The CDO Office

Mandate, Organisation, and Operating Modes

Frédéric Verhelst · Version 1.4 · 16 June 2026

Why a Chief Data Officer

Organisations are deploying AI agents that make decisions, take actions, and interact with customers, suppliers, and regulators. These agents reason over data the organisation holds and act under authority the organisation grants. The question is not whether to deploy. The question is whether anyone in the organisation holds the structural authority to govern what these agents are permitted to know, do, and decide. This is the organisational equivalent of **Keeper's Liability** (*Halterhaftung*) operated at machine tempo. The mandate serves as the fourth line of defence, ensuring the organisation maintains a calculable damage envelope and continuous insurability.

That is the CDO mandate. Not data management. Not analytics. Not dashboards. The structural authority to ensure that agents reason over governed meaning, operate under enforceable contracts, and produce auditable decisions. Without this authority, agent governance is distributed across IT, business units, and vendor platforms with no single point of accountability.

The mandate has a precedent in financial governance. The **CFO** owns the chart of accounts (definitions of every transaction type), the general ledger (the structured record of activity), the internal controls (constraints that fire before unauthorised activity executes), and the audit trail (provenance regulators can examine). The **CDO** mandate carries the same four functions for the agentic stack: ontology, knowledge graph, SHACL constraints, and PROV-O provenance. The structural parallel is not metaphor; it is design.

The mandate also satisfies the standard-of-care question that arrives after any agent-driven loss: did the board provide reasonable governance against the known risk? The mandate is the structural answer.

TRADITIONAL GOVERNANCE *Three lines of defence*	REQUIRED ADDITION *The fourth line*
① **First line** Process Owners. Own and run the agent in the business. ② **Second line** Risk and compliance. Set tolerance, oversee. ③ **Third line** Internal audit. Periodic independent review.	④ **Fourth line. The Capability Stack** CDO-owned, capabilities L3 to L8. Deterministic governance that fires before the agent acts, enforced at two structural gates (Ingestion L2–L3, Deployment L8–L9) with a machine-readable audit trail: reconstructable, insurable, regulator-defensible.
Human tempo · Reviews AFTER action	**Machine speed · Fires BEFORE action**

The first three lines are human and periodic. The fourth is structural and continuous. Independent assurers, for example an accredited certification body, attest the fourth line; they are not the fourth line.

What the CDO owns

The CDO's accountability is defined against the eleven capabilities of the *Agentic AI Capability Stack™*. Four zones of authority, calibrated by capability.

Capability	What the CDO owns	Authority type
L11	Strategy	Peer voice. Board and C-suite territory.
L10	Operating Model	Co-owned with COO. Governance dimension: CDO.
L9	Agent Capability	Joint custody. CDO and Process Owner.
	DEPLOYMENT GATE	CDO holds. No agent deploys without L1 to L8 in place.
L3–L8	Ontology, Knowledge Graph, Agent Contract, Guardrail, Provenance, Agent Connectivity	Full ownership. CDO governs outright.
	INGESTION GATE	CDO holds. No data enters without governed meaning.
L1–L2	Data, Data Connectivity	Standards-setting. Data Owner and CIO jointly accountable.

The reporting line

The **CDO** reports to the **CEO**. The standards-setting authority cuts across **Data Owners**' Data Domains, the **CIO**'s substrate, the **COO**'s operating model, and **Process Owners**' deployments; only the CEO has authority over all of those functions simultaneously. There is no CAIO. The CAIO role exists where the CDO mandate stopped at pipelines and dashboards.

The Process Owner

The mandate names a counterpart role rarely formalised in current organisational design: the **Process Owner**. The Process Owner is the senior business executive accountable for the operational process the agent operates within. Where the **Data Owner** is accountable for what data means within their Data Domain (Customer, Product, Supplier), the Process Owner is accountable for the business process the agent serves (Customer Service, Procurement, Financial Reporting). Both are senior business executive roles, typically at VP or SVP grade; neither is itself C-suite. Best practice is to scope agents narrowly to specific roles within a process rather than to broad mandates.

Data Owner and Process Owner are accountability roles, not necessarily different people. The structural separation is between the act of attestation (source-side) and the act of approval (destination-side). Auditability comes from naming the act.

The Process Owner role is what makes the **Deployment Gate** structurally enforceable. After the gate fires, the agent enters joint custody: the CDO continues to enforce the agent's contract, guardrails, and provenance; the Process Owner holds operational liability for the outcomes the agent produces. Each retains unilateral halt authority within their domain. Reinstatement requires both signatures.

Four sovereignties: three links and the ground

Three sovereignty dimensions operate as a causal chain. **Semantic sovereignty** (owning the ontology on open standards) is the precondition for **enforcement sovereignty** (the CDO can update constraints on the CDO's governance schedule, not the vendor's release schedule): you cannot enforce what you have not defined. Enforcement sovereignty is the precondition for **execution sovereignty** (verifiable evidence that the agent ran the constraints as specified): 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 itself does not name. **Jurisdictional sovereignty** asks whether the platform running the agents is insulated from foreign directives, or whether a third party holds the off-switch. An export-control or sanctions order can compel a provider to disable a model for every customer overnight, and data 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, however well you own them. This is why the stack must sit on open standards: portability is what lets the ontology, the constraints, and the provenance be re-established in another jurisdiction. **The mandate cannot be bought. It must be held.**

The accountability map

Two views of one mandate. The first, below, names who answers for what across the C-suite. The second, overleaf, resolves that authority to the specific acts at each capability and control point. Each function retains its accountability; the CDO sets the standards all must meet.

