

SAP Business Data Cloud Enterprise Governance Framework

A Comprehensive Enterprise Governance Model for Data Products, Semantics, Ownership, Security, Quality, Lineage, AI Readiness, and Business Value

Sanjeeve Kumar Gajadi*

*(HCL Technologies, Bengaluru, Karnataka, India)

Email: sanjeevekumar.g@hcltech.com

Abstract:

SAP Business Data Cloud introduces an enterprise data foundation that connects SAP and non-SAP information to trusted business semantics, analytics, planning, and Artificial Intelligence. Realizing value from this platform requires a governance model that coordinates data ownership, data products, semantic consistency, quality, lineage, security, lifecycle, access, and consumption across organizational boundaries. This paper proposes a SAP Business Data Cloud Enterprise Governance Framework integrating enterprise architecture, data governance, SAP Datasphere, SAP HANA Cloud, SAP Analytics Cloud, metadata, data products, AI readiness, and Responsible AI. The framework defines governance domains, decision rights, operating roles, quality controls, access policies, data product lifecycle stages, observability, and measurable KPIs/KRIs. It enables organizations to move from fragmented data management toward governed, reusable, business-aligned data products that support analytics and AI while preserving compliance, traceability, and enterprise trust.

Keywords — *SAP Business Data Cloud, SAP Datasphere, Data Governance, Data Products, Semantic Layer, Data Quality, Lineage, SAP HANA Cloud, AI Readiness, Enterprise Architecture*

I. INTRODUCTION

Enterprise data environments frequently contain duplicated extracts, inconsistent business definitions, unclear ownership, and disconnected governance. SAP Business Data Cloud creates an opportunity to establish a governed business data foundation across analytics and AI.

Governance should be designed as an operating model that connects business ownership, technology architecture, semantic management, security, and measurable data-product value.

II. GOVERNANCE OBJECTIVES

The framework aims to improve trust, reuse, discoverability, quality, compliance, lineage, and business accountability while reducing duplicate data pipelines and uncontrolled copies.

Governance must support agility. Controls should be automated and embedded into platform workflows so teams can deliver data products quickly without sacrificing standards.

III. DATA DOMAIN AND OWNERSHIP MODEL

Business domains should own authoritative definitions and critical data products. Each data domain requires accountable owners, stewards, technical custodians, and consumer responsibilities.

Ownership should include decisions on definitions, quality thresholds, access, lifecycle, and remediation rather than only documenting names in a catalog.

IV. DATA PRODUCT GOVERNANCE

A data product should have a defined purpose, owner, consumers, service level, schema, semantic model, quality rules, lineage, access classification, and lifecycle status.

Products should be discoverable, reusable, versioned, and measured for adoption and value. Deprecated or duplicate products should be retired systematically.

V. SEMANTIC GOVERNANCE

Trusted analytics and AI require consistent business semantics. Measures, dimensions, hierarchies, units, and calculation logic should be governed and reused across data products.

Semantic changes should be version-controlled, impact-assessed, and communicated to consumers because seemingly small definition changes can alter executive reporting and AI outcomes.

VI. DATA QUALITY MANAGEMENT

Quality controls should cover completeness, validity, accuracy, consistency, timeliness, uniqueness, and referential integrity. Critical data elements should have explicit thresholds and accountable remediation.

Quality observability should identify recurring defects at source rather than relying on downstream cleansing.

VII. LINEAGE AND METADATA

Technical and business lineage should show where data originates, how it is transformed, which products consume it, and which reports or AI use cases depend on it.

Metadata should connect business definitions, owners, classifications, quality indicators, policies, and technical assets to improve impact analysis and auditability.

VIII. SECURITY AND ACCESS GOVERNANCE

Access should follow least privilege, data classification, purpose limitation, jurisdiction, and business role. Sensitive information may require masking, row-level restrictions, or segregated spaces.

Policies should apply consistently across storage, semantic models, analytics, data sharing, and AI consumption.

IX. SAP DATASPHERE AND PLATFORM GOVERNANCE

SAP Datasphere spaces, connections, models, data flows, and business layers should follow naming, ownership, transport, development, and lifecycle standards.

SAP HANA Cloud and other platform services should use controlled capacity, backup, monitoring, and security configurations aligned with enterprise architecture.

X. AI READINESS AND RESPONSIBLE AI

Data products used for AI should have stronger requirements for provenance, freshness, bias assessment, access control, and suitability for the intended task.

Governance should record which AI services consume each data product and enable rapid impact analysis when source data or semantics change.

XI. OPERATING MODEL

A data governance council should coordinate enterprise standards while domain teams retain

accountability for business meaning and product outcomes.

Enterprise architecture, security, legal, privacy, data engineering, analytics, and AI governance functions should participate according to risk and regulatory relevance.

XII. KPIS AND KRIS

KPIs can include certified data-product adoption, quality pass rate, lineage coverage, reuse rate, issue resolution time, and reduction in duplicate pipelines.

KRIs can include unauthorized access attempts, stale products, broken lineage, critical quality breaches, and unowned high-impact data assets.

XIII. IMPLEMENTATION ROADMAP

Organizations can begin by inventorying critical data assets, identifying priority domains, defining ownership, and establishing a small set of governed data products.

Governance can then expand through metadata automation, quality observability, policy-as-code, semantic standards, and portfolio management.

XIV. CONCLUSION

SAP Business Data Cloud can provide an enterprise foundation for analytics and AI when data is managed as governed products rather than isolated technical assets.

The proposed framework connects ownership, semantics, quality, lineage, security, platform governance, and AI readiness into a scalable operating model for trusted enterprise data.

REFERENCES

- [1] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.
- [2] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems.
- [3] ISO 31000:2018, Risk management — Guidelines.
- [4] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.
- [5] National Institute of Standards and Technology, AI RMF Generative Artificial Intelligence Profile, 2024.
- [6] National Institute of Standards and Technology, SP 800-207: Zero Trust Architecture, 2020.
- [7] The Open Group, TOGAF Standard, 10th Edition, 2022.
- [8] ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2019.
- [9] SAP SE, SAP Business Technology Platform Documentation.
- [10] SAP SE, SAP AI Core and SAP AI Launchpad Documentation.

- [11] SAP SE, SAP Integration Suite Documentation.
- [12] SAP SE, SAP HANA Cloud Documentation.
- [13] SAP SE, SAP Cloud Identity Services Documentation.
- [14] SAP SE, SAP Cloud ALM Documentation.
- [15] SAP SE, SAP Business Data Cloud and SAP Datasphere Documentation.
- [16] OWASP Foundation, OWASP Top 10 for Large Language Model Applications.
- [17] MITRE, ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems.
- [18] OECD, Recommendation of the Council on Artificial Intelligence.
- [19] IEEE, Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems.
- [20] DAMA International, DAMA-DMBOK2: Data Management Body of Knowledge, 2017.

AUTHOR BIOGRAPHY

Sanjeeve Kumar Gajadi is an SAP Enterprise Architect and Lead Consultant with extensive experience in SAP Datasphere, SAP Business Data Cloud, SAP HANA, SAP Analytics Cloud, enterprise architecture, data governance, integration, and AI-enabled transformation. His professional interests include data products, semantic governance, enterprise data architecture, and Responsible AI.

ACKNOWLEDGMENT

The author acknowledges the contributions of enterprise architecture practitioners, international standards bodies, AI governance communities, security researchers, and SAP documentation teams whose published guidance informed the concepts synthesized in this paper.