

AI in Sight

See · Secure · Scale

Diagnostic report, sample excerpt

Organisation A, a fictional insurer · 1,200 employees

Illustrative example. Report structure may vary depending on your organisation and on the depth and breadth of your diagnostic needs.

Builders are anyone in the organisation who creates AI assets. *AI assets* range from AI-written code to prompts reused regularly in formal and informal processes.

Executive summary

Scope: 186 builders surveyed across 14 departments · 412 AI assets declared, 338 assessed in detail · 22 interviews with management, IT, risk, finance and procurement · aggregated usage data from the organisation's AI tools.

Five findings

- 1 Most AI assets are invisible.** 71% of assessed assets are known only to their users. No register or catalogue exists.
- 2 42 assets are business-critical or higher, and 33 of them are ungoverned.** They include a month-end reconciliation automation that writes into the general ledger.
- 3 The best work is unprotected.** 48 high-impact assets are well built, yet 39 of them are invisible to the organisation.
- 4 Confidence runs ahead of practice.** 78% of builders with high-impact assets describe systematic verification; 41% are assessed at that level.
- 5 Governance exists on paper.** An AI policy and an approved tool are in place, yet 58% of builders don't know the rules and 44% build elsewhere.

Three urgent actions

Individual assets	Organisation-wide governance	Scale
30 days · Assets Secure the critical assets Give the 19 invisible business-critical assets a named owner, a backup person and minimal documentation.	60 days · Governance Establish governance Start a light register and change control, beginning with the 109 assets rated cross-functional or higher.	90 days · Scale Harmonise and reuse Consolidate nine parallel claims summarisers into one supported solution and retire personal subscriptions: lower cost, one version to maintain.

Lens 1 · Assets

What has been built, and what depends on it

Builders declared 412 AI assets. Their three most used were assessed in detail for criticality, robustness and governance status.

412

assets declared by 186 builders

109

rated cross-functional or higher

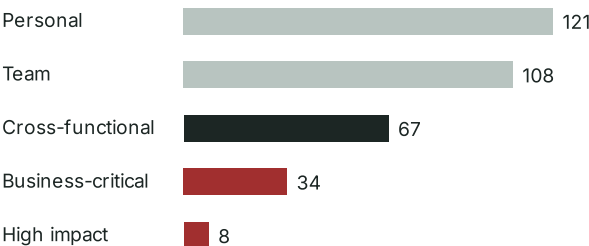
71%

known only to their users

93

automations, agents and AI-written apps

Criticality of assessed assets



338 assets assessed in detail. Criticality follows the most severe of six impact factors.

Where they sit



Under government assets three examples

Asset	Criticality	What we found
Health and social care information system	High	Drives into the general ledger. Built by one vendor on a personal automation account. No documentation, no testing period.
Driver and freight agent operations	High	Sample · detail blurred
Claims fraud flag script (internal)	High	AI-written code used by three teams. Nobody but the author can maintain it. The author has changed role.

Duplication and cost

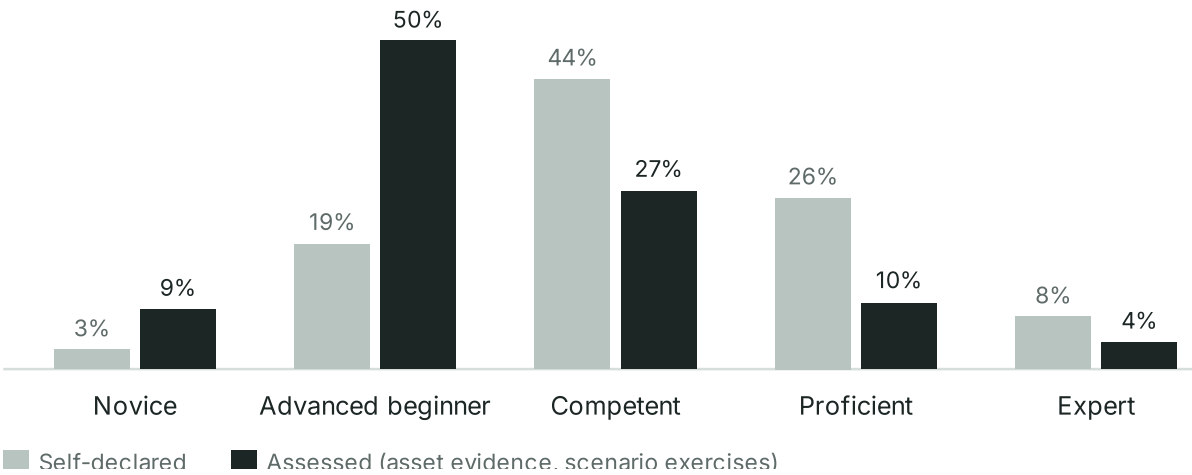
Three separate systems summarise claims files, built independently in six teams. 17 personnel or equivalent in subscriptions are in use alongside the approved tool, and 22 months run on per-lead services with no budget cover.

