

GETDQI FREE RESOURCE



Data Quality Index: The Standard

The normative reference for data quality and AI governance maturity

Version 1.0 | May 2026 | 12 domains | 112 measures | 6-level maturity model

Designed for teams building trustworthy data, AI readiness, and measurable governance capability.

1. Preamble

1.1 Scope

This document is the DQI Standard: the normative reference for the Q4IT Data Quality Index (DQI) ecosystem. It defines what organisations are expected to achieve at each maturity level across 12 governance domains and 112 individual measures. It is the reference against which DQI assessments are conducted, DQI certifications are awarded, and DQI education content is developed.

The Standard applies to all organisations that undergo a DQI assessment, regardless of sector, size, or geography. Sector-specific guidance is provided within measure descriptors where regulatory obligations differ by sector. The Standard does not replace applicable law or regulation - it provides a governance framework that is aligned to and supports compliance with the normative references listed in Section 1.3.

1.2 How to Use This Standard

The Standard is structured as follows:

- Section 1 (this section): scope, normative references, definitions, version governance, and the maturity model.
- Sections 2-13: one section per domain, each containing the domain purpose statement, regulatory context, and full measure specifications.
- Annex A: alignment matrix - DQI measures mapped to ISO 8000.
- Annex B: alignment matrix - DQI measures mapped to ISO/IEC 42001.
- Annex C: alignment matrix - DQI measures mapped to EU AI Act obligations.
- Annex D: alignment matrix - DQI measures mapped to GDPR articles.

When conducting a DQI assessment, assessors score each measure on a scale of 0-5 using the level descriptors in this Standard. Each descriptor defines what the organisation must demonstrate to achieve that level. Descriptors are written as observable states. Where a descriptor lists multiple characteristics, the organisation must demonstrate all of them to achieve that level. A partial demonstration is scored at the level below.

1.3 Normative References

The following standards and regulations are normative references for this Standard. Where this Standard cross-references a specific clause, that clause is cited. Where no clause is cited, the reference applies in general.

Reference	Full Title	Relevance
ISO 8000-8:2015	Data quality - Part 8: Information and data quality: Concepts and measuring	Primary spine for data quality principles, dimensions, and management. Domains 1-4, 12.
ISO 8000-61:2016	Data quality - Part 61: Data quality management: Process reference model	Data quality process management. Domains 3, 4, 6.
ISO 8000-110:2009	Data quality - Part 110: Master data: Exchange of characteristic data	Data provenance and lineage. Domains 3, 5.
ISO/IEC 42001:2023	Artificial intelligence - Management system	AI management system requirements. Domains 5, 6, 11.
EU AI Act (Regulation 2024/1689)	Regulation on Artificial Intelligence	EU AI system risk classification, governance, and compliance obligations. Domains 5, 6, 7, 9.
GDPR (Regulation 2016/679)	General Data Protection Regulation	Personal data governance, consent, retention, and security. Domains 7, 10.
UK GDPR / DPA 2018	UK General Data Protection Regulation and Data Protection Act 2018	UK equivalent of GDPR. Applied to UK operations.
NIST AI RMF (2023)	NIST Artificial Intelligence Risk Management Framework	Supplementary AI risk management reference. Domain 5.
DAMA DMBOK v2	Data Management Body of Knowledge	Supplementary data management reference. Domains 1, 2, 8, 9.

1.4 Definitions

The following terms are used throughout this Standard with the definitions given below.

Term	Definition
Data Asset	Any data resource - dataset, database, data feed, report, or AI model - that has recognised value to the organisation.
Data Owner	A named individual formally accountable for a defined data asset, including its quality, access governance, and lifecycle.
Data Steward	A named individual responsible for the day-to-day governance, quality monitoring, and issue management of a defined data asset.
Critical Data Asset	A data asset whose quality directly affects operational decisions, regulatory compliance, financial reporting, or AI system outputs.
Maturity Level	A defined stage of governance capability, described on a scale of 0 (Non-Existent) to 5 (Optimised) in this Standard.
DQI Score	The numerical output of a DQI assessment, calculated as the weighted average of domain scores. Each domain score is the average of its measure scores expressed as a percentage of the maximum possible score.
AI System	A machine-based system designed to operate with varying degrees of autonomy and that may exhibit adaptiveness after deployment (per EU AI Act definition).
High-Risk AI System	An AI system classified as high-risk under Annex III of the EU AI Act.
Training Data	Data used to train an AI model, including data used for validation and testing.
Fitness for Purpose	The degree to which a data asset meets the quality requirements of its intended use case.
Provenance	The documented origin, transformation history, and chain of custody of a data asset.
Data Contract	A formal agreement between a data producer and data consumer defining quality SLAs, freshness requirements, access terms, and change notification obligations.

1.5 The Maturity Model

All 112 measures in this Standard are scored on the following six-level maturity scale. Level descriptors for each measure are specific and observable. This table provides the general characteristics of each level.

Level	Name	General Characteristics	Typical Evidence
0	Non-Existent	No awareness, no policy, no process, and no control. Absence is confirmed by the assessor as a finding.	None. Assessor documents absence.
1	Ad Hoc	Awareness exists. Some activity occurs but it is informal, undocumented, and person-dependent. Outcomes are unpredictable.	Informal documents, verbal acknowledgement, individual knowledge.
2	Repeatable	Basic processes exist and recur. Outcomes are inconsistent but the approach is recognisable. Some documentation.	Partial documentation, inconsistent application, individual ownership.
3	Defined	Processes are documented, standardised, and consistently applied. Governance is in place. Outcomes are predictable within scope.	Formal policy, process documentation, evidence of consistent application.
4	Managed	Processes are measured. Thresholds are defined and monitored. Deviations are detected and acted on systematically.	Metrics, dashboards, exception reports, active management evidence.
5	Optimised	Continuous improvement is embedded. Benchmarking and proactive adaptation are standard practice. Best-in-class.	Improvement records, benchmark comparisons, industry contribution.

1.6 Domain Weighting

All 12 domains are weighted equally at 8.33% of the total DQI score. Equal weighting is deliberate: it preserves the integrity of the radar chart visualisation and avoids implying a hierarchy of importance that may not apply across all sectors and contexts. Domain weighting may be adjusted for sector-specific assessment variants in future versions of this Standard, subject to the version governance process in Section 1.7.

1.7 Version Governance

This Standard is version-controlled and subject to an annual review cycle. The following governance applies:

- Major versions (e.g. v1.0 to v2.0): structural changes including addition or removal of domains or measures. Requires full review board approval. Organisations mid-certification cycle have 12 months to re-assess against the new version.
- Minor versions (e.g. v1.0 to v1.1): clarifications, corrections, and additions to measure descriptors that do not change the scoring structure. Effective immediately on publication.
- A change log is published with each version. All previous versions are archived and available.
- The review board comprises Q4IT principals and invited external practitioners. Review board membership is published on the Q4IT website.

2. Domain D1: Data Value & Alignment

Domain	Data Value & Alignment
Domain ID	D1
Weighting	8.33%
Measures	8
Purpose	Data has value only when it is intentionally aligned to the outcomes the organisation is trying to achieve. This domain governs whether data assets, data initiatives, and data quality investments are explicitly connected to business strategy, operational requirements, and AI use cases. Organisations with weak value and alignment governance invest in the wrong data, build the wrong capabilities, and deploy AI on foundations that do not match their actual needs. Strong performance in this domain means data quality effort is directed where it produces measurable return.
Regulatory Context	ISO 8000-8 Clause 4 (context of the organisation). ISO 42001 Clause 4.1 (understanding the organisation). No direct EU AI Act obligation, but Article 9 (risk management) and Article 10 (data governance) assume alignment of data to AI purpose.

D1.1 - Business Glossary

Measure ID	Measure Name	Governs	Normative References
D1.1	Business Glossary	Whether a maintained, accessible, and authoritative glossary of business terms exists and is linked to data assets, reports, and AI model inputs.	ISO 8000-8 DAMA DMBOK Ch.2
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No glossary exists. Terms are undefined or understood only by individuals.	No glossary exists. Terms are undefined or understood only by individuals.	No glossary exists. Terms are undefined or understood only by individuals.
1 - Ad Hoc	Informal glossary exists in documents, wikis, or spreadsheets. Not maintained. No formal ownership. Coverage is partial and inconsistent.	Informal glossary exists in documents, wikis, or spreadsheets. Not maintained. No formal ownership. Coverage is partial and inconsistent.	Informal glossary exists in documents, wikis, or spreadsheets. Not maintained. No formal ownership. Coverage is partial and inconsistent.
2 - Repeatable	A glossary exists with definitions for major business terms. Maintained by a named owner. Not systematically linked to data assets or AI model inputs.	A glossary exists with definitions for major business terms. Maintained by a named owner. Not systematically linked to data assets or AI model inputs.	A glossary exists with definitions for major business terms. Maintained by a named owner. Not systematically linked to data assets or AI model inputs.
3 - Defined	A maintained glossary covers all critical business domains. Definitions are agreed across business units. Linked to data assets in a catalog. Reviewed on a defined cycle.	A maintained glossary covers all critical business domains. Definitions are agreed across business units. Linked to data assets in a catalog. Reviewed on a defined cycle.	A maintained glossary covers all critical business domains. Definitions are agreed across business units. Linked to data assets in a catalog. Reviewed on a defined cycle.
4 - Managed	The glossary is actively governed. Changes follow a formal approval process. Coverage is measured. Linkage to data assets, reports, and AI model inputs is verified and complete for all critical assets.	The glossary is actively governed. Changes follow a formal approval process. Coverage is measured. Linkage to data assets, reports, and AI model inputs is verified and complete for all critical assets.	The glossary is actively governed. Changes follow a formal approval process. Coverage is measured. Linkage to data assets, reports, and AI model inputs is verified and complete for all critical assets.
5 - Optimised	The glossary is the authoritative reference across the enterprise. It drives data contract definitions, AI feature specifications, and API schemas. Gaps are proactively identified and closed. Contributes to industry or standards bodies.	The glossary is the authoritative reference across the enterprise. It drives data contract definitions, AI feature specifications, and API schemas. Gaps are proactively identified and closed. Contributes to industry or standards bodies.	The glossary is the authoritative reference across the enterprise. It drives data contract definitions, AI feature specifications, and API schemas. Gaps are proactively identified and closed. Contributes to industry or standards bodies.

D1.2 - Use Case Linkage

Measure ID	Measure Name	Governs	Normative References
D1.2	Use Case Linkage	Whether critical reports, AI models, and data products are formally linked to documented business KPIs and strategic objectives.	ISO 8000-8 Clause 4 ISO 42001 Clause 4.1
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No linkage between data assets or AI models and business KPIs. Data produced without reference to outcomes.	No linkage between data assets or AI models and business KPIs. Data produced without reference to outcomes.	No linkage between data assets or AI models and business KPIs. Data produced without reference to outcomes.
1 - Ad Hoc	Some reports are informally associated with business objectives. Linkage is verbal or implied. Not documented.	Some reports are informally associated with business objectives. Linkage is verbal or implied. Not documented.	Some reports are informally associated with business objectives. Linkage is verbal or implied. Not documented.
2 - Repeatable	Major dashboards and reports are linked to KPIs. AI models are not formally linked. Linkage is documented but not verified.	Major dashboards and reports are linked to KPIs. AI models are not formally linked. Linkage is documented but not verified.	Major dashboards and reports are linked to KPIs. AI models are not formally linked. Linkage is documented but not verified.
3 - Defined	All critical reports and AI models are formally linked to documented KPIs. Linkage is recorded in a data catalog or register. Reviewed annually.	All critical reports and AI models are formally linked to documented KPIs. Linkage is recorded in a data catalog or register. Reviewed annually.	All critical reports and AI models are formally linked to documented KPIs. Linkage is recorded in a data catalog or register. Reviewed annually.
4 - Managed	Linkage is complete, verified, and actively maintained. New data products require KPI linkage before approval. AI model purpose is formally documented against strategic objectives.	Linkage is complete, verified, and actively maintained. New data products require KPI linkage before approval. AI model purpose is formally documented against strategic objectives.	Linkage is complete, verified, and actively maintained. New data products require KPI linkage before approval. AI model purpose is formally documented against strategic objectives.
5 - Optimised	Use case linkage drives resource allocation decisions. Orphaned data products are identified and retired. Linkage analysis informs AI strategy and investment prioritisation.	Use case linkage drives resource allocation decisions. Orphaned data products are identified and retired. Linkage analysis informs AI strategy and investment prioritisation.	Use case linkage drives resource allocation decisions. Orphaned data products are identified and retired. Linkage analysis informs AI strategy and investment prioritisation.

D1.3 - ROI Measurement

Measure ID	Measure Name	Governs	Normative References
D1.3	ROI Measurement	Whether an agreed methodology exists for quantifying the return on investment from data quality and data governance initiatives.	ISO 8000-8 DAMA DMBOK Ch.1
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No attempt to measure ROI from data or AI initiatives. Investment decisions made without financial justification.	No attempt to measure ROI from data or AI initiatives. Investment decisions made without financial justification.	No attempt to measure ROI from data or AI initiatives. Investment decisions made without financial justification.
1 - Ad Hoc	ROI discussed informally. No agreed methodology. Estimates made ad hoc by individual teams.	ROI discussed informally. No agreed methodology. Estimates made ad hoc by individual teams.	ROI discussed informally. No agreed methodology. Estimates made ad hoc by individual teams.
2 - Repeatable	ROI is estimated for major data initiatives using an informal but consistent approach. Not applied across all initiatives.	ROI is estimated for major data initiatives using an informal but consistent approach. Not applied across all initiatives.	ROI is estimated for major data initiatives using an informal but consistent approach. Not applied across all initiatives.
3 - Defined	An agreed ROI methodology exists and is applied to all significant data and AI initiatives. Results reported to senior leadership on a defined cadence.	An agreed ROI methodology exists and is applied to all significant data and AI initiatives. Results reported to senior leadership on a defined cadence.	An agreed ROI methodology exists and is applied to all significant data and AI initiatives. Results reported to senior leadership on a defined cadence.
4 - Managed	ROI is tracked pre- and post-initiative. Actual versus forecast is measured. Methodology is refined based on outcomes. Data quality cost of poor quality (COPQ) is quantified.	ROI is tracked pre- and post-initiative. Actual versus forecast is measured. Methodology is refined based on outcomes. Data quality cost of poor quality (COPQ) is quantified.	ROI is tracked pre- and post-initiative. Actual versus forecast is measured. Methodology is refined based on outcomes. Data quality cost of poor quality (COPQ) is quantified.
5 - Optimised	ROI measurement is embedded in investment governance. Data quality value is a standing item in business case review. Benchmarked against peer organisations.	ROI measurement is embedded in investment governance. Data quality value is a standing item in business case review. Benchmarked against peer organisations.	ROI measurement is embedded in investment governance. Data quality value is a standing item in business case review. Benchmarked against peer organisations.

D1.4 - Stakeholder Satisfaction

Measure ID	Measure Name	Governs	Normative References
D1.4	Stakeholder Satisfaction	Whether satisfaction with data products and data services is measured and whether findings are acted upon.	ISO 8000-8 DAMA DMBOK Ch.1
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No measurement of stakeholder satisfaction with data.	No measurement of stakeholder satisfaction with data.	No measurement of stakeholder satisfaction with data.
1 - Ad Hoc	Satisfaction captured informally through conversations. No formal survey or measurement.	Satisfaction captured informally through conversations. No formal survey or measurement.	Satisfaction captured informally through conversations. No formal survey or measurement.
2 - Repeatable	Periodic satisfaction surveys conducted. Results reviewed but actions not systematically tracked.	Periodic satisfaction surveys conducted. Results reviewed but actions not systematically tracked.	Periodic satisfaction surveys conducted. Results reviewed but actions not systematically tracked.
3 - Defined	Structured satisfaction measurement in place. Results reviewed by data leadership. Actions tracked to resolution.	Structured satisfaction measurement in place. Results reviewed by data leadership. Actions tracked to resolution.	Structured satisfaction measurement in place. Results reviewed by data leadership. Actions tracked to resolution.
4 - Managed	Satisfaction metrics trend over time. Net Promoter Score or equivalent applied to data products. Dissatisfaction triggers formal review.	Satisfaction metrics trend over time. Net Promoter Score or equivalent applied to data products. Dissatisfaction triggers formal review.	Satisfaction metrics trend over time. Net Promoter Score or equivalent applied to data products. Dissatisfaction triggers formal review.
5 - Optimised	Satisfaction drives data product roadmap. Results benchmarked against peers. Satisfaction is a key metric in data leadership performance objectives.	Satisfaction drives data product roadmap. Results benchmarked against peers. Satisfaction is a key metric in data leadership performance objectives.	Satisfaction drives data product roadmap. Results benchmarked against peers. Satisfaction is a key metric in data leadership performance objectives.

D1.5 - Requirements Traceability

Measure ID	Measure Name	Governs	Normative References
D1.5	Requirements Traceability	Whether business and regulatory requirements are traced end-to-end through to datasets, pipelines, and AI model inputs.	ISO 8000-8 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No traceability. Requirements exist separately from data assets. Connection is implicit at best.	No traceability. Requirements exist separately from data assets. Connection is implicit at best.	No traceability. Requirements exist separately from data assets. Connection is implicit at best.
1 - Ad Hoc	Requirements are informally associated with some data assets. Traceability depends on individual knowledge.	Requirements are informally associated with some data assets. Traceability depends on individual knowledge.	Requirements are informally associated with some data assets. Traceability depends on individual knowledge.
2 - Repeatable	Requirements are traced for major projects using a consistent method. Not applied universally. Traceability is not maintained after delivery.	Requirements are traced for major projects using a consistent method. Not applied universally. Traceability is not maintained after delivery.	Requirements are traced for major projects using a consistent method. Not applied universally. Traceability is not maintained after delivery.
3 - Defined	Requirements traceability is applied to all significant data and AI initiatives. Documented and maintained in a register or tool. Reviewed at delivery and at defined intervals.	Requirements traceability is applied to all significant data and AI initiatives. Documented and maintained in a register or tool. Reviewed at delivery and at defined intervals.	Requirements traceability is applied to all significant data and AI initiatives. Documented and maintained in a register or tool. Reviewed at delivery and at defined intervals.
4 - Managed	End-to-end traceability is maintained from business requirement through to data asset, pipeline, and AI model input. Changes to requirements trigger impact assessment on downstream assets.	End-to-end traceability is maintained from business requirement through to data asset, pipeline, and AI model input. Changes to requirements trigger impact assessment on downstream assets.	End-to-end traceability is maintained from business requirement through to data asset, pipeline, and AI model input. Changes to requirements trigger impact assessment on downstream assets.
5 - Optimised	Traceability is automated where possible. Impact analysis is available on demand. Regulatory change triggers automatic assessment of affected data assets and AI models.	Traceability is automated where possible. Impact analysis is available on demand. Regulatory change triggers automatic assessment of affected data assets and AI models.	Traceability is automated where possible. Impact analysis is available on demand. Regulatory change triggers automatic assessment of affected data assets and AI models.

