Chief Data Officer

Role Specification · Companion to the Mandate

Version 2.1 · Modes 1 and 2 · 16 June 2026

Purpose of the role

This is the role specification for the **Chief Data Officer (CDO)**, the companion to *The CDO Office: Mandate, Organisation, and Operating Modes*. The Mandate sets out the governance structure; this document specifies the role that holds it: what it is accountable for, who fills it, and how it scales. It is written as a standard for the role rather than a notice for a particular vacancy.

The role exists because AI agents act under authority the organisation grants and reason over data it holds. The authority to govern what those agents are permitted to know, do, and decide cannot be split across IT, the business units, and vendor platforms without opening an accountability gap that no other executive can close. The argument is made in full in the Mandate and in Articles 3b and 3c; what follows is the role it implies.

Reporting line and scope

Reports to	Chief Executive Officer. The standards-setting authority cuts across Data Owners, the CIO, the COO, and Process Owners; only the CEO holds authority over all of those functions at once. There is no Chief AI Officer above the role.
Direct reports	Heads of the seven capability groups that make up the CDO office, named under The organisation the role leads on page 2. The full structure and RACI are set out in the Mandate.
Cross-functional partners	Data Owners across data domains; Process Owners across business processes; CIO; COO; General Counsel; Chief Risk Officer.
Board interface	Member of, or standing presenter to, the board audit and risk committee. Standard-of-care attestations on agent governance feed board oversight.
Tenure	Indefinite. The CDO is a permanent enterprise function, not a transformation or fixed-term role.

Key accountabilities and decision rights

The role carries four accountabilities that cannot be partially delegated. Together they constitute the fourth line of defence: deterministic enforcement that fires before an agent acts, at machine tempo, alongside the three traditional lines (operational management, risk and compliance, internal audit) that operate at human tempo. The structure that makes each one enforceable is specified in the Mandate and the Capability Stack; what follows is what the role-holder answers for and decides.

Meaning and connectivity	Accountable that the enterprise reasons and acts through a governed meaning capability on open standards it owns, rather than a vendor's proprietary equivalent. Decides what is admitted to that capability and which standards it rests on.
The two control gates	Holds the CDO side of both gates. At the **Ingestion Gate**, approves data into governed meaning on the Data Owner's attestation. At the **Deployment Gate**, attests that governance content is complete and scoped before the Process Owner accepts the agent into the business.
Halt authority	Holds unilateral authority to halt any agent for a governance breach, in parallel with the Process Owner's authority to halt for operational failure. Reinstatement requires both signatures.
Audit and standard of care	Accountable that every agent decision leaves machine-readable, vendor-independent audit evidence, reconstructable without the platform. This is the structural answer to the standard-of-care question after any agent-driven loss.

The organisation the role leads

The CDO office is a governance function, not a data team with a new title. It is made up of seven capability groups. Ontology Engineering (L3) and Knowledge Graph Architecture (L4) build the meaning capability. Governance Operations (L5 to L9) and Agent Integration (L8 to L9) operate the gates and agent connectivity. Governance Assurance (L5 to L11) runs the audit chain, structurally independent of the gate operators so they are not auditing themselves. Data Governance and Stewardship (L1 to L2) and Data Quality Management (L1 to L3) work the data foundation the Ingestion Gate rests on. The full structure, capability scope, and RACI are set out in the Mandate.

Required background and experience

Senior leadership trajectory of 15 or more years across data, governance, and large-scale operational or transformation programmes, including executive-level accountability (Head of, VP, or C-1) for an enterprise-scale data or governance remit. A track record of carrying board-facing governance responsibility in regulated, high-liability, or safety-critical settings.

Architectural fluency in the W3C semantic stack (OWL, SHACL, PROV-O, RDF, SPARQL). This is not a delegable competency. The role-holder must engage at architectural depth with ontology engineers, vendor architects, and external auditors; reading semantic specifications and reasoning about constraints is part of the day-to-day role.

Cross-functional executive presence. The ability to engage with Process Owners, Data Owners, CIO, COO, General Counsel, and Chief Risk Officer as peer, not as adviser. The mandate carries veto authority at the two gates; the role-holder must be able to exercise it against operational pressure when required.

Vendor governance experience. Demonstrated ability to negotiate semantic, enforcement, execution, and jurisdictional sovereignty into platform contracts as deal-stoppers, and familiarity with the contractual criteria that prevent sovereignty collapsing to the vendor.