Function	Accountable for	CDO relationship
Board	Mandate charter, fiduciary oversight, risk appetite	CDO contributes the governance case. Board charters gate authority and sets the risk appetite the deployment thresholds operationalise.
Process Owner	Operational process and outcomes the agent produces	Joint custody of L9. Unilateral halt authority within the process.
CIO	Substrate: databases, pipelines, security	CDO sets provenance and verifiability standards.
COO	Operating model: human-agent roles, escalation	Co-owns L10 governance dimension with CDO.
CRO	Enterprise risk-tolerance frameworks	Co-owns the tolerance frameworks the CDO encodes as SHACL guardrails and operationalises into the minimum maturity deployment thresholds.

Capability and gate RACI

The principal-level RACI across every capability and both structural gates. Each capability ownership act carries a single Accountable principal; the two gates each appear as paired acts, the source attesting and the destination approving, so the separation of duties is named.

Capability	Activity	CIO	Data Owner	CDO	Process Owner	COO	C-suite / Board
L11	Setting board mandate and risk tolerance			C		C	A
L10	Setting cross-process operating model	I		C	C	A	C
L9	Operating the agent and accepting outcomes			C	A		
	Halting the agent for operational failure			I	A		
	Halting the agent for governance breach			A	I		
L8/L9	**Approving operational acceptance**	I	I	C	A		
	Attesting governance content	I	I	A	C		
L8	Defining agent connectivity	C		A	C		
L5–L7	Building agent contracts, guardrails, provenance		C	A	C		
L3–L4	Defining ontology and knowledge graph		C	A	C		
L2/L3	**Approving admission to meaning capability**	I	C	A			
	Attesting data meets agent-readiness	I	A	C			
L2	Establishing data connectivity substrate	A	C	C			
L1	Defining data fitness for the data domain		A	C			

A accountable · C consulted · I informed.
At each gate the source attests and the destination approves, with one principal Accountable for each act and the counterpart Consulted. In operation either named principal may halt the agent unilaterally; reinstatement requires both signatures.
Legal, Risk (CRO), and CISO set the enterprise standards the CDO encodes as guardrails (L5 to L7) and the risk appetite the deployment thresholds operationalise; they are Consulted on the constraint capabilities and at the gates rather than shown as a separate column.
Responsible operational doers (Data Steward, Data Custodian, BU Governance Lead, escalation team) sit in the operational RACI developed in the CDO Playbook, not in this board-level view.

Where to start

The mandate scales with the scope of autonomous operation. Three modes define the progression. The two structural gates apply at every mode; only the delegation scales.

Mode	Scope, and where operational accountability sits
1 · Governed Infrastructure	A few agents inside a business unit. The CDO defines standard governance contracts and holds both gates; the Process Owner selects from pre-approved templates and retains operational accountability for outcomes.
2 · Delegated Governance	One fully agentic workflow, end to end. The Process Owner formally delegates technical governance of the agentic portion to the CDO by charter or board resolution, and retains operational liability for outcomes.
3 · Operational Accountability	A fully agentic, demanned division. The CDO inherits the Process Owner role; CDO, Process Owner, and Division Head become a single role-holder. Both gates still fire, the audit acts remaining distinct.

The organisation under the CDO

The CDO office is a governance function, not a data team with a new title. Seven capability groups report to the CDO. Four build and operate the meaning capabilities (L3 to L9). One runs assurance across the audit chain, structurally independent from Governance Operations so the gate operators are not auditing themselves. Two work the data foundation and the Ingestion Gate (L1 to L3): one governs what data means and stewards it; the other assures it is fit for agents to reason over.

Capability group	What it does	Capability
Ontology Engineering	Formal ontologies (OWL), controlled vocabularies (SKOS). Aligned to BFO, POSC Caesar, CFIHOS, FIBO.	**L3**
Knowledge Graph Architecture	Organisational knowledge graph (RDF, SPARQL). Grounded in the L3 ontology.	**L4**
Governance Operations	Agent contracts (ODRL), guardrails (SHACL), provenance (PROV-O). Operates both gates. Continuous L9 runtime monitoring supporting halt authority.	**L5–L9**
Agent Integration	Agent connectivity protocols (MCP, A2A). Deployment governance. Uniform protocol access.	**L8–L9**
Governance Assurance	Audit-chain analysis across agents and over time. Drift detection, asymmetry surfacing, near-miss pattern reporting. Independent from Governance Operations; feeds board oversight.	**L5–L11**
Data Governance & Stewardship	Data policy, ownership, semantic compatibility, and provenance standards at source. Dotted-line to Data Stewards.	**L1–L2**
Data Quality Management	Sets agent-readiness quality standards (completeness, conformance, freshness) and runs the fitness checks the Ingestion Gate attestation rests on. Guards meaning against agent write-back degradation across the chain. Works with Data Governance towards Data Owners, Stewards, and custodians.	**L1–L3**

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. As external executive advisor he wrote the digital strategy and value case for the Tyra Redevelopment Final Investment Decision, the largest single capital investment on the Danish Continental Shelf (a Mærsk Oil joint venture with Shell and Chevron, later operated by TotalEnergies), reporting to the VP Tyra Redevelopment; he then led digitalisation through the Mærsk-to-TotalEnergies transition and became Head of Data Office at TotalEnergies EP Danmark, owning the enterprise data mandate, before most recently bringing agentic AI into safety-critical maritime operations. He advises boards on agentic AI liability and insurability, and partners with C-suites on the Chief Data Officer mandate this document sets out. He is 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). For vendor coverage: the Vendor Coverage Diagnostic. For the framework argument: Article 3b; for the operating modes, liability, and delegation framework: Article 3c. Both at theontologyimperative.substack.com. All artefacts at fredericverhelst.com/TOI-library. Licensed CC BY-ND 4.0 with attribution.