D1.6 - Impact Assessment

Measure ID	Measure Name	Governs	Normative References
D1.6	Impact Assessment	Whether the business impact of data quality issues is formally assessed before release of data products, reports, or AI models.	ISO 8000-61 ISO 42001 Clause 8.4 EU AI Act Article 9
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No impact assessment conducted. Data and AI released without consideration of potential business impact.	No impact assessment conducted. Data and AI released without consideration of potential business impact.	No impact assessment conducted. Data and AI released without consideration of potential business impact.
1 - Ad Hoc	Impact considered informally by individuals. No formal process. Assessment depends on who is involved.	Impact considered informally by individuals. No formal process. Assessment depends on who is involved.	Impact considered informally by individuals. No formal process. Assessment depends on who is involved.
2 - Repeatable	Impact assessment conducted for major releases. Informal. No standard approach or documentation template.	Impact assessment conducted for major releases. Informal. No standard approach or documentation template.	Impact assessment conducted for major releases. Informal. No standard approach or documentation template.
3 - Defined	A formal impact assessment process exists and is applied consistently before release. Documented. Reviewed by a named approver.	A formal impact assessment process exists and is applied consistently before release. Documented. Reviewed by a named approver.	A formal impact assessment process exists and is applied consistently before release. Documented. Reviewed by a named approver.
4 - Managed	Impact assessment is mandatory for all data and AI releases. Includes business risk, regulatory exposure, and AI-specific considerations. Results tracked over time.	Impact assessment is mandatory for all data and AI releases. Includes business risk, regulatory exposure, and AI-specific considerations. Results tracked over time.	Impact assessment is mandatory for all data and AI releases. Includes business risk, regulatory exposure, and AI-specific considerations. Results tracked over time.
5 - Optimised	Impact assessment is integrated into the data and AI governance lifecycle. Pre- and post-release impact is compared. Findings inform future governance decisions.	Impact assessment is integrated into the data and AI governance lifecycle. Pre- and post-release impact is compared. Findings inform future governance decisions.	Impact assessment is integrated into the data and AI governance lifecycle. Pre- and post-release impact is compared. Findings inform future governance decisions.

D1.7 - Data Product Ownership

Measure ID	Measure Name	Governs	Normative References
D1.7	Data Product Ownership	Whether data products are formally owned, versioned, and managed as business assets with defined lifecycles.	ISO 8000-8 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Data products are not recognised as business assets. No ownership, versioning, or lifecycle management.	Data products are not recognised as business assets. No ownership, versioning, or lifecycle management.	Data products are not recognised as business assets. No ownership, versioning, or lifecycle management.
1 - Ad Hoc	Some data products have informal owners. Versioning and lifecycle management are absent.	Some data products have informal owners. Versioning and lifecycle management are absent.	Some data products have informal owners. Versioning and lifecycle management are absent.
2 - Repeatable	Major data products have named owners. Versioning is inconsistently applied. No formal lifecycle process.	Major data products have named owners. Versioning is inconsistently applied. No formal lifecycle process.	Major data products have named owners. Versioning is inconsistently applied. No formal lifecycle process.
3 - Defined	All critical data products have formal owners. Versioning is applied. A defined lifecycle process covers creation, change, and retirement.	All critical data products have formal owners. Versioning is applied. A defined lifecycle process covers creation, change, and retirement.	All critical data products have formal owners. Versioning is applied. A defined lifecycle process covers creation, change, and retirement.
4 - Managed	Data product ownership is embedded in governance. Owner accountability is measured. Lifecycle events are recorded. Deprecation follows a formal process.	Data product ownership is embedded in governance. Owner accountability is measured. Lifecycle events are recorded. Deprecation follows a formal process.	Data product ownership is embedded in governance. Owner accountability is measured. Lifecycle events are recorded. Deprecation follows a formal process.
5 - Optimised	Data products are managed as strategic business assets. Product thinking is applied: roadmaps, versioning, SLAs, consumer contracts. Ownership is a recognised organisational role.	Data products are managed as strategic business assets. Product thinking is applied: roadmaps, versioning, SLAs, consumer contracts. Ownership is a recognised organisational role.	Data products are managed as strategic business assets. Product thinking is applied: roadmaps, versioning, SLAs, consumer contracts. Ownership is a recognised organisational role.

D1.8 - Strategic Alignment

Measure ID	Measure Name	Governs	Normative References
D1.8	Strategic Alignment	Whether the data strategy is formally aligned to the organisation's business strategy and AI strategy, with alignment reviewed on a defined cycle.	ISO 8000-8 Clause 4 ISO 42001 Clause 4.1
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No data strategy exists. Data activity is disconnected from organisational strategy.	No data strategy exists. Data activity is disconnected from organisational strategy.	No data strategy exists. Data activity is disconnected from organisational strategy.
1 - Ad Hoc	A data strategy exists informally or as part of an IT strategy. Not formally aligned to business or AI strategy.	A data strategy exists informally or as part of an IT strategy. Not formally aligned to business or AI strategy.	A data strategy exists informally or as part of an IT strategy. Not formally aligned to business or AI strategy.
2 - Repeatable	A data strategy is documented. High-level alignment to business strategy is stated. Alignment to AI strategy is absent or implicit.	A data strategy is documented. High-level alignment to business strategy is stated. Alignment to AI strategy is absent or implicit.	A data strategy is documented. High-level alignment to business strategy is stated. Alignment to AI strategy is absent or implicit.
3 - Defined	A data strategy is formally documented, reviewed annually, and explicitly aligned to both business and AI strategy. Alignment is validated with business leadership.	A data strategy is formally documented, reviewed annually, and explicitly aligned to both business and AI strategy. Alignment is validated with business leadership.	A data strategy is formally documented, reviewed annually, and explicitly aligned to both business and AI strategy. Alignment is validated with business leadership.
4 - Managed	Strategic alignment is actively maintained. Changes to business or AI strategy trigger a formal review of the data strategy. Gaps are tracked and addressed.	Strategic alignment is actively maintained. Changes to business or AI strategy trigger a formal review of the data strategy. Gaps are tracked and addressed.	Strategic alignment is actively maintained. Changes to business or AI strategy trigger a formal review of the data strategy. Gaps are tracked and addressed.
5 - Optimised	The data strategy is a live governance document. It drives resource allocation, capability investment, and AI initiative sequencing. Alignment is validated by executive leadership.	The data strategy is a live governance document. It drives resource allocation, capability investment, and AI initiative sequencing. Alignment is validated by executive leadership.	The data strategy is a live governance document. It drives resource allocation, capability investment, and AI initiative sequencing. Alignment is validated by executive leadership.

3. Domain D2: Data Ownership & Stewardship

Domain	Data Ownership & Stewardship
Domain ID	D2
Weighting	8.33%
Measures	8
Purpose	Data governance without accountability is aspiration without effect. This domain governs whether clear, enforceable accountability for data assets is assigned to named individuals, whether those individuals have the authority and tools to act, and whether the organisation has the structural mechanisms to resolve data quality issues and make governance decisions. Weak ownership is the single most common root cause of data quality failures across all sectors.
Regulatory Context	ISO 8000-8 Clause 5 (leadership and accountability). ISO 42001 Clause 5 (leadership). GDPR Article 5(2) (accountability principle) requires demonstrable accountability for data processing.

D2.1 - Formalised Roles

Measure ID	Measure Name	Governs	Normative References
D2.1	Formalised Roles	Whether Data Owners and Data Stewards are formally assigned, trained, and held accountable for defined data assets.	ISO 8000-8 Clause 5 DAMA DMBOK Ch.3 GDPR Art.5(2)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No data ownership roles exist. Accountability is absent.	No data ownership roles exist. Accountability is absent.	No data ownership roles exist. Accountability is absent.
1 - Ad Hoc	Data ownership is discussed but not formally assigned. Individuals may act as de facto owners without formal recognition.	Data ownership is discussed but not formally assigned. Individuals may act as de facto owners without formal recognition.	Data ownership is discussed but not formally assigned. Individuals may act as de facto owners without formal recognition.
2 - Repeatable	Data owners are named for major data assets. Roles are not formally documented. Training is absent.	Data owners are named for major data assets. Roles are not formally documented. Training is absent.	Data owners are named for major data assets. Roles are not formally documented. Training is absent.
3 - Defined	Data Owner and Data Steward roles are formally defined, documented, and assigned for all critical data assets. Role descriptions exist. Basic training is provided.	Data Owner and Data Steward roles are formally defined, documented, and assigned for all critical data assets. Role descriptions exist. Basic training is provided.	Data Owner and Data Steward roles are formally defined, documented, and assigned for all critical data assets. Role descriptions exist. Basic training is provided.
4 - Managed	All critical data assets have trained, accountable Data Owners and Stewards. Role performance is reviewed. Gaps in coverage are tracked and remediated.	All critical data assets have trained, accountable Data Owners and Stewards. Role performance is reviewed. Gaps in coverage are tracked and remediated.	All critical data assets have trained, accountable Data Owners and Stewards. Role performance is reviewed. Gaps in coverage are tracked and remediated.
5 - Optimised	Data ownership is embedded in the organisational structure. Owners have formal authority. The role is recognised in job descriptions and performance frameworks. Coverage is complete.	Data ownership is embedded in the organisational structure. Owners have formal authority. The role is recognised in job descriptions and performance frameworks. Coverage is complete.	Data ownership is embedded in the organisational structure. Owners have formal authority. The role is recognised in job descriptions and performance frameworks. Coverage is complete.

D2.2 - Accountability Mapping

Measure ID	Measure Name	Governs	Normative References
D2.2	Accountability Mapping	Whether accountability for data quality and governance is mapped via a formal RACI or equivalent across the full data lifecycle.	ISO 8000-8 Clause 5 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No accountability mapping. Responsibility for data quality is unclear or assumed to belong to IT.	No accountability mapping. Responsibility for data quality is unclear or assumed to belong to IT.	No accountability mapping. Responsibility for data quality is unclear or assumed to belong to IT.
1 - Ad Hoc	Accountability is informally understood within teams. Not documented.	Accountability is informally understood within teams. Not documented.	Accountability is informally understood within teams. Not documented.
2 - Repeatable	A RACI or equivalent exists for major data domains. Not applied universally. Not maintained.	A RACI or equivalent exists for major data domains. Not applied universally. Not maintained.	A RACI or equivalent exists for major data domains. Not applied universally. Not maintained.
3 - Defined	A formal RACI covers all critical data assets and governance activities. Reviewed annually. Applied consistently.	A formal RACI covers all critical data assets and governance activities. Reviewed annually. Applied consistently.	A formal RACI covers all critical data assets and governance activities. Reviewed annually. Applied consistently.
4 - Managed	The RACI is actively maintained and reflects current organisational structure. Changes to teams or systems trigger RACI updates. Accountability gaps are identified and closed.	The RACI is actively maintained and reflects current organisational structure. Changes to teams or systems trigger RACI updates. Accountability gaps are identified and closed.	The RACI is actively maintained and reflects current organisational structure. Changes to teams or systems trigger RACI updates. Accountability gaps are identified and closed.
5 - Optimised	Accountability mapping is embedded in governance tooling. Changes in data asset ownership are automatically reflected. Compliance with accountability requirements is auditable.	Accountability mapping is embedded in governance tooling. Changes in data asset ownership are automatically reflected. Compliance with accountability requirements is auditable.	Accountability mapping is embedded in governance tooling. Changes in data asset ownership are automatically reflected. Compliance with accountability requirements is auditable.

D2.3 - Stewardship Workflow

Measure ID	Measure Name	Governs	Normative References
D2.3	Stewardship Workflow	Whether a defined workflow exists for data issue triage, assignment, resolution, and closure.	ISO 8000-61 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No workflow. Data quality issues are raised informally or not at all.	No workflow. Data quality issues are raised informally or not at all.	No workflow. Data quality issues are raised informally or not at all.
1 - Ad Hoc	Issues are raised informally. Resolution depends on individual effort. No tracking.	Issues are raised informally. Resolution depends on individual effort. No tracking.	Issues are raised informally. Resolution depends on individual effort. No tracking.
2 - Repeatable	A basic issue triage process exists. Issues are logged but resolution is inconsistent. No SLA.	A basic issue triage process exists. Issues are logged but resolution is inconsistent. No SLA.	A basic issue triage process exists. Issues are logged but resolution is inconsistent. No SLA.
3 - Defined	A defined stewardship workflow covers issue logging, assignment, resolution, and closure. SLAs are defined. Issues are tracked to closure.	A defined stewardship workflow covers issue logging, assignment, resolution, and closure. SLAs are defined. Issues are tracked to closure.	A defined stewardship workflow covers issue logging, assignment, resolution, and closure. SLAs are defined. Issues are tracked to closure.
4 - Managed	The workflow is enforced through tooling. SLA compliance is measured and reported. Root cause analysis is conducted for recurring issues.	The workflow is enforced through tooling. SLA compliance is measured and reported. Root cause analysis is conducted for recurring issues.	The workflow is enforced through tooling. SLA compliance is measured and reported. Root cause analysis is conducted for recurring issues.
5 - Optimised	The stewardship workflow is integrated with data observability tooling. Issues are automatically detected and triaged. Root cause patterns inform proactive governance.	The stewardship workflow is integrated with data observability tooling. Issues are automatically detected and triaged. Root cause patterns inform proactive governance.	The stewardship workflow is integrated with data observability tooling. Issues are automatically detected and triaged. Root cause patterns inform proactive governance.

D2.4 - Performance Metrics

Measure ID	Measure Name	Governs	Normative References
D2.4	Performance Metrics	Whether Data Owners and Stewards have defined KPIs and whether performance against those KPIs is measured and reviewed.	ISO 8000-8 Clause 9 ISO 42001 Clause 9
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No performance metrics for data ownership or stewardship roles.	No performance metrics for data ownership or stewardship roles.	No performance metrics for data ownership or stewardship roles.
1 - Ad Hoc	Performance discussed informally. No defined KPIs.	Performance discussed informally. No defined KPIs.	Performance discussed informally. No defined KPIs.
2 - Repeatable	KPIs exist for some roles. Measurement is inconsistent. Review is infrequent.	KPIs exist for some roles. Measurement is inconsistent. Review is infrequent.	KPIs exist for some roles. Measurement is inconsistent. Review is infrequent.
3 - Defined	KPIs are defined for all Data Owner and Steward roles. Performance is reviewed on a defined cadence by data leadership.	KPIs are defined for all Data Owner and Steward roles. Performance is reviewed on a defined cadence by data leadership.	KPIs are defined for all Data Owner and Steward roles. Performance is reviewed on a defined cadence by data leadership.
4 - Managed	KPIs are measured, trended, and reported. Performance against KPIs influences resource allocation and programme prioritisation.	KPIs are measured, trended, and reported. Performance against KPIs influences resource allocation and programme prioritisation.	KPIs are measured, trended, and reported. Performance against KPIs influences resource allocation and programme prioritisation.
5 - Optimised	Data governance performance is embedded in organisational KPIs. Ownership performance data is used to continuously improve governance programme design.	Data governance performance is embedded in organisational KPIs. Ownership performance data is used to continuously improve governance programme design.	Data governance performance is embedded in organisational KPIs. Ownership performance data is used to continuously improve governance programme design.

D2.5 - Executive Sponsorship

Measure ID	Measure Name	Governs	Normative References
D2.5	Executive Sponsorship	Whether active, named executive sponsorship for data quality and governance exists and is visible.	ISO 8000-8 Clause 5 ISO 42001 Clause 5.1
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No executive sponsorship. Data governance has no senior advocate.	No executive sponsorship. Data governance has no senior advocate.	No executive sponsorship. Data governance has no senior advocate.
1 - Ad Hoc	Senior individuals express support informally. No named sponsor. No active engagement.	Senior individuals express support informally. No named sponsor. No active engagement.	Senior individuals express support informally. No named sponsor. No active engagement.
2 - Repeatable	A named executive sponsor exists. Engagement is periodic. Sponsorship is not visible to the organisation.	A named executive sponsor exists. Engagement is periodic. Sponsorship is not visible to the organisation.	A named executive sponsor exists. Engagement is periodic. Sponsorship is not visible to the organisation.
3 - Defined	A named executive sponsor is active. Sponsorship is visible. The sponsor chairs or participates in governance forums. Investment decisions are supported.	A named executive sponsor is active. Sponsorship is visible. The sponsor chairs or participates in governance forums. Investment decisions are supported.	A named executive sponsor is active. Sponsorship is visible. The sponsor chairs or participates in governance forums. Investment decisions are supported.
4 - Managed	Executive sponsorship is embedded in governance structure. The sponsor is accountable for governance outcomes. Sponsorship is recognised in the organisation's risk and assurance frameworks.	Executive sponsorship is embedded in governance structure. The sponsor is accountable for governance outcomes. Sponsorship is recognised in the organisation's risk and assurance frameworks.	Executive sponsorship is embedded in governance structure. The sponsor is accountable for governance outcomes. Sponsorship is recognised in the organisation's risk and assurance frameworks.
5 - Optimised	Data governance is a board-level agenda item. The sponsor has a formal mandate. Governance maturity is reported to the board on a defined cycle.	Data governance is a board-level agenda item. The sponsor has a formal mandate. Governance maturity is reported to the board on a defined cycle.	Data governance is a board-level agenda item. The sponsor has a formal mandate. Governance maturity is reported to the board on a defined cycle.

