

AI Governance Assessment

Version 0.1 · CC BY-NC 4.0 — attribute to Contextual Agentic, contextualagentic.com

Eighteen questions to ask before an agent is given authority over anything that matters. Each has a scoring note, and the scoring notes are deliberately hard to pass by intending to.

Drafted for the companion material of The Contextual Agentic Enterprise. Not a compliance instrument and not mapped to any regulation. Use it to find the argument you cannot yet make.

Scoring

- **0** — No. Or: we intend to.
- **1** — Partly — it exists for some paths, or on paper only.
- **2** — Yes, and I can show you the artefact right now.

Purpose

GA-01 — Can you state what this agent is for in one sentence without using the word "AI"?

What a 2 looks like — A written purpose that names the outcome and the system of record it touches.

GA-02 — Is there a decision it must never make, written down?

What a 2 looks like — An exclusion list, and a control that enforces at least one item on it.

GA-03 — Who is accountable for its actions by name, not by team?

What a 2 looks like — A named owner who knows they are the owner.

Authority

GA-04 — What is the largest irreversible thing it can do unaided?

What a 2 looks like — A specific answer with a number, derived from the grant rather than guessed.

GA-05 — Who approved that, and when?

What a 2 looks like — An approval record with a date and a scope.

GA-06 — How would you remove its authority in the next five minutes?

What a 2 looks like — A procedure someone has actually executed in a drill.

Context

GA-07 — Where does it get its facts, and how do you know they are current?

What a 2 looks like — A named source with a freshness guarantee and a staleness alert.

GA-08 — Can content it retrieves change what it does?

What a 2 looks like — A prompt-injection test suite in CI with failing cases recorded.

GA-09 — Does it see anything the person it acts for could not see themselves?

What a 2 looks like — Entitlement filtering at retrieval, with a test for two principals.

Enforcement

GA-10 — What stops it doing the thing you most fear, and is that thing code?

What a 2 looks like — A named control outside the model, with the test that exercises it.

GA-11 — What happens when that control is unavailable?

What a 2 looks like — A fault-injection result showing a refusal.

GA-12 — Has anyone tried to talk it past its controls?

What a 2 looks like — A red-team exercise with findings and fixes.

Evidence

GA-13 — If it did something wrong last Tuesday, what could you show an auditor?

What a 2 looks like — A record retrieved in front of the asker, in under a minute.

GA-14 — Could that record have been edited?

What a 2 looks like — Retention lock or a verified hash chain, and a verification run.

GA-15 — Are refusals recorded as carefully as successes?

What a 2 looks like — A refusal count you can quote, and someone who watches it.

Oversight

GA-16 — How many decisions a day does a human have to review, and can they?

What a 2 looks like — A measured review load compared against measured human capacity.

GA-17 — When did a reviewer last say no?

What a 2 looks like — A specific recent example. "Never" is an answer worth investigating.

Economics

GA-18 — What is the denominator in your cost-per-task figure?

What a 2 looks like — A definition that includes failures, reviews and rework, agreed with finance.

Purpose and professional-use notice

This book, course and related articles are designed to help readers understand, discuss and apply practical approaches to real enterprise challenges involving artificial intelligence, architecture, governance, security, data and operating models.

The material is educational. It is intended to support informed thinking, better questions, stronger design decisions and meaningful professional work. It is not a ready-made solution for every organisation or situation.

Adapt what you learn to your own context. Before applying any idea, framework, pattern, checklist or technical approach, consider your organisation's objectives, people, systems, data, risk appetite, contractual commitments, laws, regulatory obligations and governance requirements. Obtain the appropriate internal approvals and independent professional advice where needed.

The material does not constitute legal, financial, investment, tax, regulatory, privacy, cyber-security, safety, employment, procurement, audit, medical or other professional advice. It should not be relied on as a substitute for advice tailored to your particular circumstances.

The views, frameworks and examples are the author's independent professional perspectives. They do not represent the views, policies, strategies, recommendations or endorsement of any employer, client, partner, vendor, regulator or other organisation.

Application requires organisation-specific architecture, security, privacy, legal, regulatory, operational, safety, accessibility, commercial and governance review, together with appropriate approvals. Full disclaimer:
<https://contextualagenticenterprise.com/disclaimer/>