THE ONTOLOGY IMPERATIVE

Trustworthy Agentic AI for Boards, CDOs, and CTOs

Agentic AI Readiness Assessment

Zone × Aspect Self-Assessment for Agentic AI Governance

Frédéric Verhelst · Version 1.2 · 16 June 2026

Purpose

The *Agentic AI Readiness Assessment* is a self-administered diagnostic instrument. It places an organisation against the eleven capabilities of *The Agentic AI Capability Stack™*, each representing a distinct capability the organisation must own, operate, and govern, and produces, in one sitting, an honest map of where capability and governance discipline stand today. The output is intended to inform a board conversation about scope of deployment, the operating mode the Chief Data Officer's mandate should take, and where remediation must begin before any agent reasoning over governed meaning can responsibly enter production.

The rubric is built in the tradition of the TotalEnergies *Self-Assessment Scales* for data management and the Statoil *IO Capability Resource Matrix* for integrated operations. Both proved, in operating environments, that an honest four-level rubric applied across the right capability axes surfaces a maturity profile leadership can act on. Both also taught a second lesson: rate independent aspects of each capability separately, then read the pattern across them. A capability can be technically present but ownerless; it can be owned but unenforced. Conflating those states into a single score hides the diagnostic.

Throughout this instrument, "CDO" designates the C-suite executive accountable for cross-cutting data, analytics, and AI governance. The title varies across organisations (Chief Data Officer / CDO, Chief Data and Analytics Officer / CDAO, Chief Data and AI Officer); the structural argument applies regardless.

How the instrument is organised

The eleven capabilities of the Stack are grouped into four **zones**: Infrastructure (L1–L2), Governance (L3–L8), Capability (L9), and Organisational (L10–L11). Within each zone, three **aspects** are rated independently:

Technology	What exists. The artefact, tool, standard, or infrastructure you can point at, open, query, and version-control. Catalogues, ontologies, SHACL libraries, PROV-O records, orchestration frameworks.
Ownership	Who owns it. The seat in the org chart, the reporting line, the charter. Named Data Owners, named Process Owners, a CDO Office reporting to the CEO. Whether the role exists and holds the authority, not whether the authority is yet used.
Enforcement	Whether it fires. The constraint enforced before action, the gate operating as a paired act, attestation recorded, the audit chain queryable, halt exercised when evidence requires it. Authority used, not merely granted. Discipline beyond declaration.

The four maturity levels

1	**Absent**	The aspect does not exist in any form. No owner is named, no standard is documented, no artefact can be pointed to. Agents operating on this aspect do so without governance scaffolding.
2	**Ad hoc**	The aspect exists in isolated projects, pilots, or vendor platforms. Practice is inconsistent across business units. Ownership is implicit. Standards live in slide decks rather than enforceable artefacts.
3	**Defined**	The aspect is formally defined: open standards selected, ownership named in the org chart, the artefact written down and version-controlled. Roll-out is in progress but not yet enforced at every deployment.
4	**Operational**	The aspect is built, governed under the CDO mandate, and proven on a controlled pilot: demonstrably enforced, with audit evidence from the test. Ready to govern agents at scale. Updates run on the CDO's schedule, not the vendor's. Insurability is supportable.

How to read a result

The score that matters is not the average. It is the lowest aspect within each zone, and the pattern of lows across the four zones. An agentic stack reasons and acts through every zone and every aspect. The weakest link defines what the stack is, in fact, capable of governing.

The assessment matrix

Four zones, three aspects per zone, four maturity columns. Rate each aspect independently by selecting the column whose description matches today's operating reality. The result is twelve scores, not one. Read down for the zone-by-zone story; read across an aspect row for the discipline story within a zone.