D2.6 - Cross-Functional Council

Measure ID	Measure Name	Governs	Normative References
D2.6	Cross-Functional Council	Whether a cross-functional data governance council or equivalent forum meets regularly with recorded outcomes and followed-up actions.	ISO 8000-8 Clause 5 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No cross-functional governance forum.	No cross-functional governance forum.	No cross-functional governance forum.
1 - Ad Hoc	Ad hoc meetings occur. No standing agenda. No minutes. No follow-up.	Ad hoc meetings occur. No standing agenda. No minutes. No follow-up.	Ad hoc meetings occur. No standing agenda. No minutes. No follow-up.
2 - Repeatable	A governance forum meets periodically. Minutes are recorded. Actions are not consistently followed up.	A governance forum meets periodically. Minutes are recorded. Actions are not consistently followed up.	A governance forum meets periodically. Minutes are recorded. Actions are not consistently followed up.
3 - Defined	A cross-functional data governance council meets on a defined schedule. Minutes are recorded. Actions are assigned and tracked to closure.	A cross-functional data governance council meets on a defined schedule. Minutes are recorded. Actions are assigned and tracked to closure.	A cross-functional data governance council meets on a defined schedule. Minutes are recorded. Actions are assigned and tracked to closure.
4 - Managed	The council has a defined mandate, terms of reference, and membership. Attendance is tracked. Decision outcomes are communicated to the organisation. Actions are measured.	The council has a defined mandate, terms of reference, and membership. Attendance is tracked. Decision outcomes are communicated to the organisation. Actions are measured.	The council has a defined mandate, terms of reference, and membership. Attendance is tracked. Decision outcomes are communicated to the organisation. Actions are measured.
5 - Optimised	The council is the authoritative governance decision-making body. Its decisions are binding. Membership spans all major business units. Its outputs feed the data strategy.	The council is the authoritative governance decision-making body. Its decisions are binding. Membership spans all major business units. Its outputs feed the data strategy.	The council is the authoritative governance decision-making body. Its decisions are binding. Membership spans all major business units. Its outputs feed the data strategy.

D2.7 - Escalation & Decision Rights

Measure ID	Measure Name	Governs	Normative References
D2.7	Escalation & Decision Rights	Whether escalation paths and data governance decision rights are clearly defined, documented, and understood by the organisation.	ISO 8000-8 Clause 5 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No escalation paths or decision rights defined.	No escalation paths or decision rights defined.	No escalation paths or decision rights defined.
1 - Ad Hoc	Escalation is handled informally. Decision rights are assumed rather than defined.	Escalation is handled informally. Decision rights are assumed rather than defined.	Escalation is handled informally. Decision rights are assumed rather than defined.
2 - Repeatable	Escalation paths are informally understood within the data team. Not documented or communicated.	Escalation paths are informally understood within the data team. Not documented or communicated.	Escalation paths are informally understood within the data team. Not documented or communicated.
3 - Defined	Escalation paths and decision rights are formally documented and communicated. Known to Data Owners and Stewards.	Escalation paths and decision rights are formally documented and communicated. Known to Data Owners and Stewards.	Escalation paths and decision rights are formally documented and communicated. Known to Data Owners and Stewards.
4 - Managed	Escalation paths are tested periodically. Decision rights are reviewed when governance structures change. Compliance is audited.	Escalation paths are tested periodically. Decision rights are reviewed when governance structures change. Compliance is audited.	Escalation paths are tested periodically. Decision rights are reviewed when governance structures change. Compliance is audited.
5 - Optimised	Decision rights are embedded in governance tooling. Escalation triggers automated notifications. Decision audit trails are maintained.	Decision rights are embedded in governance tooling. Escalation triggers automated notifications. Decision audit trails are maintained.	Decision rights are embedded in governance tooling. Escalation triggers automated notifications. Decision audit trails are maintained.

D2.8 - Stewardship Coverage

Measure ID	Measure Name	Governs	Normative References
D2.8	Stewardship Coverage	The percentage of critical data assets that have a named, active, and trained Data Owner or Steward.	ISO 8000-8 Clause 5 DAMA DMBOK Ch.3 GDPR Art.5(2)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Fewer than 10% of critical data assets have any identified owner.	Fewer than 10% of critical data assets have any identified owner.	Fewer than 10% of critical data assets have any identified owner.
1 - Ad Hoc	10-30% of critical data assets have an identified owner. Ownership is informal.	10-30% of critical data assets have an identified owner. Ownership is informal.	10-30% of critical data assets have an identified owner. Ownership is informal.
2 - Repeatable	30-60% of critical data assets have a named owner. Training and accountability are inconsistent.	30-60% of critical data assets have a named owner. Training and accountability are inconsistent.	30-60% of critical data assets have a named owner. Training and accountability are inconsistent.
3 - Defined	60-80% of critical data assets have a formally assigned, trained, and accountable owner.	60-80% of critical data assets have a formally assigned, trained, and accountable owner.	60-80% of critical data assets have a formally assigned, trained, and accountable owner.
4 - Managed	80-95% of critical data assets have a formally assigned, trained, and accountable owner. Coverage gaps are tracked and remediated.	80-95% of critical data assets have a formally assigned, trained, and accountable owner. Coverage gaps are tracked and remediated.	80-95% of critical data assets have a formally assigned, trained, and accountable owner. Coverage gaps are tracked and remediated.
5 - Optimised	Greater than 95% of critical data assets have complete, active, and accountable ownership. Coverage is audited. Gaps are closed within defined SLAs.	Greater than 95% of critical data assets have complete, active, and accountable ownership. Coverage is audited. Gaps are closed within defined SLAs.	Greater than 95% of critical data assets have complete, active, and accountable ownership. Coverage is audited. Gaps are closed within defined SLAs.

4. Domain D3: Core Data Quality

Domain	Core Data Quality
Domain ID	D3
Weighting	8.33%
Measures	12
Purpose	This domain governs the intrinsic quality characteristics of data itself: whether data is accurate, complete, consistent, timely, valid, unique, and fit for its intended purpose. These dimensions are the spine of ISO 8000 and the foundational requirement for reliable analytics and trustworthy AI. An organisation may have excellent governance structures but if the data itself is inaccurate or incomplete, those structures produce well-managed poor outcomes. Core data quality must be measured, monitored, and actively managed.
Regulatory Context	ISO 8000-8 (data quality principles). ISO 8000-61 (data quality management). ISO 42001 Clause 8 (operation). EU AI Act Article 10 (data and data governance) requires training, validation, and testing datasets to meet quality standards. GDPR Article 5(1)(d) (accuracy principle).

D3.1 - Accuracy

Measure ID	Measure Name	Governs	Normative References
D3.1	Accuracy	Whether data values correctly represent the real-world entities or events they describe, measured against trusted reference sources with automated checks.	ISO 8000-8 ISO 8000-61 GDPR Art.5(1)(d) EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No accuracy measurement. Data correctness is assumed.	No accuracy measurement. Data correctness is assumed.	No accuracy measurement. Data correctness is assumed.
1 - Ad Hoc	Accuracy checked manually and informally for known problem areas.	Accuracy checked manually and informally for known problem areas.	Accuracy checked manually and informally for known problem areas.
2 - Repeatable	Accuracy is measured for major datasets using a defined but manually executed process. Results are reviewed.	Accuracy is measured for major datasets using a defined but manually executed process. Results are reviewed.	Accuracy is measured for major datasets using a defined but manually executed process. Results are reviewed.
3 - Defined	Automated accuracy checks are in place for all critical datasets against defined reference sources. Thresholds are set. Breaches are alerted and investigated.	Automated accuracy checks are in place for all critical datasets against defined reference sources. Thresholds are set. Breaches are alerted and investigated.	Automated accuracy checks are in place for all critical datasets against defined reference sources. Thresholds are set. Breaches are alerted and investigated.
4 - Managed	Accuracy is continuously monitored. Trends are tracked over time. Root cause analysis is conducted for breaches. Remediation is tracked.	Accuracy is continuously monitored. Trends are tracked over time. Root cause analysis is conducted for breaches. Remediation is tracked.	Accuracy is continuously monitored. Trends are tracked over time. Root cause analysis is conducted for breaches. Remediation is tracked.
5 - Optimised	Accuracy measurement is fully automated across all data assets. AI-driven anomaly detection supplements rule-based checks. Accuracy SLAs are contractually defined in data contracts.	Accuracy measurement is fully automated across all data assets. AI-driven anomaly detection supplements rule-based checks. Accuracy SLAs are contractually defined in data contracts.	Accuracy measurement is fully automated across all data assets. AI-driven anomaly detection supplements rule-based checks. Accuracy SLAs are contractually defined in data contracts.

D3.2 - Completeness

Measure ID	Measure Name	Governs	Normative References
D3.2	Completeness	Whether data contains all required values and whether completeness thresholds are defined and enforced for critical datasets.	ISO 8000-8 ISO 8000-61 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No completeness measurement. Missing values are not tracked.	No completeness measurement. Missing values are not tracked.	No completeness measurement. Missing values are not tracked.
1 - Ad Hoc	Completeness is checked informally for known gaps.	Completeness is checked informally for known gaps.	Completeness is checked informally for known gaps.
2 - Repeatable	Completeness thresholds are defined for major datasets. Measurement is periodic and manual.	Completeness thresholds are defined for major datasets. Measurement is periodic and manual.	Completeness thresholds are defined for major datasets. Measurement is periodic and manual.
3 - Defined	Completeness thresholds are formally defined and enforced for all critical datasets. Automated monitoring is in place. Breaches are alerted.	Completeness thresholds are formally defined and enforced for all critical datasets. Automated monitoring is in place. Breaches are alerted.	Completeness thresholds are formally defined and enforced for all critical datasets. Automated monitoring is in place. Breaches are alerted.
4 - Managed	Completeness is monitored continuously. Trends are tracked. Incomplete data is quarantined pending remediation. Root cause analysis is standard.	Completeness is monitored continuously. Trends are tracked. Incomplete data is quarantined pending remediation. Root cause analysis is standard.	Completeness is monitored continuously. Trends are tracked. Incomplete data is quarantined pending remediation. Root cause analysis is standard.
5 - Optimised	Completeness is governed at the point of data collection. Incomplete data cannot enter critical pipelines. Completeness SLAs are defined in data contracts.	Completeness is governed at the point of data collection. Incomplete data cannot enter critical pipelines. Completeness SLAs are defined in data contracts.	Completeness is governed at the point of data collection. Incomplete data cannot enter critical pipelines. Completeness SLAs are defined in data contracts.

D3.3 - Consistency

Measure ID	Measure Name	Governs	Normative References
D3.3	Consistency	Whether data definitions and values are applied consistently across all systems, domains, and use cases.	ISO 8000-8 ISO 8000-61 DAMA DMBOK Ch.2
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No consistency management. Conflicting definitions and values across systems are accepted.	No consistency management. Conflicting definitions and values across systems are accepted.	No consistency management. Conflicting definitions and values across systems are accepted.
1 - Ad Hoc	Inconsistencies are known but unmanaged. Reconciliation is manual and ad hoc.	Inconsistencies are known but unmanaged. Reconciliation is manual and ad hoc.	Inconsistencies are known but unmanaged. Reconciliation is manual and ad hoc.
2 - Repeatable	Consistency is managed for major shared data elements. Inconsistencies between systems are documented and remediation is planned.	Consistency is managed for major shared data elements. Inconsistencies between systems are documented and remediation is planned.	Consistency is managed for major shared data elements. Inconsistencies between systems are documented and remediation is planned.
3 - Defined	Data definitions are standardised and applied consistently across critical systems. Inconsistencies are detected and resolved through a formal process.	Data definitions are standardised and applied consistently across critical systems. Inconsistencies are detected and resolved through a formal process.	Data definitions are standardised and applied consistently across critical systems. Inconsistencies are detected and resolved through a formal process.
4 - Managed	Consistency is actively monitored across all systems. Discrepancies trigger automated alerts. Changes to definitions follow a formal approval process.	Consistency is actively monitored across all systems. Discrepancies trigger automated alerts. Changes to definitions follow a formal approval process.	Consistency is actively monitored across all systems. Discrepancies trigger automated alerts. Changes to definitions follow a formal approval process.
5 - Optimised	Consistency is enforced at the point of integration. Data contracts define agreed definitions. Definitional changes are managed through a governed change process with impact assessment.	Consistency is enforced at the point of integration. Data contracts define agreed definitions. Definitional changes are managed through a governed change process with impact assessment.	Consistency is enforced at the point of integration. Data contracts define agreed definitions. Definitional changes are managed through a governed change process with impact assessment.

D3.4 - Timeliness

Measure ID	Measure Name	Governs	Normative References
D3.4	Timeliness	Whether SLAs for data freshness are defined, monitored, and met for all critical data assets and AI model inputs.	ISO 8000-8 ISO 42001 Clause 8 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No freshness SLAs. Data latency is unknown or unmanaged.	No freshness SLAs. Data latency is unknown or unmanaged.	No freshness SLAs. Data latency is unknown or unmanaged.
1 - Ad Hoc	Freshness is considered informally. SLAs are not defined.	Freshness is considered informally. SLAs are not defined.	Freshness is considered informally. SLAs are not defined.
2 - Repeatable	Freshness SLAs are defined for major data feeds. Monitoring is manual.	Freshness SLAs are defined for major data feeds. Monitoring is manual.	Freshness SLAs are defined for major data feeds. Monitoring is manual.
3 - Defined	Freshness SLAs are formally defined for all critical data assets. Automated monitoring is in place. Breaches are alerted and investigated.	Freshness SLAs are formally defined for all critical data assets. Automated monitoring is in place. Breaches are alerted and investigated.	Freshness SLAs are formally defined for all critical data assets. Automated monitoring is in place. Breaches are alerted and investigated.
4 - Managed	Freshness SLA compliance is tracked and reported. Trends are analysed. Chronic breaches trigger pipeline or architecture review.	Freshness SLA compliance is tracked and reported. Trends are analysed. Chronic breaches trigger pipeline or architecture review.	Freshness SLA compliance is tracked and reported. Trends are analysed. Chronic breaches trigger pipeline or architecture review.
5 - Optimised	Freshness is governed end-to-end across the data supply chain. SLA compliance is included in data contracts. Latency budgets are defined for AI inference pipelines.	Freshness is governed end-to-end across the data supply chain. SLA compliance is included in data contracts. Latency budgets are defined for AI inference pipelines.	Freshness is governed end-to-end across the data supply chain. SLA compliance is included in data contracts. Latency budgets are defined for AI inference pipelines.

D3.5 - Validity

Measure ID	Measure Name	Governs	Normative References
D3.5	Validity	Whether data values are validated against business rules at ingestion and in-flight across pipelines.	ISO 8000-61 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No validation rules. Invalid data enters systems undetected.	No validation rules. Invalid data enters systems undetected.	No validation rules. Invalid data enters systems undetected.
1 - Ad Hoc	Validation occurs informally at point of use. Not at ingestion.	Validation occurs informally at point of use. Not at ingestion.	Validation occurs informally at point of use. Not at ingestion.
2 - Repeatable	Validation rules exist for major data sources. Applied at ingestion for some pipelines.	Validation rules exist for major data sources. Applied at ingestion for some pipelines.	Validation rules exist for major data sources. Applied at ingestion for some pipelines.
3 - Defined	Validation rules are defined for all critical data elements and applied at ingestion and in-flight. Invalid data is rejected or quarantined.	Validation rules are defined for all critical data elements and applied at ingestion and in-flight. Invalid data is rejected or quarantined.	Validation rules are defined for all critical data elements and applied at ingestion and in-flight. Invalid data is rejected or quarantined.
4 - Managed	Validation rules are version-controlled. New data sources require validation rule definition before ingestion. Rule coverage is measured.	Validation rules are version-controlled. New data sources require validation rule definition before ingestion. Rule coverage is measured.	Validation rules are version-controlled. New data sources require validation rule definition before ingestion. Rule coverage is measured.
5 - Optimised	Validation is fully automated and embedded in the data platform. Rule libraries are maintained. AI-specific input validation rules are defined for each model in production.	Validation is fully automated and embedded in the data platform. Rule libraries are maintained. AI-specific input validation rules are defined for each model in production.	Validation is fully automated and embedded in the data platform. Rule libraries are maintained. AI-specific input validation rules are defined for each model in production.

D3.6 - Uniqueness

Measure ID	Measure Name	Governs	Normative References
D3.6	Uniqueness	Whether duplicate detection and deduplication processes are in place for critical data assets, particularly master data.	ISO 8000-8 ISO 8000-61 GDPR Art.5(1)(c)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No duplicate management. Duplicates are accepted.	No duplicate management. Duplicates are accepted.	No duplicate management. Duplicates are accepted.
1 - Ad Hoc	Duplicates are identified manually when they cause visible problems.	Duplicates are identified manually when they cause visible problems.	Duplicates are identified manually when they cause visible problems.
2 - Repeatable	Deduplication is in place for customer master data. Not extended to other critical assets.	Deduplication is in place for customer master data. Not extended to other critical assets.	Deduplication is in place for customer master data. Not extended to other critical assets.
3 - Defined	Duplicate detection and deduplication are applied to all critical master data assets. Process is documented and results are monitored.	Duplicate detection and deduplication are applied to all critical master data assets. Process is documented and results are monitored.	Duplicate detection and deduplication are applied to all critical master data assets. Process is documented and results are monitored.
4 - Managed	Deduplication is automated. Match rates and false positive rates are tracked. Golden record management is in place for key entities.	Deduplication is automated. Match rates and false positive rates are tracked. Golden record management is in place for key entities.	Deduplication is automated. Match rates and false positive rates are tracked. Golden record management is in place for key entities.
5 - Optimised	Uniqueness is governed across the enterprise. Deduplication is embedded in ingestion pipelines. Entity resolution applies across all critical data domains.	Uniqueness is governed across the enterprise. Deduplication is embedded in ingestion pipelines. Entity resolution applies across all critical data domains.	Uniqueness is governed across the enterprise. Deduplication is embedded in ingestion pipelines. Entity resolution applies across all critical data domains.

D3.7 - Integrity

Measure ID	Measure Name	Governs	Normative References
D3.7	Integrity	Whether referential integrity constraints are enforced across datasets and between systems.	ISO 8000-8 ISO 8000-61
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No referential integrity enforcement. Orphaned and broken relationships are common.	No referential integrity enforcement. Orphaned and broken relationships are common.	No referential integrity enforcement. Orphaned and broken relationships are common.
1 - Ad Hoc	Integrity issues are identified reactively when they cause reporting failures.	Integrity issues are identified reactively when they cause reporting failures.	Integrity issues are identified reactively when they cause reporting failures.
2 - Repeatable	Referential integrity is enforced within major transactional systems. Cross-system integrity is not managed.	Referential integrity is enforced within major transactional systems. Cross-system integrity is not managed.	Referential integrity is enforced within major transactional systems. Cross-system integrity is not managed.
3 - Defined	Referential integrity constraints are defined and enforced across all critical datasets. Cross-system integrity is monitored.	Referential integrity constraints are defined and enforced across all critical datasets. Cross-system integrity is monitored.	Referential integrity constraints are defined and enforced across all critical datasets. Cross-system integrity is monitored.
4 - Managed	Integrity violations are detected automatically and trigger incident workflows. Root cause analysis identifies systemic issues.	Integrity violations are detected automatically and trigger incident workflows. Root cause analysis identifies systemic issues.	Integrity violations are detected automatically and trigger incident workflows. Root cause analysis identifies systemic issues.
5 - Optimised	Integrity is governed across the full data estate including the data lake and AI feature stores. Violations cannot propagate to production AI systems.	Integrity is governed across the full data estate including the data lake and AI feature stores. Violations cannot propagate to production AI systems.	Integrity is governed across the full data estate including the data lake and AI feature stores. Violations cannot propagate to production AI systems.

