support owners.	Early completions and clarified records.
Week 3	Remind, escalate, and resolve exceptions.	Reduced overdue population.
Week 4	Close cycle, analyze metrics, report, and prioritize improvements.	Executive report and improvement backlog.

30-minute operating review agenda

22. Confirm overall health and material changes.
23. Review coverage and attestation performance against targets.
24. Discuss the oldest or highest-impact exceptions.
25. Review unknown, expired, or revoked verification outcomes.
26. Approve owners and due dates for remediation.
27. Select one program improvement for the next cycle.

Program anti-patterns

- Expanding required metadata until owners cannot maintain it.
- Treating “active” as an assurance or compliance approval.
- Assigning ownership to teams rather than accountable people.
- Creating a new identity for every minor version.
- Running attestations without escalation or consequence.
- Building complex integration before proving the manual operating model.
- Measuring only the number of registrations rather than coverage, currency, and exceptions.

12 Your First Five Moves

Use the next 48 hours to replace blank-page anxiety with visible momentum.

28. Send the executive pitch deck to a prospective sponsor and request a 30-minute decision meeting.
29. Complete the readiness assessment with one architecture, governance, and platform stakeholder.
30. Select a pilot population that is important enough to matter but small enough to complete.
31. Customize the one-page charter and identity standard in the Operating Toolkit.
32. Schedule the day-30 operating review before the pilot begins.

REMEMBER The goal is not to prove that the organization knows everything about every AI. The goal is to create a durable mechanism for identity, accountable ownership, current registration, visible exceptions, and continuous improvement.

Keypass product boundary

Keypass provides a canonical AI identity registry: register an AI once, give it a persistent Key ID, record organizational ownership and accountable ownership, verify registration status, and maintain attestation and audit history. It complements—not replaces—security, compliance, risk, observability, policy, model evaluation, and runtime authentication systems.

Continue

- Documentation: <https://aikeypass.com/docs>
- Developer integration patterns: <https://aikeypass.com/community>
- Product and registration: <https://aikeypass.com/>

This blueprint is an operational starting point, not legal, regulatory, security, or audit advice. Adapt scope, cadence, evidence, escalation, and status rules to your organization's obligations and risk profile.