Equivalent senior backgrounds

The first generation of agentic-AI-capable CDOs will come from a range of adjacent senior backgrounds, not from prior tenure in a role the structure has only recently made coherent. Recognised entry paths include Heads of Data Office, VPs of Data and Analytics with cross-functional accountability, Directors of Integrated Operations with data architecture remits, programme leaders on enterprise data or governance transformation, senior data architects with explicit governance accountability, and CDOs from adjacent sectors making lateral transitions. What unifies them is direct accountability for enterprise data architecture at scale, combined with architectural depth in semantic technologies. **Prior CDO tenure is one path among these, not a prerequisite.**

Strongly preferred

Architectural depth on at least one production knowledge graph or ontology deployment at enterprise scale. Experience with insurance and audit frameworks for AI liability (D&O and professional indemnity calibrations). Industrial domain depth in the hiring organisation's sector. Familiarity with offshore safety, financial controls, or other dual-key operational governance conventions, the parallel to the joint-custody pattern between CDO and Process Owner at L9.

How the role scales: Mode 1 to Mode 2

The role scales materially in scope, team size, and KPI orientation between Modes 1 and 2, though the accountabilities and reporting line do not change. Both gates apply at every mode; only the delegation scales. A CDO who builds successful Mode 1 infrastructure grows into the Mode 2 role; the role does not change identity.

Dimension	Mode 1: Governed Infrastructure	Mode 2: Delegated Governance
Scope	A few agents inside a single business unit. The foundational ontology is under construction. The CDO defines standard governance contracts and holds both gates; the Process Owner selects from pre-approved templates and retains operational accountability for outcomes.	One fully agentic workflow, end to end, the pattern extending to further workflows as they mature. 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.
Team size	10 to 15. Ontology Engineering and Governance Operations primary; other capability groups in formation.	25 to 40. All seven capability groups operational. Governance Assurance structurally independent.
Primary KPIs	Number of vetted agent templates; Ingestion Gate throughput; Deployment Gate approval rate; zero unauthorised deployments.	Workflow governance maturity; charter completeness; halt-and-restart cycles; provenance audit coverage; insurance posture.
Time allocation	About 60% infrastructure (ontology, knowledge graph, gates); about 30% governance operations; about 10% board and C-suite engagement.	About 40% governance operations; about 30% Process Owner strategic engagement; about 20% board and C-suite; about 10% infrastructure evolution.
Transition	18 to 24 months typical to mature into Mode 2, contingent on agent-footprint growth.	Indefinite for many processes. Mode 3 emerges only where divisions become demanned.

Risk, liability, and insurability

The role carries explicit **governance accountability**, not operational accountability. The CDO answers for whether structural enforcement was complete, scoped, and operating at the time of any agent-driven loss event; the CDO does not answer for the operational outcomes that follow a gate fire. Where Article 26 of the EU AI Act, the 2024 revision of the EU Product Liability Directive, US *Caremark* precedents, or comparable frameworks elsewhere create operator-level liability for AI-driven outcomes, that liability flows to the Process Owner under post-gate joint custody, not to the CDO.

The CDO is accountable for **evidencing that the structural controls were in place** at the time of the loss event: the governance-content attestation at deployment, the provenance audit chain, and the operation of the halt authority. That evidence must be reconstructable from the audit chain (PROV-O) without reliance on the vendor. D&O coverage and professional indemnity calibrations for the role should reflect this scope. The role is structurally insurable; an uninsurable CDO mandate is a sign the mandate is not yet structurally enforceable.

What this role is not

The boundaries matter as much as the remit. The role is not a Chief AI Officer under a different name; the CDO governs the meaning and the controls agents act through, not the AI strategy or the model portfolio. It is not a data team rebranded; it is a control function with veto authority at two gates. It carries governance accountability, not operational accountability; the CDO answers for whether enforcement was complete and operating, the Process Owner for the outcomes that follow. It is not a transformation or fixed-term role; it is a permanent enterprise function. And it does not require prior tenure in the role itself: the requirement is architectural depth and senior governance accountability, not a previous CDO title.

About this specification

This role specification is the companion to *The CDO Office: Mandate, Organisation, and Operating Modes*. The Mandate sets out the governance structure, the four sovereignties, the capability and gate RACI, and the organisation; this document specifies the role that holds it. Both describe the Chief Data Officer at organisational Modes 1 (Governed Infrastructure) and 2 (Delegated Governance). The Mode 3 variant (Operational Accountability for a demanned division) is a categorically different role, described in a separate artefact.

Canonical references: the Agentic AI Capability Stack™ (v3) and The CDO Office Mandate; Articles 3b and 3c at theontologyimperative.substack.com. All artefacts at fredericverhelst.com/TOI-library. Licensed CC BY-ND 4.0 with attribution.