D3.8 - Provenance

Measure ID	Measure Name	Governs	Normative References
D3.8	Provenance	Whether the origin, transformation history, and lineage of data are recorded and traceable.	ISO 8000-110 ISO 42001 Clause 8 EU AI Act Art.10,12
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No provenance recording. Data origin is unknown.	No provenance recording. Data origin is unknown.	No provenance recording. Data origin is unknown.
1 - Ad Hoc	Provenance is informally understood for some datasets. Not documented.	Provenance is informally understood for some datasets. Not documented.	Provenance is informally understood for some datasets. Not documented.
2 - Repeatable	Provenance is recorded for major datasets. Transformation history is partially documented.	Provenance is recorded for major datasets. Transformation history is partially documented.	Provenance is recorded for major datasets. Transformation history is partially documented.
3 - Defined	Provenance and transformation history are recorded for all critical data assets. Lineage is traceable from source to consumption point.	Provenance and transformation history are recorded for all critical data assets. Lineage is traceable from source to consumption point.	Provenance and transformation history are recorded for all critical data assets. Lineage is traceable from source to consumption point.
4 - Managed	Provenance is automatically captured by the data platform. Lineage is available on demand. Changes to source systems trigger lineage review.	Provenance is automatically captured by the data platform. Lineage is available on demand. Changes to source systems trigger lineage review.	Provenance is automatically captured by the data platform. Lineage is available on demand. Changes to source systems trigger lineage review.
5 - Optimised	Full end-to-end provenance is maintained automatically. Lineage includes AI training data, model versions, and inference inputs. Provenance is part of the AI audit trail.	Full end-to-end provenance is maintained automatically. Lineage includes AI training data, model versions, and inference inputs. Provenance is part of the AI audit trail.	Full end-to-end provenance is maintained automatically. Lineage includes AI training data, model versions, and inference inputs. Provenance is part of the AI audit trail.

D3.9 - Precision

Measure ID	Measure Name	Governs	Normative References
D3.9	Precision	Whether data is captured and stored at the precision required for its intended use cases, including AI model inputs.	ISO 8000-8 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Precision requirements are not considered.	Precision requirements are not considered.	Precision requirements are not considered.
1 - Ad Hoc	Precision is considered informally for known use cases.	Precision is considered informally for known use cases.	Precision is considered informally for known use cases.
2 - Repeatable	Precision is assessed for major use cases. AI model input precision is not formally considered.	Precision is assessed for major use cases. AI model input precision is not formally considered.	Precision is assessed for major use cases. AI model input precision is not formally considered.
3 - Defined	Precision requirements are formally assessed for all critical use cases. Data is captured and stored at the required precision.	Precision requirements are formally assessed for all critical use cases. Data is captured and stored at the required precision.	Precision requirements are formally assessed for all critical use cases. Data is captured and stored at the required precision.
4 - Managed	Precision requirements are documented per use case. AI model input precision is validated as part of the AI readiness gate.	Precision requirements are documented per use case. AI model input precision is validated as part of the AI readiness gate.	Precision requirements are documented per use case. AI model input precision is validated as part of the AI readiness gate.
5 - Optimised	Precision governance covers all data assets and use cases. Precision degradation through transformation is detected and governed.	Precision governance covers all data assets and use cases. Precision degradation through transformation is detected and governed.	Precision governance covers all data assets and use cases. Precision degradation through transformation is detected and governed.

D3.10 - Credibility

Measure ID	Measure Name	Governs	Normative References
D3.10	Credibility	Whether data sources are assessed and rated for trustworthiness, and whether those ratings are applied when selecting data for AI training and analytics.	ISO 8000-8 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No credibility assessment. All data sources are treated as equally trustworthy.	No credibility assessment. All data sources are treated as equally trustworthy.	No credibility assessment. All data sources are treated as equally trustworthy.
1 - Ad Hoc	Source credibility is informally understood. No formal rating.	Source credibility is informally understood. No formal rating.	Source credibility is informally understood. No formal rating.
2 - Repeatable	A trusted source register exists for some data domains. Not applied to AI inputs.	A trusted source register exists for some data domains. Not applied to AI inputs.	A trusted source register exists for some data domains. Not applied to AI inputs.
3 - Defined	All critical data sources are assessed and rated for credibility. Ratings are documented. Low-credibility sources are flagged.	All critical data sources are assessed and rated for credibility. Ratings are documented. Low-credibility sources are flagged.	All critical data sources are assessed and rated for credibility. Ratings are documented. Low-credibility sources are flagged.
4 - Managed	Credibility ratings are actively maintained. Changes to source quality trigger rating review. AI training data source credibility is a mandatory pre-condition for model development.	Credibility ratings are actively maintained. Changes to source quality trigger rating review. AI training data source credibility is a mandatory pre-condition for model development.	Credibility ratings are actively maintained. Changes to source quality trigger rating review. AI training data source credibility is a mandatory pre-condition for model development.
5 - Optimised	Credibility is embedded in data supply chain governance. Automated credibility monitoring detects source quality degradation. Credibility ratings are included in data contracts.	Credibility is embedded in data supply chain governance. Automated credibility monitoring detects source quality degradation. Credibility ratings are included in data contracts.	Credibility is embedded in data supply chain governance. Automated credibility monitoring detects source quality degradation. Credibility ratings are included in data contracts.

D3.11 - Auditability

Measure ID	Measure Name	Governs	Normative References
D3.11	Auditability	Whether every change to a critical data asset can be traced, attributed, and reconstructed.	ISO 8000-110 ISO 42001 Clause 8 EU AI Act Art.12 GDPR Art.5(2)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No change audit. Data changes are untracked.	No change audit. Data changes are untracked.	No change audit. Data changes are untracked.
1 - Ad Hoc	Change logging exists in some transactional systems. Not applied universally.	Change logging exists in some transactional systems. Not applied universally.	Change logging exists in some transactional systems. Not applied universally.
2 - Repeatable	Change audit logs exist for major transactional systems. Analytics and lake data are not covered.	Change audit logs exist for major transactional systems. Analytics and lake data are not covered.	Change audit logs exist for major transactional systems. Analytics and lake data are not covered.
3 - Defined	Change audit logs are in place for all critical data assets. Logs are tamper-evident. Changes can be attributed to individuals or processes.	Change audit logs are in place for all critical data assets. Logs are tamper-evident. Changes can be attributed to individuals or processes.	Change audit logs are in place for all critical data assets. Logs are tamper-evident. Changes can be attributed to individuals or processes.
4 - Managed	Audit logs are actively reviewed. Anomalous changes trigger investigation. Logs are retained for defined periods aligned to regulatory requirements.	Audit logs are actively reviewed. Anomalous changes trigger investigation. Logs are retained for defined periods aligned to regulatory requirements.	Audit logs are actively reviewed. Anomalous changes trigger investigation. Logs are retained for defined periods aligned to regulatory requirements.
5 - Optimised	Full auditability is automated. Changes to AI training data, model artefacts, and inference inputs are logged. Audit trails support regulatory challenge and model reproducibility.	Full auditability is automated. Changes to AI training data, model artefacts, and inference inputs are logged. Audit trails support regulatory challenge and model reproducibility.	Full auditability is automated. Changes to AI training data, model artefacts, and inference inputs are logged. Audit trails support regulatory challenge and model reproducibility.

D3.12 - Fitness for Purpose

Measure ID	Measure Name	Governs	Normative References
D3.12	Fitness for Purpose	Whether data quality is formally assessed against the specific requirements of each intended use case, including AI model development and deployment.	ISO 8000-8 ISO 8000-61 ISO 42001 Clause 8.4 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Fitness for purpose is not assessed. Data is used without validation against use case requirements.	Fitness for purpose is not assessed. Data is used without validation against use case requirements.	Fitness for purpose is not assessed. Data is used without validation against use case requirements.
1 - Ad Hoc	Fitness is considered informally by analysts before use.	Fitness is considered informally by analysts before use.	Fitness is considered informally by analysts before use.
2 - Repeatable	Fitness assessment is conducted for major analytics use cases. AI use cases are not formally covered.	Fitness assessment is conducted for major analytics use cases. AI use cases are not formally covered.	Fitness assessment is conducted for major analytics use cases. AI use cases are not formally covered.
3 - Defined	A formal fitness for purpose assessment is conducted before all significant data use, including AI model development. Assessment criteria are defined.	A formal fitness for purpose assessment is conducted before all significant data use, including AI model development. Assessment criteria are defined.	A formal fitness for purpose assessment is conducted before all significant data use, including AI model development. Assessment criteria are defined.
4 - Managed	Fitness assessment is mandatory and documented. Results are recorded. Unfit data cannot be used without an approved exception. AI readiness gate includes fitness assessment.	Fitness assessment is mandatory and documented. Results are recorded. Unfit data cannot be used without an approved exception. AI readiness gate includes fitness assessment.	Fitness assessment is mandatory and documented. Results are recorded. Unfit data cannot be used without an approved exception. AI readiness gate includes fitness assessment.
5 - Optimised	Fitness for purpose is assessed automatically against use case profiles. AI model data requirements are formally specified. Fitness assessment results are part of the AI governance audit trail.	Fitness for purpose is assessed automatically against use case profiles. AI model data requirements are formally specified. Fitness assessment results are part of the AI governance audit trail.	Fitness for purpose is assessed automatically against use case profiles. AI model data requirements are formally specified. Fitness assessment results are part of the AI governance audit trail.

5. Domain D4: Pipeline Quality & Operations

Domain	Pipeline Quality & Operations
Domain ID	D4
Weighting	8.33%
Measures	10
Purpose	Data quality deteriorates in transit. Pipelines that ingest, transform, and deliver data introduce errors through incomplete validation, undocumented transformations, undetected failures, and ungoverned change. This domain governs the operational quality of data pipelines from ingestion through to delivery, including the pipelines that feed AI systems. Organisations with mature pipeline governance can trace exactly what happened to data between source and consumption, detect failures before they affect downstream decisions, and ensure AI model inputs are consistently of known quality.
Regulatory Context	ISO 8000-61 (data quality management operations). ISO 42001 Clause 8 (operation). EU AI Act Article 10 requires that data used for training, validation, and testing undergoes appropriate data preparation processing.

D4.1 - Ingestion Controls

Measure ID	Measure Name	Governs	Normative References
D4.1	Ingestion Controls	Whether ingestion processes are governed with quality gates that validate data before it enters pipelines.	ISO 8000-61 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No ingestion controls. All data enters pipelines regardless of quality.	No ingestion controls. All data enters pipelines regardless of quality.	No ingestion controls. All data enters pipelines regardless of quality.
1 - Ad Hoc	Informal checks occur for known problem sources. No systematic gate.	Informal checks occur for known problem sources. No systematic gate.	Informal checks occur for known problem sources. No systematic gate.
2 - Repeatable	Quality gates exist at ingestion for major data sources. Not universally applied.	Quality gates exist at ingestion for major data sources. Not universally applied.	Quality gates exist at ingestion for major data sources. Not universally applied.
3 - Defined	Formal quality gates are in place at ingestion for all critical data pipelines. Failed data is quarantined and investigated.	Formal quality gates are in place at ingestion for all critical data pipelines. Failed data is quarantined and investigated.	Formal quality gates are in place at ingestion for all critical data pipelines. Failed data is quarantined and investigated.
4 - Managed	Ingestion gates are automated and version-controlled. Gate rules are reviewed when source systems change. Coverage is measured.	Ingestion gates are automated and version-controlled. Gate rules are reviewed when source systems change. Coverage is measured.	Ingestion gates are automated and version-controlled. Gate rules are reviewed when source systems change. Coverage is measured.
5 - Optimised	Ingestion governance is embedded in the data platform. No data enters a production pipeline without passing a formal quality gate. AI training pipelines have enhanced gate criteria.	Ingestion governance is embedded in the data platform. No data enters a production pipeline without passing a formal quality gate. AI training pipelines have enhanced gate criteria.	Ingestion governance is embedded in the data platform. No data enters a production pipeline without passing a formal quality gate. AI training pipelines have enhanced gate criteria.

D4.2 - Transformation Integrity

Measure ID	Measure Name	Governs	Normative References
D4.2	Transformation Integrity	Whether all data transformations are documented, tested, and validated to ensure they do not introduce errors or unintended changes.	ISO 8000-61 ISO 42001 Clause 8 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Transformations are undocumented. Errors introduced in transformation are undetected.	Transformations are undocumented. Errors introduced in transformation are undetected.	Transformations are undocumented. Errors introduced in transformation are undetected.
1 - Ad Hoc	Key transformations are informally understood. Documentation is absent or informal.	Key transformations are informally understood. Documentation is absent or informal.	Key transformations are informally understood. Documentation is absent or informal.
2 - Repeatable	Major transformations are documented. Testing is ad hoc.	Major transformations are documented. Testing is ad hoc.	Major transformations are documented. Testing is ad hoc.
3 - Defined	All critical transformations are documented, tested, and version-controlled. Documentation is maintained when transformations change.	All critical transformations are documented, tested, and version-controlled. Documentation is maintained when transformations change.	All critical transformations are documented, tested, and version-controlled. Documentation is maintained when transformations change.
4 - Managed	Transformation testing is automated. Changes to transformations require formal review. Transformation lineage is captured and linked to data provenance.	Transformation testing is automated. Changes to transformations require formal review. Transformation lineage is captured and linked to data provenance.	Transformation testing is automated. Changes to transformations require formal review. Transformation lineage is captured and linked to data provenance.
5 - Optimised	All transformations are governed through a formal change process. Transformation logic is version-controlled and linked to data lineage. AI feature engineering transformations are subject to enhanced review.	All transformations are governed through a formal change process. Transformation logic is version-controlled and linked to data lineage. AI feature engineering transformations are subject to enhanced review.	All transformations are governed through a formal change process. Transformation logic is version-controlled and linked to data lineage. AI feature engineering transformations are subject to enhanced review.

D4.3 - Monitoring & Alerting

Measure ID	Measure Name	Governs	Normative References
D4.3	Monitoring & Alerting	Whether pipeline health is monitored in real time with automated alerts for failures, anomalies, and SLA breaches.	ISO 8000-61 ISO 42001 Clause 9
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No monitoring. Pipeline failures are discovered when downstream systems are affected.	No monitoring. Pipeline failures are discovered when downstream systems are affected.	No monitoring. Pipeline failures are discovered when downstream systems are affected.
1 - Ad Hoc	Manual checks occur periodically. No automated monitoring.	Manual checks occur periodically. No automated monitoring.	Manual checks occur periodically. No automated monitoring.
2 - Repeatable	Monitoring is in place for major pipelines. Alerting is inconsistent.	Monitoring is in place for major pipelines. Alerting is inconsistent.	Monitoring is in place for major pipelines. Alerting is inconsistent.
3 - Defined	Real-time monitoring and automated alerting is in place for all critical pipelines. Alerts are routed to responsible owners.	Real-time monitoring and automated alerting is in place for all critical pipelines. Alerts are routed to responsible owners.	Real-time monitoring and automated alerting is in place for all critical pipelines. Alerts are routed to responsible owners.
4 - Managed	Monitoring coverage is measured and gaps are tracked. Alert quality is reviewed. False positives are minimised through tuning.	Monitoring coverage is measured and gaps are tracked. Alert quality is reviewed. False positives are minimised through tuning.	Monitoring coverage is measured and gaps are tracked. Alert quality is reviewed. False positives are minimised through tuning.
5 - Optimised	Unified observability platform covers all pipelines including AI training and inference. Anomaly detection supplements threshold-based alerting.	Unified observability platform covers all pipelines including AI training and inference. Anomaly detection supplements threshold-based alerting.	Unified observability platform covers all pipelines including AI training and inference. Anomaly detection supplements threshold-based alerting.

D4.4 - Error Handling

Measure ID	Measure Name	Governs	Normative References
D4.4	Error Handling	Whether a robust error handling framework is in place covering logging, incident classification, and workflow for resolution.	ISO 8000-61
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No error handling framework. Failures are managed ad hoc.	No error handling framework. Failures are managed ad hoc.	No error handling framework. Failures are managed ad hoc.
1 - Ad Hoc	Errors are logged informally in some pipelines. No consistent approach.	Errors are logged informally in some pipelines. No consistent approach.	Errors are logged informally in some pipelines. No consistent approach.
2 - Repeatable	Error logging exists for major pipelines. Incident workflow is partially defined.	Error logging exists for major pipelines. Incident workflow is partially defined.	Error logging exists for major pipelines. Incident workflow is partially defined.
3 - Defined	A formal error handling framework covers all critical pipelines. Errors are logged, classified, and routed through a defined incident workflow.	A formal error handling framework covers all critical pipelines. Errors are logged, classified, and routed through a defined incident workflow.	A formal error handling framework covers all critical pipelines. Errors are logged, classified, and routed through a defined incident workflow.
4 - Managed	Error handling is automated where possible. Error trends are analysed. Chronic errors trigger root cause investigation and remediation.	Error handling is automated where possible. Error trends are analysed. Chronic errors trigger root cause investigation and remediation.	Error handling is automated where possible. Error trends are analysed. Chronic errors trigger root cause investigation and remediation.
5 - Optimised	Error handling is integrated with the observability platform. AI pipeline errors trigger enhanced investigation given downstream model impact.	Error handling is integrated with the observability platform. AI pipeline errors trigger enhanced investigation given downstream model impact.	Error handling is integrated with the observability platform. AI pipeline errors trigger enhanced investigation given downstream model impact.

