The Agentic AI Capability Stack™

A Framework for Trustworthy Agentic AI

Frédéric Verhelst · Version 3.1 · 13 June 2026

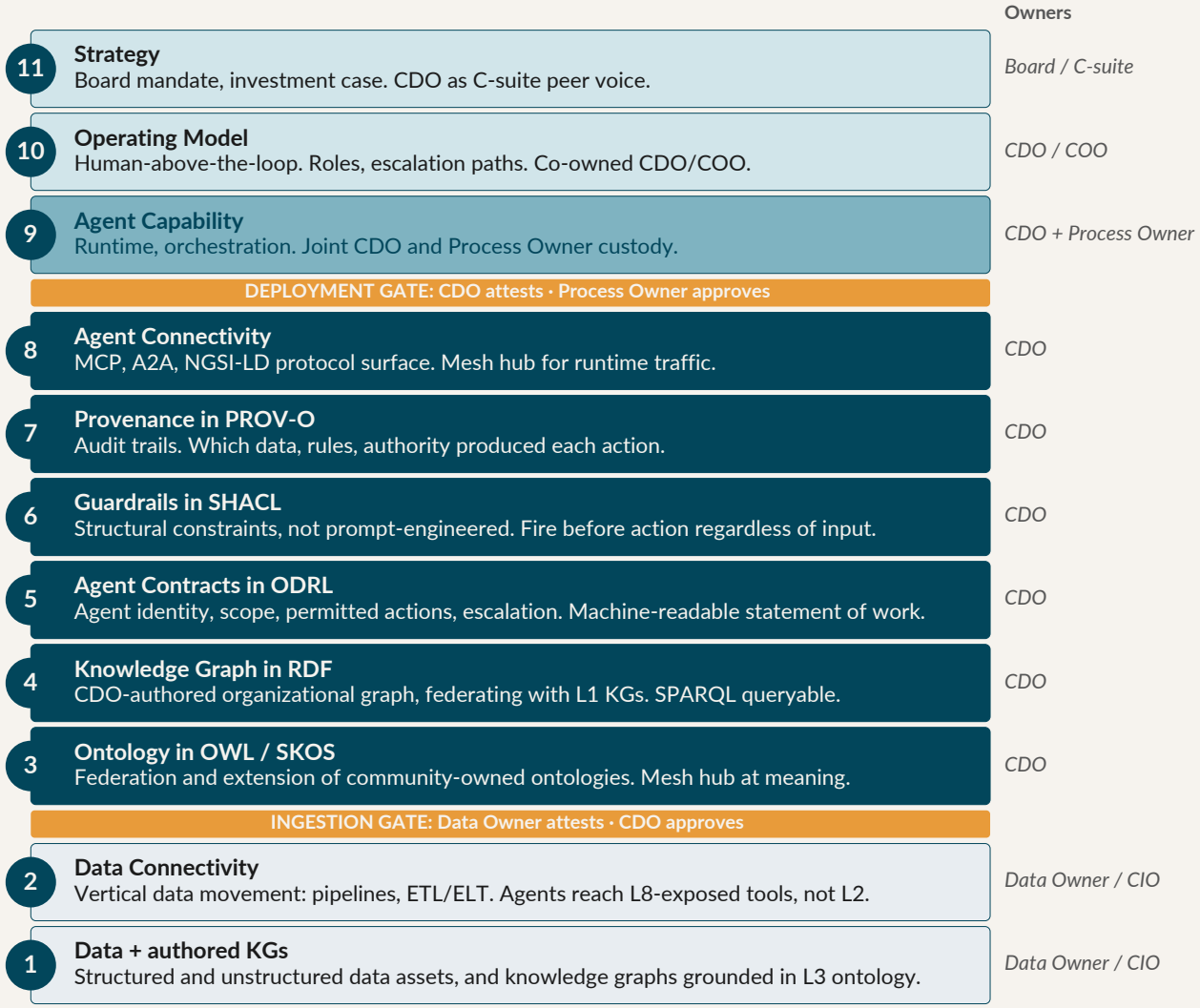
In brief. The eleven capabilities an enterprise must own, and who owns each, to deploy agentic AI it can govern, on open standards it controls rather than a vendor's. Two gates decide what enters the meaning capability and what reaches production.

Page 1: the capabilities and their owners. Page 2: how the governance capabilities wire together at runtime. Page 3: the governance structure, the four sovereignties, and the CDO mandate.

The Agentic AI Capability Stack™ names what an enterprise must put in place to deploy agentic AI it can govern, and who owns each capability. It is both a diagnostic and a specification. Each capability sits on open standards under independent governance bodies, not proprietary formats: open standards keep ownership and portability with the organisation, while a vendor format transfers that control to the supplier. It does not prescribe which vendor, platform, or implementation.