Aspect	1 – Absent	2 – Ad hoc	3 – Defined	4 – Operational
Organisational · Capabilities 10–11 · Operating Model, Strategy				
Technology	No operating-model documentation. No insurability view. No board materials.	Operating-mode design for selected processes. Board materials ad hoc.	Operating modes documented per process. Standard of care articulated. Insurability scoped.	Documentation complete per agent class. Insurability and standard of care current.
Ownership	CDO absent or below the C-suite. Co-governance undefined. No board sponsor.	CDO has a voice but not a seat. Co-governance informal. Sponsor unclear.	CDO reports to the CEO. CDO/COO co-governance defined. Board sponsor named.	CDO is a C-suite peer with a board interface. Co-governance roles staffed.
Enforcement	No escalation paths. Board does not review agentic AI. No standard-of-care evidence.	Escalation informal. Board oversight irregular and reactive.	Escalation documented. Board review cadence set and beginning to operate.	Escalation drilled. Board reviews assurance reports every cycle. Care continuously evidenced.
Capability · Capability 9 · Agent Capability, runtime				
Technology	Agents in pilots without orchestration. No registry. Monitoring per vendor.	Some orchestration tooling. Registry partial. Monitoring inconsistent.	Orchestration framework selected. Registry complete. Monitoring designed.	Orchestration, registry and runtime monitoring built and proven on a controlled pilot.
Ownership	No Process Owners. Joint custody undefined. Accountability falls between teams.	Process Owners named informally. Custody project-specific.	Process Owners named per process. Joint-custody charter with CDO documented.	Process Owner role and joint-custody charter defined and exercised on the pilot.
Enforcement	No Deployment Gate. Agents go live unreviewed. Halt does not fire.	Ad hoc reviews. Not structurally gated. No paired-act discipline.	Deployment Gate documented. Criteria published. Both signatures required.	Deployment Gate exercised on the pilot: custody accepted, CDO attests, both recorded; halt fired in test.
Governance · Capabilities 3–8 · Meaning, KG, Contracts, Guardrails, Provenance, Connectivity				
Technology	No ontology. SQL schemas treated as definitions. No KG, SHACL, ODRL, PROV-O.	Glossaries in catalogue tools. Isolated KGs. Prose policies. Logs by application.	OWL ontology drafted on open standards. RDF/SPARQL selected. Templates exist.	Ontology, KG, contracts, SHACL guardrails, PROV-O all built and live.
Ownership	No CDO Office. No capability groups. Meaning capability ownerless.	Some ontology work in pilots. Capability spread across vendors and BUs.	CDO Office stood up. Capability groups named. Mandate and halt authority chartered.	CDO reports to the CEO. Groups staffed. Governance Assurance has an independent reporting line.
Enforcement	No standards enforced. No gates. No audit chain. Ungoverned by design.	Some standards published but not enforced. Gates not operating.	Both gates documented, criteria published. Constraints validate in a test path.	SHACL fires before action on the pilot. Both gates exercised as paired acts. Audit chain queryable end to end. Halt exercised in test.
Infrastructure · Capabilities 1–2 · Data, Data Connectivity				
Technology	No catalogue. Point-to-point integrations. No lineage tooling.	Catalogue in some BUs. Pipelines documented in pockets. Lineage partial.	Enterprise catalogue deployed. Lineage tooling in place. Substrate documented.	End-to-end lineage live. All pipelines catalogued. Provenance hooks ready for L7.
Ownership	No Data Owners. No CIO substrate ownership. No domain structure.	Data Owners named informally. Domains overlap and conflict.	Data Domains scoped. Data Owners appointed with a charter; CIO accountable for the substrate.	Every domain has a Data Owner with a charter; CIO owns the substrate. Stewards and Custodians embedded.
Enforcement	Quality not measured. No standards. Substrate ungoverned end to end.	Quality measured project by project. Standards in slide decks.	Quality standards documented. Catalogue policies in place. Lineage governance defined.	Quality continuously monitored. Ingestion Gate enforces; Data Owners attest at the gate.