D4.5 - Volume & Velocity

Measure ID	Measure Name	Governs	Normative References
D4.5	Volume & Velocity	Whether pipelines are designed and tested to handle peak data volumes and velocity without quality degradation.	ISO 8000-61 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Volume and velocity are not considered in pipeline design.	Volume and velocity are not considered in pipeline design.	Volume and velocity are not considered in pipeline design.
1 - Ad Hoc	Peak load is managed reactively when failures occur.	Peak load is managed reactively when failures occur.	Peak load is managed reactively when failures occur.
2 - Repeatable	Major pipelines are tested for volume. Velocity is not formally managed.	Major pipelines are tested for volume. Velocity is not formally managed.	Major pipelines are tested for volume. Velocity is not formally managed.
3 - Defined	Volume and velocity requirements are defined for all critical pipelines. Performance testing is conducted. Degradation at peak is detected and investigated.	Volume and velocity requirements are defined for all critical pipelines. Performance testing is conducted. Degradation at peak is detected and investigated.	Volume and velocity requirements are defined for all critical pipelines. Performance testing is conducted. Degradation at peak is detected and investigated.
4 - Managed	Volume and velocity SLAs are formally defined. Capacity planning is proactive. Degradation triggers automatic investigation.	Volume and velocity SLAs are formally defined. Capacity planning is proactive. Degradation triggers automatic investigation.	Volume and velocity SLAs are formally defined. Capacity planning is proactive. Degradation triggers automatic investigation.
5 - Optimised	Pipelines are designed for elastic scale. Volume and velocity are continuously monitored. AI inference pipeline latency SLAs are defined and monitored.	Pipelines are designed for elastic scale. Volume and velocity are continuously monitored. AI inference pipeline latency SLAs are defined and monitored.	Pipelines are designed for elastic scale. Volume and velocity are continuously monitored. AI inference pipeline latency SLAs are defined and monitored.

D4.6 - Dependency Management

Measure ID	Measure Name	Governs	Normative References
D4.6	Dependency Management	Whether upstream and downstream pipeline dependencies are mapped, managed, and considered in change and incident management.	ISO 8000-61
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Dependencies are unknown. Cascade failures occur without warning.	Dependencies are unknown. Cascade failures occur without warning.	Dependencies are unknown. Cascade failures occur without warning.
1 - Ad Hoc	Key dependencies are informally understood.	Key dependencies are informally understood.	Key dependencies are informally understood.
2 - Repeatable	Dependencies are mapped for major pipelines. Not fully maintained.	Dependencies are mapped for major pipelines. Not fully maintained.	Dependencies are mapped for major pipelines. Not fully maintained.
3 - Defined	All critical pipeline dependencies are formally mapped and maintained. Dependency maps are used in change management and incident response.	All critical pipeline dependencies are formally mapped and maintained. Dependency maps are used in change management and incident response.	All critical pipeline dependencies are formally mapped and maintained. Dependency maps are used in change management and incident response.
4 - Managed	Dependency management is integrated with change management tooling. Changes to upstream systems trigger downstream impact assessment.	Dependency management is integrated with change management tooling. Changes to upstream systems trigger downstream impact assessment.	Dependency management is integrated with change management tooling. Changes to upstream systems trigger downstream impact assessment.
5 - Optimised	Full dependency graph is maintained automatically. AI model dependencies on upstream data pipelines are formally tracked. Upstream changes trigger AI model re-evaluation.	Full dependency graph is maintained automatically. AI model dependencies on upstream data pipelines are formally tracked. Upstream changes trigger AI model re-evaluation.	Full dependency graph is maintained automatically. AI model dependencies on upstream data pipelines are formally tracked. Upstream changes trigger AI model re-evaluation.

D4.7 - Testing & Validation

Measure ID	Measure Name	Governs	Normative References
D4.7	Testing & Validation	Whether pipelines are subject to formal unit, integration, and regression testing before deployment and after change.	ISO 8000-61 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No formal pipeline testing.	No formal pipeline testing.	No formal pipeline testing.
1 - Ad Hoc	Testing occurs informally before major releases.	Testing occurs informally before major releases.	Testing occurs informally before major releases.
2 - Repeatable	Unit and integration testing is in place for major pipelines. Regression testing is absent.	Unit and integration testing is in place for major pipelines. Regression testing is absent.	Unit and integration testing is in place for major pipelines. Regression testing is absent.
3 - Defined	Unit, integration, and regression testing are applied to all critical pipelines. Testing is mandatory before deployment.	Unit, integration, and regression testing are applied to all critical pipelines. Testing is mandatory before deployment.	Unit, integration, and regression testing are applied to all critical pipelines. Testing is mandatory before deployment.
4 - Managed	Test coverage is measured. Test results are tracked over time. Failing tests block deployment. Testing is automated.	Test coverage is measured. Test results are tracked over time. Failing tests block deployment. Testing is automated.	Test coverage is measured. Test results are tracked over time. Failing tests block deployment. Testing is automated.
5 - Optimised	Test-driven development is applied to pipeline engineering. AI training and inference pipelines have enhanced test suites. Test results are part of the AI governance record.	Test-driven development is applied to pipeline engineering. AI training and inference pipelines have enhanced test suites. Test results are part of the AI governance record.	Test-driven development is applied to pipeline engineering. AI training and inference pipelines have enhanced test suites. Test results are part of the AI governance record.

D4.8 - Incident Response

Measure ID	Measure Name	Governs	Normative References
D4.8	Incident Response	Whether a defined, tested incident response process exists for pipeline failures, covering detection, communication, resolution, and post-incident review.	ISO 8000-61
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No incident response process. Failures are managed reactively by whoever notices them.	No incident response process. Failures are managed reactively by whoever notices them.	No incident response process. Failures are managed reactively by whoever notices them.
1 - Ad Hoc	Incidents are managed informally. No defined process.	Incidents are managed informally. No defined process.	Incidents are managed informally. No defined process.
2 - Repeatable	An incident response process exists for major pipelines. Not universally applied.	An incident response process exists for major pipelines. Not universally applied.	An incident response process exists for major pipelines. Not universally applied.
3 - Defined	A formal incident response process covers all critical pipelines. Roles and responsibilities are defined. Post-incident reviews are conducted.	A formal incident response process covers all critical pipelines. Roles and responsibilities are defined. Post-incident reviews are conducted.	A formal incident response process covers all critical pipelines. Roles and responsibilities are defined. Post-incident reviews are conducted.
4 - Managed	Incident response times are measured against SLAs. Recurring incidents trigger root cause programmes. Lessons learned are applied.	Incident response times are measured against SLAs. Recurring incidents trigger root cause programmes. Lessons learned are applied.	Incident response times are measured against SLAs. Recurring incidents trigger root cause programmes. Lessons learned are applied.
5 - Optimised	Incident response is integrated with observability tooling. AI pipeline incidents trigger enhanced response given model dependency. All incidents contribute to governance improvement.	Incident response is integrated with observability tooling. AI pipeline incidents trigger enhanced response given model dependency. All incidents contribute to governance improvement.	Incident response is integrated with observability tooling. AI pipeline incidents trigger enhanced response given model dependency. All incidents contribute to governance improvement.

D4.9 - Change Management

Measure ID	Measure Name	Governs	Normative References
D4.9	Change Management	Whether pipeline changes are subject to formal review, approval, and impact assessment before deployment.	ISO 8000-61 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Pipeline changes are made informally without review.	Pipeline changes are made informally without review.	Pipeline changes are made informally without review.
1 - Ad Hoc	Changes are discussed informally before implementation.	Changes are discussed informally before implementation.	Changes are discussed informally before implementation.
2 - Repeatable	A change management process exists for major pipelines. Informally applied.	A change management process exists for major pipelines. Informally applied.	A change management process exists for major pipelines. Informally applied.
3 - Defined	All critical pipeline changes are subject to formal review and approval. Impact assessment is conducted. Changes are documented.	All critical pipeline changes are subject to formal review and approval. Impact assessment is conducted. Changes are documented.	All critical pipeline changes are subject to formal review and approval. Impact assessment is conducted. Changes are documented.
4 - Managed	Change management is enforced through tooling. Changes to AI-feeding pipelines require enhanced review. Post-change validation is mandatory.	Change management is enforced through tooling. Changes to AI-feeding pipelines require enhanced review. Post-change validation is mandatory.	Change management is enforced through tooling. Changes to AI-feeding pipelines require enhanced review. Post-change validation is mandatory.
5 - Optimised	Change management is integrated with CI/CD pipeline governance. All changes are logged, reviewed, and linked to impact assessments. AI model re-validation is triggered by upstream pipeline changes.	Change management is integrated with CI/CD pipeline governance. All changes are logged, reviewed, and linked to impact assessments. AI model re-validation is triggered by upstream pipeline changes.	Change management is integrated with CI/CD pipeline governance. All changes are logged, reviewed, and linked to impact assessments. AI model re-validation is triggered by upstream pipeline changes.

D4.10 - Observability

Measure ID	Measure Name	Governs	Normative References
D4.10	Observability	Whether full observability is in place across pipeline stages, enabling end-to-end visibility of data flow, quality, and health.	ISO 8000-61 ISO 42001 Clause 9
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No observability. Pipeline state is unknown.	No observability. Pipeline state is unknown.	No observability. Pipeline state is unknown.
1 - Ad Hoc	Observability is limited to manual checks.	Observability is limited to manual checks.	Observability is limited to manual checks.
2 - Repeatable	Observability tooling is in place for major pipelines. Coverage is inconsistent.	Observability tooling is in place for major pipelines. Coverage is inconsistent.	Observability tooling is in place for major pipelines. Coverage is inconsistent.
3 - Defined	Observability covers all critical pipeline stages. Data lineage, quality metrics, and health indicators are visible.	Observability covers all critical pipeline stages. Data lineage, quality metrics, and health indicators are visible.	Observability covers all critical pipeline stages. Data lineage, quality metrics, and health indicators are visible.
4 - Managed	A unified observability platform provides end-to-end visibility. Dashboards are accessible to data owners and consumers. Anomalies are auto-detected.	A unified observability platform provides end-to-end visibility. Dashboards are accessible to data owners and consumers. Anomalies are auto-detected.	A unified observability platform provides end-to-end visibility. Dashboards are accessible to data owners and consumers. Anomalies are auto-detected.
5 - Optimised	Full observability is embedded in the data platform. AI pipeline observability includes training data quality, feature drift, and inference input quality.	Full observability is embedded in the data platform. AI pipeline observability includes training data quality, feature drift, and inference input quality.	Full observability is embedded in the data platform. AI pipeline observability includes training data quality, feature drift, and inference input quality.

6. Domain D5: AI Readiness & Provenance

Domain	AI Readiness & Provenance
Domain ID	D5
Weighting	8.33%
Measures	12
Purpose	AI systems are only as trustworthy as the data that shapes them. This domain governs the data governance controls specific to AI development and deployment: the provenance of training data, the quality of that data before use, the detection of bias and drift, the governance of features, and the controls on inputs at inference time. This is the domain most directly relevant to EU AI Act compliance and the domain where the consequences of poor governance are most severe. An AI model trained on unvalidated, undocumented, or biased data is not a governed asset - it is an ungoverned risk.
Regulatory Context	EU AI Act Articles 9, 10, 12, 13, 17 (risk management, data governance, logging, transparency, accuracy). ISO 42001 Clause 8 (operation, AI system development). GDPR Articles 5, 13, 22 (data quality, transparency, automated decision-making). NIST AI RMF Govern, Map, Measure, Manage functions.

D5.1 - Training Data Provenance

Measure ID	Measure Name	Governs	Normative References
D5.1	Training Data Provenance	Whether the origin, lineage, version, and transformation history of all training data is documented and maintained for every AI system in production.	EU AI Act Art.10 ISO 42001 Clause 8.4 NIST AI RMF
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No provenance documentation for training data. Data origin is unknown.	No provenance documentation for training data. Data origin is unknown.	No provenance documentation for training data. Data origin is unknown.
1 - Ad Hoc	Provenance is informally understood by model developers. Not documented.	Provenance is informally understood by model developers. Not documented.	Provenance is informally understood by model developers. Not documented.
2 - Repeatable	Provenance is documented for some AI systems. No standard approach. Documentation is not maintained after model deployment.	Provenance is documented for some AI systems. No standard approach. Documentation is not maintained after model deployment.	Provenance is documented for some AI systems. No standard approach. Documentation is not maintained after model deployment.
3 - Defined	Training data provenance is formally documented for all AI systems in production. Documentation covers origin, version, and key transformations. Maintained when models are updated.	Training data provenance is formally documented for all AI systems in production. Documentation covers origin, version, and key transformations. Maintained when models are updated.	Training data provenance is formally documented for all AI systems in production. Documentation covers origin, version, and key transformations. Maintained when models are updated.
4 - Managed	Provenance documentation is version-controlled alongside model artefacts. Changes to training data trigger provenance record updates. Documentation is reviewed at each model update.	Provenance documentation is version-controlled alongside model artefacts. Changes to training data trigger provenance record updates. Documentation is reviewed at each model update.	Provenance documentation is version-controlled alongside model artefacts. Changes to training data trigger provenance record updates. Documentation is reviewed at each model update.
5 - Optimised	Full provenance is automatically captured and maintained. Lineage covers raw source through to model training. Provenance records support regulatory audit and model reproducibility.	Full provenance is automatically captured and maintained. Lineage covers raw source through to model training. Provenance records support regulatory audit and model reproducibility.	Full provenance is automatically captured and maintained. Lineage covers raw source through to model training. Provenance records support regulatory audit and model reproducibility.

D5.2 - Training Data Quality

Measure ID	Measure Name	Governs	Normative References
D5.2	Training Data Quality	Whether training data is formally assessed against defined quality thresholds before model development begins.	EU AI Act Art.10 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Training data quality is not assessed. Models are trained on whatever data is available.	Training data quality is not assessed. Models are trained on whatever data is available.	Training data quality is not assessed. Models are trained on whatever data is available.
1 - Ad Hoc	Quality is informally reviewed by model developers before training.	Quality is informally reviewed by model developers before training.	Quality is informally reviewed by model developers before training.
2 - Repeatable	Quality is assessed for some AI initiatives. No defined thresholds. Assessment is not documented.	Quality is assessed for some AI initiatives. No defined thresholds. Assessment is not documented.	Quality is assessed for some AI initiatives. No defined thresholds. Assessment is not documented.
3 - Defined	Formal quality thresholds are defined for training data. Assessment is conducted and documented before model development begins. Subthreshold data is rejected or remediated.	Formal quality thresholds are defined for training data. Assessment is conducted and documented before model development begins. Subthreshold data is rejected or remediated.	Formal quality thresholds are defined for training data. Assessment is conducted and documented before model development begins. Subthreshold data is rejected or remediated.
4 - Managed	Quality assessment results are recorded alongside model artefacts. Threshold definitions are reviewed and updated based on model performance data.	Quality assessment results are recorded alongside model artefacts. Threshold definitions are reviewed and updated based on model performance data.	Quality assessment results are recorded alongside model artefacts. Threshold definitions are reviewed and updated based on model performance data.
5 - Optimised	Training data quality assessment is automated. AI systems cannot enter development without a passed quality gate. Assessment results are part of the model governance record.	Training data quality assessment is automated. AI systems cannot enter development without a passed quality gate. Assessment results are part of the model governance record.	Training data quality assessment is automated. AI systems cannot enter development without a passed quality gate. Assessment results are part of the model governance record.

D5.3 - Bias & Representativeness

Measure ID	Measure Name	Governs	Normative References
D5.3	Bias & Representativeness	Whether training datasets are formally assessed for bias and demographic or structural representativeness before use.	EU AI Act Art.10 ISO 42001 Clause 8.4 NIST AI RMF
MATURITY LEVEL DESC IPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No bias assessment. Representativeness is not considered.	No bias assessment. Representativeness is not considered.	No bias assessment. Representativeness is not considered.
1 - Ad Hoc	Bias is discussed informally among model developers. No formal assessment.	Bias is discussed informally among model developers. No formal assessment.	Bias is discussed informally among model developers. No formal assessment.
2 - Repeatable	Bias assessment is conducted for some AI systems. No standard methodology. Results are not documented.	Bias assessment is conducted for some AI systems. No standard methodology. Results are not documented.	Bias assessment is conducted for some AI systems. No standard methodology. Results are not documented.
3 - Defined	A formal bias and representativeness assessment is conducted for all AI training datasets before model development. Methodology is defined. Results are documented.	A formal bias and representativeness assessment is conducted for all AI training datasets before model development. Methodology is defined. Results are documented.	A formal bias and representativeness assessment is conducted for all AI training datasets before model development. Methodology is defined. Results are documented.
4 - Managed	Bias assessment results inform model development decisions. Identified bias is addressed before training or formally accepted with documented rationale. Assessment is repeated when training data changes.	Bias assessment results inform model development decisions. Identified bias is addressed before training or formally accepted with documented rationale. Assessment is repeated when training data changes.	Bias assessment results inform model development decisions. Identified bias is addressed before training or formally accepted with documented rationale. Assessment is repeated when training data changes.
5 - Optimised	Bias governance is embedded in the AI development lifecycle. Automated bias detection tools supplement manual assessment. Post-deployment bias monitoring is in place.	Bias governance is embedded in the AI development lifecycle. Automated bias detection tools supplement manual assessment. Post-deployment bias monitoring is in place.	Bias governance is embedded in the AI development lifecycle. Automated bias detection tools supplement manual assessment. Post-deployment bias monitoring is in place.

D5.4 - Labelling Quality

Measure ID	Measure Name	Governs	Normative References
D5.4	Labelling Quality	Where labelled data is used, whether labelling accuracy, inter-annotator agreement, and labelling process governance are documented.	EU AI Act Art.10 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No labelling governance. Label quality is unknown.	No labelling governance. Label quality is unknown.	No labelling governance. Label quality is unknown.
1 - Ad Hoc	Labelling is performed by available staff without training or quality control.	Labelling is performed by available staff without training or quality control.	Labelling is performed by available staff without training or quality control.
2 - Repeatable	Labelling guidelines exist for some AI systems. Quality checks are informal.	Labelling guidelines exist for some AI systems. Quality checks are informal.	Labelling guidelines exist for some AI systems. Quality checks are informal.
3 - Defined	Labelling process is formally documented. Inter-annotator agreement is measured. Quality thresholds are defined and enforced.	Labelling process is formally documented. Inter-annotator agreement is measured. Quality thresholds are defined and enforced.	Labelling process is formally documented. Inter-annotator agreement is measured. Quality thresholds are defined and enforced.
4 - Managed	Labelling quality is tracked over time. Labellers are trained and assessed. Disagreements are resolved through a defined arbitration process.	Labelling quality is tracked over time. Labellers are trained and assessed. Disagreements are resolved through a defined arbitration process.	Labelling quality is tracked over time. Labellers are trained and assessed. Disagreements are resolved through a defined arbitration process.
5 - Optimised	Labelling governance is embedded in the AI development platform. Label quality metrics are part of the model governance record. Third-party labelling is subject to the same standards.	Labelling governance is embedded in the AI development platform. Label quality metrics are part of the model governance record. Third-party labelling is subject to the same standards.	Labelling governance is embedded in the AI development platform. Label quality metrics are part of the model governance record. Third-party labelling is subject to the same standards.