Data enters the governed stack along two pathways:

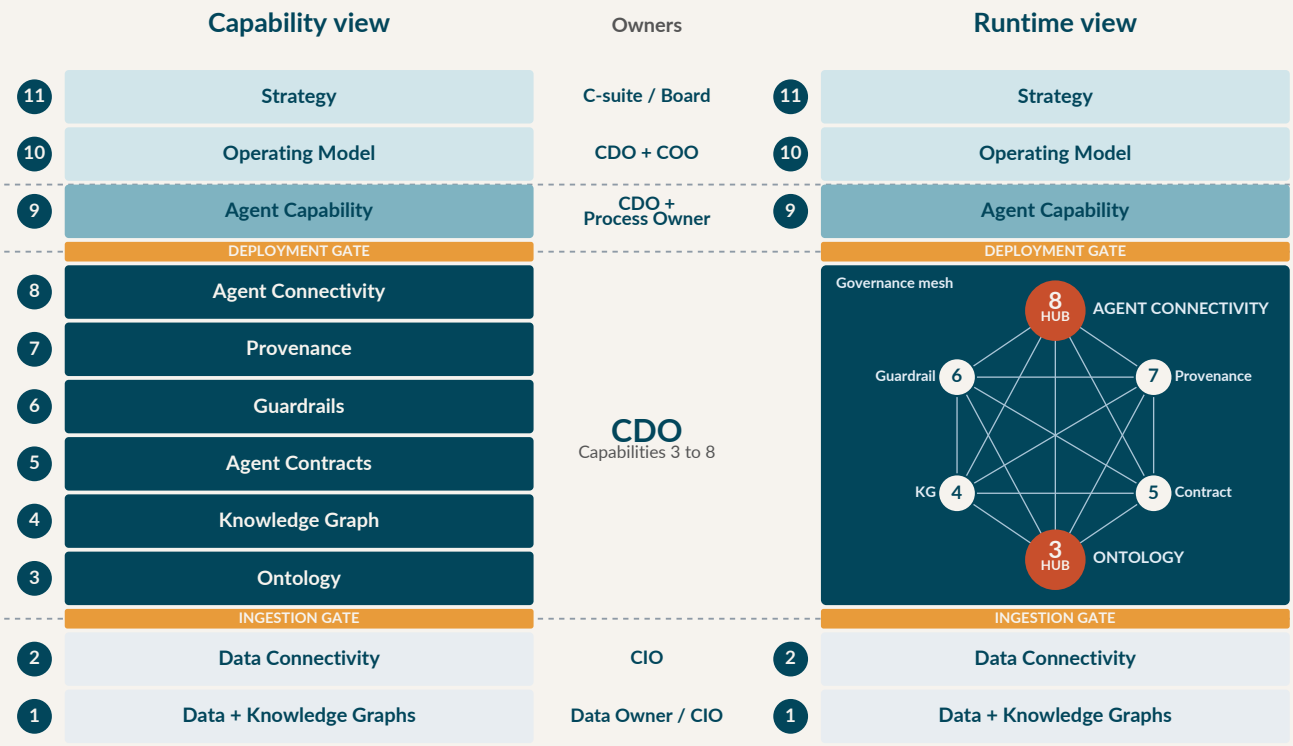
- **Vertical (data at rest).** Semantic, structured, and unstructured data moves up through the data foundation (Capabilities 1 and 2: pipelines, ETL, integration plumbing) and passes the Ingestion Gate into the governed knowledge graph.
- **Horizontal (fast-moving).** Runtime traffic (tool calls, agent-to-agent messages, user utterances, continuous context feeds) arrives at the protocol surface at Capability 8. Agents do not reach Capability 2 directly; they reach the tools exposed at Capability 8, which pull from Capability 2.



The Agentic AI Capability Stack™, v3.1: eleven capabilities, two gates, on open standards

Two views of the same eleven capabilities

The **ladder** on the left shows what to own; the **mesh** on the right shows how the governance zone wires together at runtime. **Capability 3** (Ontology) and **Capability 8** (Agent Connectivity) are the two hubs through which every governance capability reaches every other. Infrastructure (Capabilities 1 and 2) and organisation (Capabilities 10 and 11) remain sequential. **Capability 9** sits in its own zone: after the Deployment Gate, custody is shared between the CDO (continuing to enforce standards) and the Process Owner (accepting operational liability).



Inherits the structural pattern of the IO Capability Stack (Edwards 2006 at bp; Norwegian IO Center 2010–2014; five operators).

Capability by capability

L11 · Strategy. Board mandate and the AI investment case. CDO contributes as C-suite peer.

L10 · Operating Model. Human-above-the-loop. Roles, decision rights, escalation paths. Co-owned CDO/COO; partnership over decision rights and judgment thresholds, not over how coordination happens.

L9 · Agent Capability. Agent runtime and orchestration. Joint custody between the CDO (continuing standards enforcement) and the Process Owner (accepting operational liability). Each retains unilateral halt authority within their domain; reinstatement requires both signatures.

L8 · Agent Connectivity. Protocol surface covering three patterns: discrete tool invocation (MCP), agent-to-agent task delegation (A2A), and continuous context state via subscribe/notify brokers (NGSI-LD), all vendor-neutral open specifications, with runtime identity expressed here (signed agent cards, OAuth 2.1, emerging DID standards). Mesh hub: every governance capability is reached through the same protocols agents use for data. The CDO's procurement test is whether the protocol can be replaced without rewriting the capabilities above.