Weakest-aspect rule. Within each zone, the score for the zone is the lowest score among its three aspects, not the average. A zone that is technically built and owned but unenforced is Ad hoc, not Defined. The same rule applies across zones for the stack as a whole.

Reading the pattern

Read both directions. Down the rows tells the zone-by-zone story: where the stack is structurally complete and where it is hollow. Across the aspect columns within a zone tells the discipline story: a zone can have its Technology column at 3 and its Enforcement column at 1, in which case capability exists but is unenforceable. In organisations that have invested in data and analytics over the past decade, a recurring profile appears: Infrastructure at 3–4 across all three aspects, the Organisational zone at 2–3, the Governance zone in the middle at 1–2 with its Enforcement aspect lower than its Technology aspect. A solid floor, an aware ceiling, a hollow middle that is hollower still on the discipline axis than on the artefact axis.

That hollow middle is the zone an agentic stack reasons and acts through, and the enforcement lag within it is the gap a CDO mandate is structurally designed to close.

Where to start

The result sets the ceiling on the operating mode the organisation can responsibly support, using the three modes defined in *The CDO Office* mandate document. The modes describe the scope of agentic delegation, not a timeline. The lowest aspect in the Governance zone usually fixes the ceiling: an organisation cannot delegate beyond the mode its Enforcement readiness can carry.

Readiness profile	Maximum mode supported	To reach the next mode
Most aspects at 1–2. Pilots without a mandate.	**Below Mode 1.** No governed delegation until the mandate and Ingestion Gate exist.	Reach **Mode 1** (Governed Infrastructure): establish the mandate, name Data and Process Owners, define the Ingestion Gate.
Infrastructure 3–4; Governance Enforcement at 1. The hollow middle.	**Mode 1 – Governed Infrastructure.** A few agents on CDO contracts. Not ready to delegate a workflow.	Reach **Mode 2** (Delegated Governance, 18–24 months): L3 ontology, Minimum Viable Ontology, pilot SHACL, close the Enforcement gap.
Mostly 3 across all aspects. Governance scaffolding in place.	**Mode 2 – Delegated Governance**, approaching Mode 3. Ready for formal delegation of a workflow.	Toward **Mode 3** (Operational Accountability): gate end to end, PROV-O on every action, independent Assurance to the board. Demanned divisions only.

How the assessment connects to deployment

The Readiness Assessment is one of two inputs to the deploy decision. The companion is the *Use Case Risk Classification Framework*, which scores a proposed deployment along ten dimensions into a risk profile. The board sets the risk appetite; the CDO, with the Chief Risk Officer and legal counsel, operationalises it into the minimum maturity thresholds each profile must clear before deployment, kept internal. A high-risk profile typically requires higher readiness on the dependent capabilities, with Enforcement at least level with Technology. This instrument provides the readiness side; it sets neither the appetite nor the thresholds.

About the author

Frédéric Verhelst, PhD (Applied Physics, TU Delft), works with boards and executive teams on the governance of trustworthy agentic AI. Twenty-five years across data, AI, and regulated industrial operations: external executive advisor on the Tyra Redevelopment FID (a Mærsk Oil joint venture with Shell and Chevron, later operated by TotalEnergies), then Head of Data Office at TotalEnergies EP Danmark, most recently bringing agentic AI into safety-critical maritime operations. Currently available for non-executive director (NED), board-advisory, and CDO appointments focused on corporate AI governance.

Canonical reference: the Agentic AI Capability Stack™ (v3). Companion artefacts: the CDO Mandate, the Board Briefing, the Vendor Coverage Diagnostic, and the CDO Role Specification. All artefacts at fredericverhelst.com/TOI-library. Licensed CC BY-ND 4.0 with attribution.

This instrument provides a self-assessment methodology. It is not regulatory advice and does not constitute an audit opinion. Organisation-specific minimum maturity thresholds for agent deployment must be set by the organisation's Chief Data Officer in consultation with legal counsel and sector regulators.