D5.5 - Feature Engineering Governance

Measure ID	Measure Name	Governs	Normative References
D5.5	Feature Engineering Governance	Whether feature definitions, transformations, and selections are documented, versioned, and governed.	ISO 42001 Clause 8.4 EU AI Act Art.10,12
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Feature engineering is undocumented. Features cannot be reproduced or explained.	Feature engineering is undocumented. Features cannot be reproduced or explained.	Feature engineering is undocumented. Features cannot be reproduced or explained.
1 - Ad Hoc	Feature definitions are informally understood by model developers. Not documented.	Feature definitions are informally understood by model developers. Not documented.	Feature definitions are informally understood by model developers. Not documented.
2 - Repeatable	Feature definitions are documented for some AI systems. No versioning.	Feature definitions are documented for some AI systems. No versioning.	Feature definitions are documented for some AI systems. No versioning.
3 - Defined	Feature definitions and transformation logic are documented and version-controlled for all AI systems. Changes follow a formal review process.	Feature definitions and transformation logic are documented and version-controlled for all AI systems. Changes follow a formal review process.	Feature definitions and transformation logic are documented and version-controlled for all AI systems. Changes follow a formal review process.
4 - Managed	Feature store is in place. Features are reusable and governed. Lineage from raw data to feature is maintained.	Feature store is in place. Features are reusable and governed. Lineage from raw data to feature is maintained.	Feature store is in place. Features are reusable and governed. Lineage from raw data to feature is maintained.
5 - Optimised	Feature governance is automated. Features cannot be used in production without formal registration and documentation. Feature lineage is part of the AI provenance record.	Feature governance is automated. Features cannot be used in production without formal registration and documentation. Feature lineage is part of the AI provenance record.	Feature governance is automated. Features cannot be used in production without formal registration and documentation. Feature lineage is part of the AI provenance record.

D5.6 - Input Validation

Measure ID	Measure Name	Governs	Normative References
D5.6	Input Validation	Whether AI model inputs are validated against defined schemas and quality thresholds at inference time.	EU AI Act Art.9,10 ISO 42001 Clause 8.5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No input validation at inference. Models receive whatever data is presented.	No input validation at inference. Models receive whatever data is presented.	No input validation at inference. Models receive whatever data is presented.
1 - Ad Hoc	Input format is validated informally for some models.	Input format is validated informally for some models.	Input format is validated informally for some models.
2 - Repeatable	Schema validation is in place for major AI systems. Quality threshold validation is absent.	Schema validation is in place for major AI systems. Quality threshold validation is absent.	Schema validation is in place for major AI systems. Quality threshold validation is absent.
3 - Defined	Schema and quality threshold validation are applied to all production AI model inputs. Invalid inputs are rejected or flagged.	Schema and quality threshold validation are applied to all production AI model inputs. Invalid inputs are rejected or flagged.	Schema and quality threshold validation are applied to all production AI model inputs. Invalid inputs are rejected or flagged.
4 - Managed	Input validation rules are version-controlled and linked to model versions. Validation failures are logged and investigated. Validation rules are reviewed when models are updated.	Input validation rules are version-controlled and linked to model versions. Validation failures are logged and investigated. Validation rules are reviewed when models are updated.	Input validation rules are version-controlled and linked to model versions. Validation failures are logged and investigated. Validation rules are reviewed when models are updated.
5 - Optimised	Input validation is automated and enforced by the AI serving infrastructure. Validation failures trigger incident workflows. AI systems cannot accept inputs that fail governance controls.	Input validation is automated and enforced by the AI serving infrastructure. Validation failures trigger incident workflows. AI systems cannot accept inputs that fail governance controls.	Input validation is automated and enforced by the AI serving infrastructure. Validation failures trigger incident workflows. AI systems cannot accept inputs that fail governance controls.

D5.7 - Data Drift Detection

Measure ID	Measure Name	Governs	Normative References
D5.7	Data Drift Detection	Whether mechanisms are in place to detect and alert on statistical drift in the data distributions used by AI models.	EU AI Act Art.9,12 ISO 42001 Clause 9 NIST AI RMF
MATURITY LEVEL DESCR IPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No drift detection. Models continue operating regardless of data distribution changes.	No drift detection. Models continue operating regardless of data distribution changes.	No drift detection. Models continue operating regardless of data distribution changes.
1 - Ad Hoc	Drift is detected manually when model performance visibly degrades.	Drift is detected manually when model performance visibly degrades.	Drift is detected manually when model performance visibly degrades.
2 - Repeatable	Drift monitoring is in place for some AI systems. No automated alerting.	Drift monitoring is in place for some AI systems. No automated alerting.	Drift monitoring is in place for some AI systems. No automated alerting.
3 - Defined	Drift detection is in place for all production AI systems. Automated alerts are triggered when drift thresholds are exceeded.	Drift detection is in place for all production AI systems. Automated alerts are triggered when drift thresholds are exceeded.	Drift detection is in place for all production AI systems. Automated alerts are triggered when drift thresholds are exceeded.
4 - Managed	Drift thresholds are calibrated based on model sensitivity. Drift alerts trigger model review. Drift history is maintained alongside model performance data.	Drift thresholds are calibrated based on model sensitivity. Drift alerts trigger model review. Drift history is maintained alongside model performance data.	Drift thresholds are calibrated based on model sensitivity. Drift alerts trigger model review. Drift history is maintained alongside model performance data.
5 - Optimised	Drift monitoring is integrated with the AI platform. Detected drift triggers automated model re-evaluation and may suspend model operation pending review.	Drift monitoring is integrated with the AI platform. Detected drift triggers automated model re-evaluation and may suspend model operation pending review.	Drift monitoring is integrated with the AI platform. Detected drift triggers automated model re-evaluation and may suspend model operation pending review.

D5.8 - Model-Data Traceability

Measure ID	Measure Name	Governs	Normative References
D5.8	Model-Data Traceability	Whether the data used to train each version of each model can be fully identified, documented, and reconstructed for audit purposes.	EU AI Act Art.10,12 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Training data cannot be identified after model deployment.	Training data cannot be identified after model deployment.	Training data cannot be identified after model deployment.
1 - Ad Hoc	Training data is informally known to model developers. Not recorded.	Training data is informally known to model developers. Not recorded.	Training data is informally known to model developers. Not recorded.
2 - Repeatable	Training data is documented for some model versions. Reconstruction is not always possible.	Training data is documented for some model versions. Reconstruction is not always possible.	Training data is documented for some model versions. Reconstruction is not always possible.
3 - Defined	The data used to train each model version is formally documented and reproducible. Documentation is maintained for the life of the model.	The data used to train each model version is formally documented and reproducible. Documentation is maintained for the life of the model.	The data used to train each model version is formally documented and reproducible. Documentation is maintained for the life of the model.
4 - Managed	Training data documentation is version-controlled alongside model artefacts. Data can be reconstructed from documented sources. Documentation is reviewed at each model update.	Training data documentation is version-controlled alongside model artefacts. Data can be reconstructed from documented sources. Documentation is reviewed at each model update.	Training data documentation is version-controlled alongside model artefacts. Data can be reconstructed from documented sources. Documentation is reviewed at each model update.
5 - Optimised	Full model-data traceability is automated. Any version of any production model can be reproduced from its documented training data. Traceability supports regulatory audit and model challenge.	Full model-data traceability is automated. Any version of any production model can be reproduced from its documented training data. Traceability supports regulatory audit and model challenge.	Full model-data traceability is automated. Any version of any production model can be reproduced from its documented training data. Traceability supports regulatory audit and model challenge.

D5.9 - AI Data Retention

Measure ID	Measure Name	Governs	Normative References
D5.9	AI Data Retention	Whether datasets used for AI training are retained, versioned, and accessible for audit for appropriate periods.	EU AI Act Art.12 ISO 42001 Clause 7.5 GDPR Art.5(1)(e)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Training data is not retained after model deployment.	Training data is not retained after model deployment.	Training data is not retained after model deployment.
1 - Ad Hoc	Retention is informal. Some training data may be retained by model developers on local systems.	Retention is informal. Some training data may be retained by model developers on local systems.	Retention is informal. Some training data may be retained by model developers on local systems.
2 - Repeatable	Retention policy exists for some AI training data. Versioning is absent.	Retention policy exists for some AI training data. Versioning is absent.	Retention policy exists for some AI training data. Versioning is absent.
3 - Defined	AI training datasets are formally retained and versioned for defined periods. Retention periods are aligned to model lifecycle and regulatory requirements.	AI training datasets are formally retained and versioned for defined periods. Retention periods are aligned to model lifecycle and regulatory requirements.	AI training datasets are formally retained and versioned for defined periods. Retention periods are aligned to model lifecycle and regulatory requirements.
4 - Managed	Retention is managed systematically. Datasets are accessible to authorised parties. Retention periods are reviewed when regulations change.	Retention is managed systematically. Datasets are accessible to authorised parties. Retention periods are reviewed when regulations change.	Retention is managed systematically. Datasets are accessible to authorised parties. Retention periods are reviewed when regulations change.
5 - Optimised	AI data retention is governed as part of the AI lifecycle. Datasets are retained in governed storage. Retention records are part of the AI audit trail.	AI data retention is governed as part of the AI lifecycle. Datasets are retained in governed storage. Retention records are part of the AI audit trail.	AI data retention is governed as part of the AI lifecycle. Datasets are retained in governed storage. Retention records are part of the AI audit trail.

D5.10 - Consent & Personal Data Provenance

Measure ID	Measure Name	Governs	Normative References
D5.10	Consent & Personal Data Provenance	Whether personal data used in AI systems is governed with documented consent, purpose limitation, and provenance records.	GDPR Art.5,6,13,22 EU AI Act Art.10 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Personal data is used in AI systems without consent governance or purpose documentation.	Personal data is used in AI systems without consent governance or purpose documentation.	Personal data is used in AI systems without consent governance or purpose documentation.
1 - Ad Hoc	Consent is managed at a system level but AI-specific use is not documented.	Consent is managed at a system level but AI-specific use is not documented.	Consent is managed at a system level but AI-specific use is not documented.
2 - Repeatable	Consent records exist but AI-specific purpose limitation is not explicitly documented.	Consent records exist but AI-specific purpose limitation is not explicitly documented.	Consent records exist but AI-specific purpose limitation is not explicitly documented.
3 - Defined	Personal data use in AI systems is documented with consent basis, purpose limitation, and provenance records. AI-specific consent is explicit where required.	Personal data use in AI systems is documented with consent basis, purpose limitation, and provenance records. AI-specific consent is explicit where required.	Personal data use in AI systems is documented with consent basis, purpose limitation, and provenance records. AI-specific consent is explicit where required.
4 - Managed	Consent and purpose documentation is maintained alongside model artefacts. Changes to AI use of personal data trigger consent review.	Consent and purpose documentation is maintained alongside model artefacts. Changes to AI use of personal data trigger consent review.	Consent and purpose documentation is maintained alongside model artefacts. Changes to AI use of personal data trigger consent review.
5 - Optimised	Consent governance for AI is automated. Personal data cannot be used in AI training without a verified consent record. Purpose limitation is enforced technically.	Consent governance for AI is automated. Personal data cannot be used in AI training without a verified consent record. Purpose limitation is enforced technically.	Consent governance for AI is automated. Personal data cannot be used in AI training without a verified consent record. Purpose limitation is enforced technically.

D5.11 - Synthetic & Augmented Data Controls

Measure ID	Measure Name	Governs	Normative References
D5.11	Synthetic & Augmented Data Controls	Where synthetic or augmented data is used in AI development, whether its generation, scope, and limitations are governed.	EU AI Act Art.10 ISO 42001 Clause 8.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Synthetic data is used without governance. Generation methods and limitations are undocumented.	Synthetic data is used without governance. Generation methods and limitations are undocumented.	Synthetic data is used without governance. Generation methods and limitations are undocumented.
1 - Ad Hoc	Synthetic data use is informally tracked.	Synthetic data use is informally tracked.	Synthetic data use is informally tracked.
2 - Repeatable	Synthetic data generation is documented for some AI systems. Limitations are not formally assessed.	Synthetic data generation is documented for some AI systems. Limitations are not formally assessed.	Synthetic data generation is documented for some AI systems. Limitations are not formally assessed.
3 - Defined	Synthetic data generation methods, scope, and limitations are formally documented. Use of synthetic data is approved through a defined process.	Synthetic data generation methods, scope, and limitations are formally documented. Use of synthetic data is approved through a defined process.	Synthetic data generation methods, scope, and limitations are formally documented. Use of synthetic data is approved through a defined process.
4 - Managed	Synthetic data governance includes quality assessment, bias evaluation, and limitation documentation. Synthetic data is labelled and tracked separately from real data.	Synthetic data governance includes quality assessment, bias evaluation, and limitation documentation. Synthetic data is labelled and tracked separately from real data.	Synthetic data governance includes quality assessment, bias evaluation, and limitation documentation. Synthetic data is labelled and tracked separately from real data.
5 - Optimised	Synthetic data is governed as a formal data asset. Generation models are version-controlled. Synthetic data cannot be used in production AI without a governance approval.	Synthetic data is governed as a formal data asset. Generation models are version-controlled. Synthetic data cannot be used in production AI without a governance approval.	Synthetic data is governed as a formal data asset. Generation models are version-controlled. Synthetic data cannot be used in production AI without a governance approval.

D5.12 - AI Readiness Gate

Measure ID	Measure Name	Governs	Normative References
D5.12	AI Readiness Gate	Whether a formal process exists to certify that data is ready before AI initiatives are permitted to begin development or deployment.	EU AI Act Art.9,10 ISO 42001 Clause 8.4 NIST AI RMF
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No readiness gate. AI initiatives begin without data governance assessment.	No readiness gate. AI initiatives begin without data governance assessment.	No readiness gate. AI initiatives begin without data governance assessment.
1 - Ad Hoc	Readiness is informally assessed by model developers or project managers.	Readiness is informally assessed by model developers or project managers.	Readiness is informally assessed by model developers or project managers.
2 - Repeatable	An informal readiness review occurs for major AI initiatives. No standard criteria.	An informal readiness review occurs for major AI initiatives. No standard criteria.	An informal readiness review occurs for major AI initiatives. No standard criteria.
3 - Defined	A formal AI readiness gate is defined and applied before all AI initiatives. Gate criteria cover data quality, provenance, bias assessment, and consent. Results are documented.	A formal AI readiness gate is defined and applied before all AI initiatives. Gate criteria cover data quality, provenance, bias assessment, and consent. Results are documented.	A formal AI readiness gate is defined and applied before all AI initiatives. Gate criteria cover data quality, provenance, bias assessment, and consent. Results are documented.
4 - Managed	The readiness gate is enforced. AI initiatives cannot proceed without a gate pass. Gate outcomes are reviewed by data governance leadership.	The readiness gate is enforced. AI initiatives cannot proceed without a gate pass. Gate outcomes are reviewed by data governance leadership.	The readiness gate is enforced. AI initiatives cannot proceed without a gate pass. Gate outcomes are reviewed by data governance leadership.
5 - Optimised	The readiness gate is embedded in the AI governance lifecycle. Gate passes are version-controlled. Failed gates trigger a defined remediation process. Gate outcomes are part of the AI audit trail.	The readiness gate is embedded in the AI governance lifecycle. Gate passes are version-controlled. Failed gates trigger a defined remediation process. Gate outcomes are part of the AI audit trail.	The readiness gate is embedded in the AI governance lifecycle. Gate passes are version-controlled. Failed gates trigger a defined remediation process. Gate outcomes are part of the AI audit trail.

7. Domain D6: Governance & Compliance

Domain	Governance & Compliance
Domain ID	D6
Weighting	8.33%
Measures	10
Purpose	This domain governs the structural governance layer: the policies, processes, metadata management, lineage transparency, and regulatory compliance controls that make data quality governance enforceable rather than aspirational. It is the bridge between ownership (Domain 2) and operational quality (Domains 3 and 4), providing the formal framework within which quality is defined, enforced, and audited. Organisations with strong governance and compliance maturity can demonstrate to regulators, auditors, and customers that their data and AI practices are controlled.
Regulatory Context	ISO 8000-8 Clause 4-10 (full standard). ISO 42001 Clauses 4-10. EU AI Act Articles 9, 11, 12, 17 (risk management, technical documentation, logging, quality management). GDPR Articles 5, 24, 25, 30 (principles, accountability, privacy by design, records of processing).

D6.1 - Policy Framework

Measure ID	Measure Name	Governs	Normative References
D6.1	Policy Framework	Whether a documented, published, and enforced data governance policy framework exists.	ISO 8000-8 Clause 5 ISO 42001 Clause 5 GDPR Art.24
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No governance policies exist.	No governance policies exist.	No governance policies exist.
1 - Ad Hoc	Governance principles are informally understood but not documented.	Governance principles are informally understood but not documented.	Governance principles are informally understood but not documented.
2 - Repeatable	Policies exist as documents but are not published, enforced, or consistently applied.	Policies exist as documents but are not published, enforced, or consistently applied.	Policies exist as documents but are not published, enforced, or consistently applied.
3 - Defined	A formal governance policy framework is documented, published, and reviewed on a defined cycle. Policies cover data quality, ownership, access, and AI governance.	A formal governance policy framework is documented, published, and reviewed on a defined cycle. Policies cover data quality, ownership, access, and AI governance.	A formal governance policy framework is documented, published, and reviewed on a defined cycle. Policies cover data quality, ownership, access, and AI governance.
4 - Managed	Policies are enforced through process and tooling. Compliance with policies is audited. Policy exceptions require formal approval.	Policies are enforced through process and tooling. Compliance with policies is audited. Policy exceptions require formal approval.	Policies are enforced through process and tooling. Compliance with policies is audited. Policy exceptions require formal approval.
5 - Optimised	The policy framework is the authoritative governance reference. Policies are embedded in process automation. Policy compliance is continuously monitored.	The policy framework is the authoritative governance reference. Policies are embedded in process automation. Policy compliance is continuously monitored.	The policy framework is the authoritative governance reference. Policies are embedded in process automation. Policy compliance is continuously monitored.