Lens 2 · People

How well people build

Levels are assessed from three sources: how builders describe their practice, the evidence in the assets they own, and scenario exercises on a sample. Set against self-declaration, the assessment shows where confidence and practice diverge.

Verification practice of the 94 builders who own high-impact assets



78% describe themselves as competent or better. 41% are assessed at that level. The gap is widest in claims operations and finance, where most business-critical assets sit.

Other observations

Observation	Self-declared	Assessed	Insights
Emergency documentation, tests, hardware	75% competent or better	38%	There is a wide spread in ratings across the team.
Hardware design	55% proficient or better	22%	A small group ratings themselves 4 or higher with the top person 100%.

Sample · detail blurred

By department

Department	Builder	High impact assets	Verification gap
Claims operations	15	15	Large
Finance	15	15	Large
Underwriting	15	15	Medium
Customer service	15	15	Medium

Lens 3 · Organisation

Can the organisation see and govern what is built?

Organisational maturity is read from facts: what exists, what is known, and what works in practice. Management interviews are set against builders' experience.

1 Ad hoc
Nobody knows what exists

2 Tolerated and fragmented
Use allowed, practices diverge, duplicates grow

3 Defined
Rules, approved tools and a register exist

4 Managed
Governance and lifecycle work in practice

5 AI-enabled
Assets managed as a portfolio

Organisation A: level 2. Some level 3 elements exist on paper but are not known or applied.

Evidence		
Area	What management reports	What the other teams share
Rules	An AI policy was published in 2020.	50% of builders don't know the rules or follow them well.
Tools	An enterprise AI catalogue is available to all staff.	50% of builders build with other tools, 5% of important subscriptions.
Inventory	IT maintains an application inventory.	It contains up to 50 assets. 70% of assets are known only to their users.
Records	Each business unit maintains different sets.	5% of assets had a formal record, none of the subscriptions.
The results level 3		
Rules known by builders, a register covering high impact assets, critically items applied, and one approved mode for building.		

Across the three lenses

Where the lenses disagree

Each lens alone describes a situation. The contradictions between them explain it, and point to where action pays off.

People x Organisation

Capable builders, blind organisation

39 of the 48 well-built, high-impact assets are invisible. The organisation's best AI work is neither protected nor reused: if these builders leave, the knowledge leaves with them, and nobody else benefits from what they solved.

People self-declared x People assessed

Confidence runs ahead of practice

In claims operations and finance, builders rate their verification practice highly, while most of the business-critical assets there have neither tests nor error detection. Generic AI training would not close this gap; targeted practice on real assets would.

Organisation stated x Builders' view

Conversations on paper

The policy, the approved test and the review process exist, but builders don't read them in their work. The issue is reach, not design: rules nobody encounters cannot shape behaviour.

Assets x Organisation

Displacement follows invisibility

New claims submissions in six teams are a symptom, without a solution, rebuilding is faster than finding. Concentration without a solution would see the pattern return within a year.

Assets x People

The best builders are the largest single problem of builders

27 of the 48 builders with assets located in one person, and 7 of those builders are among the most productive in the organisation.

Sample · detail blurred

Recommendations

The first 90 days

Recommendations are sequenced, owned and scaled to criticality. Tool requirements are specified; tool choices remain the organisation's.

See

Days 1 to 30

- 1. Establish the AI strategy and governance framework.
- 2. Identify key business processes for AI integration.
- 3. Conduct a pilot project to test AI capabilities.
- 4. Develop a data management plan.
- 5. Establish a cross-functional AI working group.

Secure

Days 1 to 60

- 1. Secure executive sponsorship and funding.
- 2. Identify key stakeholders and build relationships.
- 3. Develop a detailed AI implementation plan.
- 4. Conduct a risk assessment.
- 5. Establish a data governance framework.

Scale

Days 30 to 90

- 1. Scale successful pilot projects across the organisation.
- 2. Implement AI governance and monitoring mechanisms.
- 3. Develop a continuous learning and improvement process.
- 4. Establish a feedback loop for AI performance.
- 5. Review and update the AI strategy and governance framework.

Sample · detail blurred

A real diagnostic starts with a conversation

Which populations, which lenses, what depth: the scope is shaped around your organisation, your risks and your priorities.

onspaceship.earth/ai-in-sight