L7 · Provenance in PROV-O. Machine-readable audit trail. Which data, which rules, which authority produced each agent action. The logbook that makes agent operations auditable, insurable, and reconstructible after the fact.

L6 · Guardrails in SHACL. Structural constraint enforcement against the ontology. Not prompt-engineered or RLHF-learned guardrails. Fire before action regardless of input phrasing.

L5 · Agent Contracts in ODRL. Scope, permitted actions, decision authority, escalation routes. The contractor's statement of work, machine-readable. Defines what the agent may invoke, drawing on L3 ontology types and L4 instances. Agent identity is defined here in contractual terms: which agent this is, what authority it holds, what scope it operates within.

L4 · Knowledge Graph in RDF. CDO-authored organisational graph, federating L1 graphs in place. SPARQL queryable. The operational graph the agent reasons over: competitors can license the same LLM but cannot buy your graph.

L3 · Ontology in OWL / SKOS. Mesh hub at meaning. Federation and extension of community-owned ontologies (BFO, POSC Caesar, CFIHOS, FIBO).

L2 · Data Connectivity. Pipelines, ETL/ELT, message buses. Agents do not reach L2 directly; they reach L8-exposed tools that pull from L2.

L1 · Data + authored KGs. Structured and unstructured data assets, and any domain knowledge graphs grounded in the L3 ontology.

Governance structure

Four zones. Two gates. Source attests, destination approves. One reporting line.

Organizational Zone

Board and C-suite own Capabilities 10 and 11. CDO contributes as peer voice.

The **CDO** sits at the C-suite table as a peer voice on governance and trustworthiness, contributing the investment case for the Stack. At **Capability 10**, the CDO/COO partnership is over decision rights and judgment thresholds, not over how agentic coordination happens at machine speed.

Capability Zone

Capability 9. Joint custody between the CDO and the Process Owner.

After the Deployment Gate fires, the agent enters joint custody. The **CDO** continues to enforce the standards built into the agent (contract, guardrails, provenance). The **Process Owner**, the senior business executive accountable for the operational process the agent operates within, accepts operational liability for outcomes. Each holds unilateral halt authority within their domain; reinstatement requires both signatures. The structural pattern parallels offshore safety convention.

Governance Zone

CDO owns Capabilities 3 through 8 outright.

Meaning capability (L3), knowledge graph (L4), agent contracts (L5), SHACL guardrails (L6), PROV-O provenance (L7), Agent Connectivity (L8), with no co-ownership inside the zone. Both gates operate under one grammar: the role accountable for the source capability attests; the role accountable for the destination governance approves. At the **Ingestion Gate**: the **Data Owner** attests data meets agent-readiness standards, the **CDO** approves admission. At the **Deployment Gate**: the **CDO** attests governance content is complete, the **Process Owner** approves operational acceptance. Two acts per gate, two named people, one audit record. Preventive structural enforcement, not detective monitoring.

Infrastructure Zone

Data Owner content. CIO substrate. CDO standards. Stewards and Custodians operate.

Capabilities 1 and 2 jointly held under DAMA-DMBoK discipline. The **Data Owner** is accountable for what the data means within their **Data Domain**. The **CIO** is accountable for the technical substrate. The **CDO** sets quality, semantic compatibility, and provenance standards both must satisfy before the ingestion gate. **Data Stewards** execute under the Data Owner; **Data Custodians** operate under the CIO. The CDO reports to the CEO, with standards-setting authority cutting across Data Owners, CIO, COO, and Process Owners. No CAIO: that role exists where the CDO mandate stopped at pipelines and dashboards.

Four sovereignties: three links and the ground

Semantic sovereignty (own the ontology) is the precondition for **enforcement sovereignty** (own the constraints): you cannot enforce what you have not defined. Enforcement sovereignty is the precondition for **execution sovereignty** (verify the constraints actually fired in the runtime that ran them): you cannot verify what you have not constrained. Lose any link and every downstream sovereignty collapses to whoever owns the missing capability, almost always the vendor.

These three links rest on a fourth the chain does not name. **Jurisdictional sovereignty** asks whether a third party holds the off-switch: an export-control or sanctions order can disable a model for every customer overnight, and backups do not restore an agent that can no longer reason. Lose a link and the chain collapses to whoever owns it; lose the ground and all three go dark at once. This is why the stack sits on open standards: portability is what lets the ontology, constraints, and provenance be re-established in another jurisdiction. The mandate cannot be bought; it must be held.

The minimum viable ontology

The Stack is a precondition for deployment, not an enterprise-wide mapping programme. Bound scope to one domain: one supplier process, one customer journey, one underwriting workflow. Build the OWL ontology by federating community-owned references (BFO, POSC Caesar, CFIHOS, FIBO), apply the full Stack within that perimeter, and expand as capability matures. **Jim Hendler: *"a little semantics goes a long way."***

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. He advises boards on agentic AI liability and insurability, and is currently available for NED, board-advisory, and CDO appointments focused on corporate AI governance. Companion artefacts: The CDO Office (Mandate) v1.2 and the Vendor Coverage Diagnostic Q2 2026, at fredericverhelst.com/TOI-library.