D6.2 - Metadata Management

Measure ID	Measure Name	Governs	Normative References
D6.2	Metadata Management	Whether business and technical metadata is captured, maintained, and made discoverable for all critical data assets.	ISO 8000-8 DAMA DMBOK Ch.12
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No metadata management. Data assets are discovered informally.	No metadata management. Data assets are discovered informally.	No metadata management. Data assets are discovered informally.
1 - Ad Hoc	Metadata is captured informally in spreadsheets or wikis. Not maintained.	Metadata is captured informally in spreadsheets or wikis. Not maintained.	Metadata is captured informally in spreadsheets or wikis. Not maintained.
2 - Repeatable	A data catalog captures metadata for major assets. Coverage is partial.	A data catalog captures metadata for major assets. Coverage is partial.	A data catalog captures metadata for major assets. Coverage is partial.
3 - Defined	A governed data catalog captures and maintains business and technical metadata for all critical data assets. Ownership is assigned. Metadata is kept current.	A governed data catalog captures and maintains business and technical metadata for all critical data assets. Ownership is assigned. Metadata is kept current.	A governed data catalog captures and maintains business and technical metadata for all critical data assets. Ownership is assigned. Metadata is kept current.
4 - Managed	Metadata completeness is measured and enforced. New data assets require metadata before cataloguing. Metadata quality is monitored.	Metadata completeness is measured and enforced. New data assets require metadata before cataloguing. Metadata quality is monitored.	Metadata completeness is measured and enforced. New data assets require metadata before cataloguing. Metadata quality is monitored.
5 - Optimised	Metadata is the single source of truth for data asset discovery. AI model metadata including training data references and feature definitions is governed in the catalog.	Metadata is the single source of truth for data asset discovery. AI model metadata including training data references and feature definitions is governed in the catalog.	Metadata is the single source of truth for data asset discovery. AI model metadata including training data references and feature definitions is governed in the catalog.

D6.3 - Lineage Transparency

Measure ID	Measure Name	Governs	Normative References
D6.3	Lineage Transparency	Whether data lineage can be traced from source to report or AI model for all critical data assets.	ISO 8000-110 EU AI Act Art.12 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No lineage capability. Data origin and transformation history are unknown.	No lineage capability. Data origin and transformation history are unknown.	No lineage capability. Data origin and transformation history are unknown.
1 - Ad Hoc	Lineage is informally known to individual data engineers.	Lineage is informally known to individual data engineers.	Lineage is informally known to individual data engineers.
2 - Repeatable	Lineage is documented manually for major data flows. Not maintained.	Lineage is documented manually for major data flows. Not maintained.	Lineage is documented manually for major data flows. Not maintained.
3 - Defined	Lineage is captured and available for all critical data assets from source to consumption point. Lineage is maintained when pipelines change.	Lineage is captured and available for all critical data assets from source to consumption point. Lineage is maintained when pipelines change.	Lineage is captured and available for all critical data assets from source to consumption point. Lineage is maintained when pipelines change.
4 - Managed	Lineage is automatically captured by the data platform. Changes to pipelines trigger lineage updates. Lineage is available to data owners and consumers on demand.	Lineage is automatically captured by the data platform. Changes to pipelines trigger lineage updates. Lineage is available to data owners and consumers on demand.	Lineage is automatically captured by the data platform. Changes to pipelines trigger lineage updates. Lineage is available to data owners and consumers on demand.
5 - Optimised	Full end-to-end lineage is maintained automatically including AI training data lineage, feature engineering, and inference inputs. Lineage is part of the AI governance audit trail.	Full end-to-end lineage is maintained automatically including AI training data lineage, feature engineering, and inference inputs. Lineage is part of the AI governance audit trail.	Full end-to-end lineage is maintained automatically including AI training data lineage, feature engineering, and inference inputs. Lineage is part of the AI governance audit trail.

D6.4 - Regulatory Compliance

Measure ID	Measure Name	Governs	Normative References
D6.4	Regulatory Compliance	Whether regulatory data requirements are embedded in processes and regularly audited for compliance.	GDPR Art.5,24,30 EU AI Act Art.9,17 ISO 42001 Clause 9
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Regulatory requirements are not systematically addressed.	Regulatory requirements are not systematically addressed.	Regulatory requirements are not systematically addressed.
1 - Ad Hoc	Compliance is managed reactively. No proactive programme.	Compliance is managed reactively. No proactive programme.	Compliance is managed reactively. No proactive programme.
2 - Repeatable	Key regulatory requirements are documented. Compliance is checked periodically.	Key regulatory requirements are documented. Compliance is checked periodically.	Key regulatory requirements are documented. Compliance is checked periodically.
3 - Defined	Regulatory requirements are embedded in data governance processes. Compliance is audited on a defined cycle. Findings are tracked and remediated.	Regulatory requirements are embedded in data governance processes. Compliance is audited on a defined cycle. Findings are tracked and remediated.	Regulatory requirements are embedded in data governance processes. Compliance is audited on a defined cycle. Findings are tracked and remediated.
4 - Managed	Compliance monitoring is continuous. Regulatory changes trigger impact assessment on existing processes. Compliance evidence is maintained.	Compliance monitoring is continuous. Regulatory changes trigger impact assessment on existing processes. Compliance evidence is maintained.	Compliance monitoring is continuous. Regulatory changes trigger impact assessment on existing processes. Compliance evidence is maintained.
5 - Optimised	Regulatory compliance is embedded in process automation. Evidence is continuously collected. Regulatory change is tracked through a formal horizon-scanning process.	Regulatory compliance is embedded in process automation. Evidence is continuously collected. Regulatory change is tracked through a formal horizon-scanning process.	Regulatory compliance is embedded in process automation. Evidence is continuously collected. Regulatory change is tracked through a formal horizon-scanning process.

D6.5 - EU AI Act Alignment

Measure ID	Measure Name	Governs	Normative References
D6.5	EU AI Act Alignment	Whether AI systems have been assessed against EU AI Act obligations including risk classification, and whether required controls are in place.	EU AI Act Art.6,9,10,11,12,13,17,52
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No EU AI Act assessment conducted.	No EU AI Act assessment conducted.	No EU AI Act assessment conducted.
1 - Ad Hoc	EU AI Act is known but no formal assessment has been initiated.	EU AI Act is known but no formal assessment has been initiated.	EU AI Act is known but no formal assessment has been initiated.
2 - Repeatable	A high-level EU AI Act scoping exercise has been conducted. Risk classification is incomplete.	A high-level EU AI Act scoping exercise has been conducted. Risk classification is incomplete.	A high-level EU AI Act scoping exercise has been conducted. Risk classification is incomplete.
3 - Defined	All AI systems have been classified against EU AI Act risk tiers. Required controls for each tier have been identified. A compliance programme is underway.	All AI systems have been classified against EU AI Act risk tiers. Required controls for each tier have been identified. A compliance programme is underway.	All AI systems have been classified against EU AI Act risk tiers. Required controls for each tier have been identified. A compliance programme is underway.
4 - Managed	Compliance controls for all AI systems are implemented. High-risk system obligations including technical documentation, human oversight, and logging are in place.	Compliance controls for all AI systems are implemented. High-risk system obligations including technical documentation, human oversight, and logging are in place.	Compliance controls for all AI systems are implemented. High-risk system obligations including technical documentation, human oversight, and logging are in place.
5 - Optimised	EU AI Act compliance is embedded in the AI governance lifecycle. New AI systems are assessed at initiation. Compliance evidence is maintained in the AI audit trail.	EU AI Act compliance is embedded in the AI governance lifecycle. New AI systems are assessed at initiation. Compliance evidence is maintained in the AI audit trail.	EU AI Act compliance is embedded in the AI governance lifecycle. New AI systems are assessed at initiation. Compliance evidence is maintained in the AI audit trail.

D6.6 - ISO 42001 Alignment

Measure ID	Measure Name	Governs	Normative References
D6.6	ISO 42001 Alignment	Whether an AI Management System aligned to ISO/IEC 42001 is in place or formally in development.	ISO 42001 Clauses 4-10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No awareness of ISO 42001.	No awareness of ISO 42001.	No awareness of ISO 42001.
1 - Ad Hoc	ISO 42001 is known. No assessment or alignment work has been initiated.	ISO 42001 is known. No assessment or alignment work has been initiated.	ISO 42001 is known. No assessment or alignment work has been initiated.
2 - Repeatable	A gap assessment against ISO 42001 has been completed. Alignment programme is planned.	A gap assessment against ISO 42001 has been completed. Alignment programme is planned.	A gap assessment against ISO 42001 has been completed. Alignment programme is planned.
3 - Defined	An ISO 42001 alignment programme is active. Key clauses are implemented. A target implementation date is defined.	An ISO 42001 alignment programme is active. Key clauses are implemented. A target implementation date is defined.	An ISO 42001 alignment programme is active. Key clauses are implemented. A target implementation date is defined.
4 - Managed	ISO 42001 alignment is substantially complete. An internal audit against the standard has been conducted. Findings are being addressed.	ISO 42001 alignment is substantially complete. An internal audit against the standard has been conducted. Findings are being addressed.	ISO 42001 alignment is substantially complete. An internal audit against the standard has been conducted. Findings are being addressed.
5 - Optimised	ISO 42001 certification is achieved or actively pursued. The AI management system is operational. Continual improvement is embedded.	ISO 42001 certification is achieved or actively pursued. The AI management system is operational. Continual improvement is embedded.	ISO 42001 certification is achieved or actively pursued. The AI management system is operational. Continual improvement is embedded.

D6.7 - Quality Issue Management

Measure ID	Measure Name	Governs	Normative References
D6.7	Quality Issue Management	Whether a centralised register for data quality issues exists with root cause analysis and remediation tracking.	ISO 8000-61 ISO 42001 Clause 10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No issue register. Quality issues are managed informally or not at all.	No issue register. Quality issues are managed informally or not at all.	No issue register. Quality issues are managed informally or not at all.
1 - Ad Hoc	Issues are raised informally. No central tracking.	Issues are raised informally. No central tracking.	Issues are raised informally. No central tracking.
2 - Repeatable	An issue register exists for some domains. Root cause analysis is inconsistent.	An issue register exists for some domains. Root cause analysis is inconsistent.	An issue register exists for some domains. Root cause analysis is inconsistent.
3 - Defined	A centralised data quality issue register covers all critical domains. Issues are logged, assigned, root-caused, and tracked to closure.	A centralised data quality issue register covers all critical domains. Issues are logged, assigned, root-caused, and tracked to closure.	A centralised data quality issue register covers all critical domains. Issues are logged, assigned, root-caused, and tracked to closure.
4 - Managed	Issue trends are analysed. Recurring issues trigger systemic remediation. Issue management data informs governance programme priorities.	Issue trends are analysed. Recurring issues trigger systemic remediation. Issue management data informs governance programme priorities.	Issue trends are analysed. Recurring issues trigger systemic remediation. Issue management data informs governance programme priorities.
5 - Optimised	Issue management is integrated with observability tooling. Issues are auto-detected and logged. AI-related quality issues trigger enhanced investigation.	Issue management is integrated with observability tooling. Issues are auto-detected and logged. AI-related quality issues trigger enhanced investigation.	Issue management is integrated with observability tooling. Issues are auto-detected and logged. AI-related quality issues trigger enhanced investigation.

D6.8 - Policy Enforcement

Measure ID	Measure Name	Governs	Normative References
D6.8	Policy Enforcement	Whether governance policies are enforced through automated controls rather than relying solely on manual compliance.	ISO 8000-8 ISO 42001 Clause 8 GDPR Art.25
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Policies are not enforced. Compliance depends entirely on individual behaviour.	Policies are not enforced. Compliance depends entirely on individual behaviour.	Policies are not enforced. Compliance depends entirely on individual behaviour.
1 - Ad Hoc	Enforcement is verbal or through peer pressure. No process controls.	Enforcement is verbal or through peer pressure. No process controls.	Enforcement is verbal or through peer pressure. No process controls.
2 - Repeatable	Some policies are enforced through process controls. Manual compliance checking.	Some policies are enforced through process controls. Manual compliance checking.	Some policies are enforced through process controls. Manual compliance checking.
3 - Defined	Key governance policies are enforced through defined process controls. Automated controls are in place for some policies. Exceptions require formal approval.	Key governance policies are enforced through defined process controls. Automated controls are in place for some policies. Exceptions require formal approval.	Key governance policies are enforced through defined process controls. Automated controls are in place for some policies. Exceptions require formal approval.
4 - Managed	Automated controls enforce the majority of governance policies. Manual compliance checking is reserved for complex situations. Enforcement coverage is measured.	Automated controls enforce the majority of governance policies. Manual compliance checking is reserved for complex situations. Enforcement coverage is measured.	Automated controls enforce the majority of governance policies. Manual compliance checking is reserved for complex situations. Enforcement coverage is measured.
5 - Optimised	Policy enforcement is predominantly automated. Non-compliant data or AI processes cannot reach production. Enforcement audit trails are maintained.	Policy enforcement is predominantly automated. Non-compliant data or AI processes cannot reach production. Enforcement audit trails are maintained.	Policy enforcement is predominantly automated. Non-compliant data or AI processes cannot reach production. Enforcement audit trails are maintained.

D6.9 - Third-Party Data Governance

Measure ID	Measure Name	Governs	Normative References
D6.9	Third-Party Data Governance	Whether governance standards are applied to data received from third parties including suppliers, partners, and public data sources.	ISO 8000-8 GDPR Art.28 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Third-party data enters systems without governance standards applied.	Third-party data enters systems without governance standards applied.	Third-party data enters systems without governance standards applied.
1 - Ad Hoc	Third-party data quality is assessed informally when issues arise.	Third-party data quality is assessed informally when issues arise.	Third-party data quality is assessed informally when issues arise.
2 - Repeatable	Governance standards are applied to major third-party data sources. Not universally applied.	Governance standards are applied to major third-party data sources. Not universally applied.	Governance standards are applied to major third-party data sources. Not universally applied.
3 - Defined	Governance standards are contractually required for all critical third-party data sources. Data received from third parties is subject to quality gate validation.	Governance standards are contractually required for all critical third-party data sources. Data received from third parties is subject to quality gate validation.	Governance standards are contractually required for all critical third-party data sources. Data received from third parties is subject to quality gate validation.
4 - Managed	Third-party data governance is audited. Supplier data quality performance is tracked. Poor performance triggers contractual remediation.	Third-party data governance is audited. Supplier data quality performance is tracked. Poor performance triggers contractual remediation.	Third-party data governance is audited. Supplier data quality performance is tracked. Poor performance triggers contractual remediation.
5 - Optimised	Third-party data governance is embedded in supplier contracts and procurement standards. AI training data from third parties is subject to enhanced governance including provenance verification.	Third-party data governance is embedded in supplier contracts and procurement standards. AI training data from third parties is subject to enhanced governance including provenance verification.	Third-party data governance is embedded in supplier contracts and procurement standards. AI training data from third parties is subject to enhanced governance including provenance verification.

D6.10 - Governance Audit Trail

Measure ID	Measure Name	Governs	Normative References
D6.10	Governance Audit Trail	Whether an auditable record of governance decisions, policy exceptions, and compliance actions is maintained.	ISO 8000-8 ISO 42001 Clause 7.5 EU AI Act Art.12 GDPR Art.5(2)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No governance audit trail. Decisions and exceptions are unrecorded.	No governance audit trail. Decisions and exceptions are unrecorded.	No governance audit trail. Decisions and exceptions are unrecorded.
1 - Ad Hoc	Decisions are recorded in meeting minutes informally. Not structured.	Decisions are recorded in meeting minutes informally. Not structured.	Decisions are recorded in meeting minutes informally. Not structured.
2 - Repeatable	Key governance decisions are recorded. Policy exceptions are partially documented.	Key governance decisions are recorded. Policy exceptions are partially documented.	Key governance decisions are recorded. Policy exceptions are partially documented.
3 - Defined	A formal governance audit trail records all governance decisions, policy exceptions, and compliance actions. Records are tamper-evident and retained for defined periods.	A formal governance audit trail records all governance decisions, policy exceptions, and compliance actions. Records are tamper-evident and retained for defined periods.	A formal governance audit trail records all governance decisions, policy exceptions, and compliance actions. Records are tamper-evident and retained for defined periods.
4 - Managed	The audit trail is actively reviewed. Patterns of exceptions trigger policy review. Retention periods are aligned to regulatory requirements.	The audit trail is actively reviewed. Patterns of exceptions trigger policy review. Retention periods are aligned to regulatory requirements.	The audit trail is actively reviewed. Patterns of exceptions trigger policy review. Retention periods are aligned to regulatory requirements.
5 - Optimised	The governance audit trail is automated and comprehensive. It covers data governance and AI governance decisions. The audit trail supports regulatory examination and internal assurance.	The governance audit trail is automated and comprehensive. It covers data governance and AI governance decisions. The audit trail supports regulatory examination and internal assurance.	The governance audit trail is automated and comprehensive. It covers data governance and AI governance decisions. The audit trail supports regulatory examination and internal assurance.

8. Domain D7: Security & Privacy

Domain	Security & Privacy
Domain ID	D7
Weighting	8.33%
Measures	10
Purpose	Data governance and security are complementary disciplines. Ungoverned data is often insecure data: without classification, access controls become arbitrary; without lineage, breaches cannot be scoped; without retention policies, data accumulates beyond its protective justification. This domain governs the security and privacy controls applied to data assets, with specific attention to the AI-specific security considerations that most organisations have not yet addressed. Strong performance in this domain means the organisation can demonstrate that personal and sensitive data is protected, that access is controlled and audited, and that AI systems are not exposed to adversarial threats.
Regulatory Context	GDPR Articles 5, 25, 32, 33, 34 (security, privacy by design, breach notification). UK GDPR equivalents. EU AI Act Article 15 (accuracy, robustness, cybersecurity for high-risk AI). ISO 27001 (information security management).

D7.1 - Data Encryption

Measure ID	Measure Name	Governs	Normative References
D7.1	Data Encryption	Whether all critical data assets are encrypted at rest and in transit using current cryptographic standards.	GDPR Art.32 EU AI Act Art.15 ISO 27001
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Encryption is not applied or applied only to a small subset of data.	Encryption is not applied or applied only to a small subset of data.	Encryption is not applied or applied only to a small subset of data.
1 - Ad Hoc	Encryption is applied to some critical systems. Approach is inconsistent.	Encryption is applied to some critical systems. Approach is inconsistent.	Encryption is applied to some critical systems. Approach is inconsistent.
2 - Repeatable	Encryption is applied to major systems using a defined standard. Some assets are not covered.	Encryption is applied to major systems using a defined standard. Some assets are not covered.	Encryption is applied to major systems using a defined standard. Some assets are not covered.
3 - Defined	Encryption is applied to all critical data assets at rest and in transit. Standards are defined and reviewed. Coverage is audited.	Encryption is applied to all critical data assets at rest and in transit. Standards are defined and reviewed. Coverage is audited.	Encryption is applied to all critical data assets at rest and in transit. Standards are defined and reviewed. Coverage is audited.
4 - Managed	Encryption coverage is continuously monitored. Weak or deprecated algorithms are identified and replaced. AI model artefacts and training data are encrypted.	Encryption coverage is continuously monitored. Weak or deprecated algorithms are identified and replaced. AI model artefacts and training data are encrypted.	Encryption coverage is continuously monitored. Weak or deprecated algorithms are identified and replaced. AI model artefacts and training data are encrypted.
5 - Optimised	Encryption is comprehensive and automated. Key management follows best practice. Encryption standards are reviewed on a defined cycle and updated proactively.	Encryption is comprehensive and automated. Key management follows best practice. Encryption standards are reviewed on a defined cycle and updated proactively.	Encryption is comprehensive and automated. Key management follows best practice. Encryption standards are reviewed on a defined cycle and updated proactively.

D7.2 - Access Controls

Measure ID	Measure Name	Governs	Normative References
D7.2	Access Controls	Whether role-based, least-privilege access controls are enforced and regularly reviewed for all critical data assets.	GDPR Art.25,32 EU AI Act Art.15 ISO 27001
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Access controls are absent or minimal.	Access controls are absent or minimal.	Access controls are absent or minimal.
1 - Ad Hoc	Access controls exist in some systems. Not consistently applied on a least-privilege basis.	Access controls exist in some systems. Not consistently applied on a least-privilege basis.	Access controls exist in some systems. Not consistently applied on a least-privilege basis.
2 - Repeatable	RBAC is applied to major systems. Access reviews are infrequent.	RBAC is applied to major systems. Access reviews are infrequent.	RBAC is applied to major systems. Access reviews are infrequent.
3 - Defined	RBAC with least-privilege is enforced across all critical data assets. Access reviews are conducted on a defined cycle.	RBAC with least-privilege is enforced across all critical data assets. Access reviews are conducted on a defined cycle.	RBAC with least-privilege is enforced across all critical data assets. Access reviews are conducted on a defined cycle.
4 - Managed	Access review frequency is risk-based. Privileged access is subject to enhanced controls. AI training data and model artefacts have defined access policies.	Access review frequency is risk-based. Privileged access is subject to enhanced controls. AI training data and model artefacts have defined access policies.	Access review frequency is risk-based. Privileged access is subject to enhanced controls. AI training data and model artefacts have defined access policies.
5 - Optimised	Access controls are fully automated. Provisioning and de-provisioning is governed. Access to AI systems is subject to a formal approval process.	Access controls are fully automated. Provisioning and de-provisioning is governed. Access to AI systems is subject to a formal approval process.	Access controls are fully automated. Provisioning and de-provisioning is governed. Access to AI systems is subject to a formal approval process.

D7.3 - Audit Logging

Measure ID	Measure Name	Governs	Normative References
D7.3	Audit Logging	Whether access and change logging is comprehensive, tamper-evident, and actively reviewed.	GDPR Art.32 EU AI Act Art.12 ISO 27001
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Audit logging is absent.	Audit logging is absent.	Audit logging is absent.
1 - Ad Hoc	Logging exists in some systems. Logs are not reviewed.	Logging exists in some systems. Logs are not reviewed.	Logging exists in some systems. Logs are not reviewed.
2 - Repeatable	Comprehensive logging is in place for major systems. Review is periodic.	Comprehensive logging is in place for major systems. Review is periodic.	Comprehensive logging is in place for major systems. Review is periodic.
3 - Defined	Audit logging covers all critical data assets. Logs are tamper-evident. Logs are actively reviewed on a defined schedule.	Audit logging covers all critical data assets. Logs are tamper-evident. Logs are actively reviewed on a defined schedule.	Audit logging covers all critical data assets. Logs are tamper-evident. Logs are actively reviewed on a defined schedule.
4 - Managed	Log review is automated where possible. Anomalous access patterns trigger alerts. Log retention is aligned to regulatory requirements.	Log review is automated where possible. Anomalous access patterns trigger alerts. Log retention is aligned to regulatory requirements.	Log review is automated where possible. Anomalous access patterns trigger alerts. Log retention is aligned to regulatory requirements.
5 - Optimised	Comprehensive audit logging is in place across all data and AI systems. AI system logs include inference inputs, outputs, and decision trails. Logs are integrated with a SIEM.	Comprehensive audit logging is in place across all data and AI systems. AI system logs include inference inputs, outputs, and decision trails. Logs are integrated with a SIEM.	Comprehensive audit logging is in place across all data and AI systems. AI system logs include inference inputs, outputs, and decision trails. Logs are integrated with a SIEM.

D7.4 - Regulatory Adherence

Measure ID	Measure Name	Governs	Normative References
D7.4	Regulatory Adherence	Whether the organisation demonstrably meets applicable data protection regulatory requirements including GDPR and sector-specific obligations.	GDPR Art.5,24 EU AI Act Art.15,17
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Regulatory requirements are not addressed.	Regulatory requirements are not addressed.	Regulatory requirements are not addressed.
1 - Ad Hoc	Regulatory requirements are partially known. Compliance is assumed rather than demonstrated.	Regulatory requirements are partially known. Compliance is assumed rather than demonstrated.	Regulatory requirements are partially known. Compliance is assumed rather than demonstrated.
2 - Repeatable	Key regulatory requirements are addressed. Compliance evidence is limited.	Key regulatory requirements are addressed. Compliance evidence is limited.	Key regulatory requirements are addressed. Compliance evidence is limited.
3 - Defined	Regulatory compliance is demonstrated through documented controls, audit evidence, and regular assessment. Compliance status is reported.	Regulatory compliance is demonstrated through documented controls, audit evidence, and regular assessment. Compliance status is reported.	Regulatory compliance is demonstrated through documented controls, audit evidence, and regular assessment. Compliance status is reported.
4 - Managed	Regulatory compliance is continuously monitored. Regulatory changes trigger impact assessment. External audit findings are addressed.	Regulatory compliance is continuously monitored. Regulatory changes trigger impact assessment. External audit findings are addressed.	Regulatory compliance is continuously monitored. Regulatory changes trigger impact assessment. External audit findings are addressed.
5 - Optimised	Regulatory adherence is embedded in governance. Evidence is continuously collected. External certification provides independent assurance.	Regulatory adherence is embedded in governance. Evidence is continuously collected. External certification provides independent assurance.	Regulatory adherence is embedded in governance. Evidence is continuously collected. External certification provides independent assurance.

D7.5 - Breach Response

Measure ID	Measure Name	Governs	Normative References
D7.5	Breach Response	Whether a documented, tested incident response plan for data breaches is in place.	GDPR Art.33,34 ISO 27001
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No breach response plan.	No breach response plan.	No breach response plan.
1 - Ad Hoc	Breach response is discussed but not documented.	Breach response is discussed but not documented.	Breach response is discussed but not documented.
2 - Repeatable	A breach response plan exists. It has not been tested.	A breach response plan exists. It has not been tested.	A breach response plan exists. It has not been tested.
3 - Defined	A documented breach response plan exists, is tested at least annually, and covers regulatory notification requirements.	A documented breach response plan exists, is tested at least annually, and covers regulatory notification requirements.	A documented breach response plan exists, is tested at least annually, and covers regulatory notification requirements.
4 - Managed	Breach response exercises are conducted. Lessons learned are incorporated. Response times are measured against regulatory timescales.	Breach response exercises are conducted. Lessons learned are incorporated. Response times are measured against regulatory timescales.	Breach response exercises are conducted. Lessons learned are incorporated. Response times are measured against regulatory timescales.
5 - Optimised	Breach response is rehearsed regularly at all levels including executive. AI-specific breach scenarios are included. Response capability is independently assessed.	Breach response is rehearsed regularly at all levels including executive. AI-specific breach scenarios are included. Response capability is independently assessed.	Breach response is rehearsed regularly at all levels including executive. AI-specific breach scenarios are included. Response capability is independently assessed.

D7.6 - Security Training

Measure ID	Measure Name	Governs	Normative References
D7.6	Security Training	Whether all staff handling data receive regular security and data protection training.	GDPR Art.32 ISO 27001
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No security training.	No security training.	No security training.
1 - Ad Hoc	Ad hoc security awareness. No structured programme.	Ad hoc security awareness. No structured programme.	Ad hoc security awareness. No structured programme.
2 - Repeatable	Annual security training is available. Completion is not mandatory.	Annual security training is available. Completion is not mandatory.	Annual security training is available. Completion is not mandatory.
3 - Defined	Security training is mandatory for all staff handling data. Completion is tracked. Training covers data protection and AI-relevant risks.	Security training is mandatory for all staff handling data. Completion is tracked. Training covers data protection and AI-relevant risks.	Security training is mandatory for all staff handling data. Completion is tracked. Training covers data protection and AI-relevant risks.
4 - Managed	Training is role-differentiated. Completion rates are near 100%. Training content is updated when threats or regulations change.	Training is role-differentiated. Completion rates are near 100%. Training content is updated when threats or regulations change.	Training is role-differentiated. Completion rates are near 100%. Training content is updated when threats or regulations change.
5 - Optimised	Training is continuous and embedded in onboarding. AI-specific security training is provided to all staff involved in AI development or deployment.	Training is continuous and embedded in onboarding. AI-specific security training is provided to all staff involved in AI development or deployment.	Training is continuous and embedded in onboarding. AI-specific security training is provided to all staff involved in AI development or deployment.

D7.7 - Data Classification

Measure ID	Measure Name	Governs	Normative References
D7.7	Data Classification	Whether data assets are classified by sensitivity with proportionate security controls applied to each classification tier.	GDPR Art.25,32 ISO 27001
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No data classification. All data is treated the same.	No data classification. All data is treated the same.	No data classification. All data is treated the same.
1 - Ad Hoc	Classification is informally understood. Not applied consistently.	Classification is informally understood. Not applied consistently.	Classification is informally understood. Not applied consistently.
2 - Repeatable	Classification is applied to personal data and some sensitive assets. Not universally applied.	Classification is applied to personal data and some sensitive assets. Not universally applied.	Classification is applied to personal data and some sensitive assets. Not universally applied.
3 - Defined	A formal classification scheme is in place. All critical data assets are classified. Controls are proportionate to classification.	A formal classification scheme is in place. All critical data assets are classified. Controls are proportionate to classification.	A formal classification scheme is in place. All critical data assets are classified. Controls are proportionate to classification.
4 - Managed	Classification coverage is measured and gaps are tracked. AI training data and model artefacts are classified. Classification is reviewed when data use changes.	Classification coverage is measured and gaps are tracked. AI training data and model artefacts are classified. Classification is reviewed when data use changes.	Classification coverage is measured and gaps are tracked. AI training data and model artefacts are classified. Classification is reviewed when data use changes.
5 - Optimised	Classification is automated where possible. Data cannot be ingested into production systems without classification. AI system data classification is part of the EU AI Act risk assessment.	Classification is automated where possible. Data cannot be ingested into production systems without classification. AI system data classification is part of the EU AI Act risk assessment.	Classification is automated where possible. Data cannot be ingested into production systems without classification. AI system data classification is part of the EU AI Act risk assessment.

D7.8 - Privacy by Design

Measure ID	Measure Name	Governs	Normative References
D7.8	Privacy by Design	Whether privacy impact assessments are conducted for new data and AI initiatives and whether privacy controls are embedded at design stage.	GDPR Art.25,35 EU AI Act Art.9 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Privacy is not considered at design stage.	Privacy is not considered at design stage.	Privacy is not considered at design stage.
1 - Ad Hoc	Privacy is considered informally when issues are raised.	Privacy is considered informally when issues are raised.	Privacy is considered informally when issues are raised.
2 - Repeatable	PIAs are conducted for some initiatives involving personal data. Not for AI initiatives.	PIAs are conducted for some initiatives involving personal data. Not for AI initiatives.	PIAs are conducted for some initiatives involving personal data. Not for AI initiatives.
3 - Defined	PIAs are mandatory for all new data and AI initiatives involving personal data. Conducted at design stage. Results are documented and reviewed.	PIAs are mandatory for all new data and AI initiatives involving personal data. Conducted at design stage. Results are documented and reviewed.	PIAs are mandatory for all new data and AI initiatives involving personal data. Conducted at design stage. Results are documented and reviewed.
4 - Managed	PIA results drive design decisions. Privacy controls are embedded in technical architecture. AI initiatives have enhanced PIA requirements.	PIA results drive design decisions. Privacy controls are embedded in technical architecture. AI initiatives have enhanced PIA requirements.	PIA results drive design decisions. Privacy controls are embedded in technical architecture. AI initiatives have enhanced PIA requirements.
5 - Optimised	Privacy by design is fully embedded. PIAs are integrated into the project governance framework. AI-specific privacy assessment covers automated decision-making risks.	Privacy by design is fully embedded. PIAs are integrated into the project governance framework. AI-specific privacy assessment covers automated decision-making risks.	Privacy by design is fully embedded. PIAs are integrated into the project governance framework. AI-specific privacy assessment covers automated decision-making risks.

D7.9 - AI-Specific Security

Measure ID	Measure Name	Governs	Normative References
D7.9	AI-Specific Security	Whether AI model inputs and outputs are protected against adversarial attacks, prompt injection, data poisoning, and model inversion.	EU AI Act Art.15 ISO 42001 Clause 8.5 NIST AI RMF
MATURITY LEVEL DESCR IPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No AI-specific security controls. Standard application security only.	No AI-specific security controls. Standard application security only.	No AI-specific security controls. Standard application security only.
1 - Ad Hoc	AI security risks are known. No specific controls implemented.	AI security risks are known. No specific controls implemented.	AI security risks are known. No specific controls implemented.
2 - Repeatable	Some AI security controls are in place for high-risk models. Not systematic.	Some AI security controls are in place for high-risk models. Not systematic.	Some AI security controls are in place for high-risk models. Not systematic.
3 - Defined	AI-specific security controls are defined and implemented for all production AI systems. Controls cover input validation, output monitoring, and model access.	AI-specific security controls are defined and implemented for all production AI systems. Controls cover input validation, output monitoring, and model access.	AI-specific security controls are defined and implemented for all production AI systems. Controls cover input validation, output monitoring, and model access.
4 - Managed	AI security controls are tested regularly through adversarial testing. Control coverage is measured. Threats are monitored through AI security intelligence.	AI security controls are tested regularly through adversarial testing. Control coverage is measured. Threats are monitored through AI security intelligence.	AI security controls are tested regularly through adversarial testing. Control coverage is measured. Threats are monitored through AI security intelligence.
5 - Optimised	AI security is embedded in the AI development lifecycle. Threat modelling is conducted for all AI systems. AI security controls are independently assessed.	AI security is embedded in the AI development lifecycle. Threat modelling is conducted for all AI systems. AI security controls are independently assessed.	AI security is embedded in the AI development lifecycle. Threat modelling is conducted for all AI systems. AI security controls are independently assessed.

D7.10 - Third-Party Security

Measure ID	Measure Name	Governs	Normative References
D7.10	Third-Party Security	Whether data security standards are contractually required for third-party data processors and AI vendors.	GDPR Art.28 EU AI Act Art.25,28 ISO 27001
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No security requirements in third-party contracts.	No security requirements in third-party contracts.	No security requirements in third-party contracts.
1 - Ad Hoc	Security requirements are discussed informally with key suppliers.	Security requirements are discussed informally with key suppliers.	Security requirements are discussed informally with key suppliers.
2 - Repeatable	Standard security clauses are in major contracts. Not universally applied.	Standard security clauses are in major contracts. Not universally applied.	Standard security clauses are in major contracts. Not universally applied.
3 - Defined	Minimum security standards are contractually required for all third-party data processors and AI vendors. Audit rights are included.	Minimum security standards are contractually required for all third-party data processors and AI vendors. Audit rights are included.	Minimum security standards are contractually required for all third-party data processors and AI vendors. Audit rights are included.
4 - Managed	Third-party security is assessed at onboarding and periodically thereafter. Poor performance triggers contractual remediation.	Third-party security is assessed at onboarding and periodically thereafter. Poor performance triggers contractual remediation.	Third-party security is assessed at onboarding and periodically thereafter. Poor performance triggers contractual remediation.
5 - Optimised	Third-party security governance is embedded in procurement. AI vendor security is subject to enhanced assessment. Audit rights are exercised.	Third-party security governance is embedded in procurement. AI vendor security is subject to enhanced assessment. Audit rights are exercised.	Third-party security governance is embedded in procurement. AI vendor security is subject to enhanced assessment. Audit rights are exercised.

9. Domain D8: Tooling & Technology

Domain	Tooling & Technology
Domain ID	D8
Weighting	8.33%
Measures	8
Purpose	Data governance is only as effective as the tools that support it. Manual processes degrade, inconsistency grows, and coverage fails without automation. This domain governs whether the organisation's technology choices for data management, quality monitoring, cataloguing, and AI operations are fit for purpose, well-integrated, and sufficiently automated to make governance scalable. It also addresses the critical question of AI toolchain readiness: the feature stores, model registries, and pipeline management tools that make AI governance operational rather than theoretical.
Regulatory Context	ISO 8000-61 (operational data quality management). ISO 42001 Clause 8 (AI system lifecycle tools). No direct EU AI Act tooling obligation but Article 9 (risk management systems) and Article 17 (quality management) assume tooling capability.

D8.1 - Tool Integration

Measure ID	Measure Name	Governs	Normative References
D8.1	Tool Integration	How well data catalog, quality monitoring, pipeline orchestration, and observability tools are integrated with each other.	ISO 8000-61 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No integration. Tools operate in silos.	No integration. Tools operate in silos.	No integration. Tools operate in silos.
1 - Ad Hoc	Integration is manually coordinated. Data is copied between tools.	Integration is manually coordinated. Data is copied between tools.	Integration is manually coordinated. Data is copied between tools.
2 - Repeatable	Key tools are partially integrated via file-based or scheduled interfaces.	Key tools are partially integrated via file-based or scheduled interfaces.	Key tools are partially integrated via file-based or scheduled interfaces.
3 - Defined	Core tools are integrated via APIs. Key data flows between tools automatically.	Core tools are integrated via APIs. