



CBA PRACTICE NOTE

Establishing an AI system inventory

How to find, record and classify the AI systems an organisation uses, assign owners and proportionate controls, and keep the inventory current as the foundation of AI governance.

First edition

Published September 2026

About this note

This note sets out a method for building and maintaining an inventory of the artificial intelligence systems an organisation uses. It applies the governance, risk classification and oversight domains of the CBA standards for AI governance and for artificial intelligence practice. It is written for the people responsible for AI governance, risk, compliance or technology.

A working template accompanies the note: an inventory register with the recommended fields, a risk classification worksheet and a review log.

Regulation of AI differs between jurisdictions and is changing. The note refers to published frameworks for orientation; it does not describe the legal requirements of any jurisdiction.

1. Why the inventory comes first

An AI policy sets out principles. Applying them requires knowing which systems exist, what they do and who is responsible for them. Without that knowledge, a policy cannot be applied to anything in particular, risk cannot be assessed and controls cannot be targeted. The inventory is the foundation on which the rest of AI governance is built.

2. Define what to include

Agree a working definition of an AI system for the purposes of the inventory. A practical definition includes any system that uses machine learning, statistical models or generative AI to produce predictions, recommendations, decisions or content that affect the organisation's work. It should include:

- systems built in-house;
- products and services bought from vendors that use AI;
- AI features switched on within existing software, such as drafting assistants in office tools;
- general-purpose AI assistants used by staff for work.

Err towards inclusion. It is easier to classify a system as low risk than to discover later that a consequential system was never recorded.

3. Find the systems

AI systems enter organisations by many routes, and no single source will find them all. Combine several:

- **procurement and contract records**, including software subscriptions and renewals;
- **IT asset registers** and lists of approved applications;
- **vendor documentation**, including release notes announcing new AI features in existing products;
- **expense claims and card transactions** for software subscriptions;
- **a short survey of teams**, asking what tools they use for drafting, analysis, prediction or automation;
- **interviews with the owners of key processes**, asking where decisions are informed by a model

or automated output.

Expect to find systems nobody approved. The purpose of the exercise is to know about them, not to penalise their discovery; an amnesty approach tends to produce a more complete inventory.

4. Record the essentials

For each system, record at least:

1. **Name and description:** what the system is and what it does.
2. **Process:** which business process it sits in.
3. **Decision:** what decision it informs or makes, and whether a person reviews its output before it takes effect.
4. **Affected people:** who is affected by that decision — customers, employees, applicants, the public.
5. **Owner:** the named person accountable for its use.
6. **Source:** built, bought or embedded, and the vendor where relevant.
7. **Data:** what data it uses, and whether personal or confidential data leaves the organisation.
8. **Output checks:** how its outputs are checked before they are relied on.
9. **Status:** in use, in pilot, planned or retired, with dates.

5. Classify by consequence

Assign each system a risk tier according to the consequence of its being wrong, not according to the technology it uses. Useful questions are:

- Could an error cause harm to an individual — financial, legal, reputational or to their safety?
- Does the system make or materially influence decisions about people, such as recruitment, credit, pricing or access to services?
- How many people could be affected, and how quickly?
- Would an error be noticed, and could it be corrected?
- Does the system use personal, sensitive or confidential data?

A three-tier scheme is often sufficient: high consequence, moderate consequence and low consequence. Record the reasons for each classification.

Published frameworks follow the same principle. The EU AI Act sorts systems into risk categories with obligations that increase with risk; the NIST AI Risk Management Framework and ISO/IEC 42001 both centre on assessing and treating risk in the context of each use. Whichever framework applies, the inventory provides the information it needs.

6. Match controls to the tier

Set the minimum controls for each tier. For example:

- **Low consequence:** recorded in the inventory, covered by the acceptable use policy, reviewed annually.
- **Moderate consequence:** a named owner, documented output checks, periodic sampling of

outputs, review when the system or its use changes.

- **High consequence:** an impact assessment before use, defined human oversight with the time, information and authority to override, testing for accuracy and bias, monitoring in use, a decision record, and review at least annually.

7. Make human oversight real

Where the inventory records that a person reviews a system's output, confirm that the review is meaningful. A reviewer needs time to review, information to judge whether the output is right, and authority to override it. Define what the reviewer checks, and test the arrangement by sampling reviewed outputs to see whether errors were caught.

8. Keep it current

An inventory is out of date the day after it is completed unless it is maintained. Build updates into existing processes:

- procurement adds a step asking whether a new purchase uses AI;
- IT change management records new AI features and integrations;
- owners review their entries when a system or its use changes;
- the whole inventory is reviewed on a fixed cycle, at least annually.

9. Report

Report the inventory to the people responsible for governance: the number of systems by tier, new and retired systems, high-consequence systems and the status of their controls, and any systems found outside the approved process. The report turns the inventory from a register into a tool for oversight.

Checklist

- ☐ A working definition of an AI system is agreed and includes embedded and general-purpose tools.
- ☐ Systems have been found from several sources, not from a single list.
- ☐ Each entry records the process, decision, affected people, owner, data and output checks.
- ☐ Each system is classified by consequence, with reasons recorded.
- ☐ Minimum controls are set for each tier and applied.
- ☐ Human oversight is defined and tested where it is relied on.
- ☐ Updates are built into procurement and change processes, with a fixed full review.
- ☐ The inventory is reported to those responsible for governance.

Related

- AI Governance Professional: CBA Standard, version 6.1 — cba-uk.com/standards/ai-governance
- Artificial Intelligence Professional: CBA Standard, version 6.2 — cba-uk.com/standards/ai-professional

Template: AI system inventory — cba-uk.com/toolkits

Using this publication

Citation

Corporate Business Alliance (2026). Establishing an AI system inventory: CBA Practice Note, first edition. London: Corporate Business Alliance.

Terms of use

© Corporate Business Alliance 2026. You may download, print and use this publication, and share it unaltered and free of charge, for personal study and within your organisation. It may not be sold, or republished in whole or in part, without the written permission of the Corporate Business Alliance.

Status

The CBA Standards and CBA credentials are the professional standards and certifications of the Corporate Business Alliance. CBA credentials are not regulated qualifications, and CBA is not accredited to ISO/IEC 17024; CBA claims no equivalence to the qualifications of any other body.

Publisher

Corporate Business Alliance Ltd

Registered office: 167–169 Great Portland Street, 5th Floor, London, W1W 5PF, United Kingdom
support@cba-uk.com · cba-uk.com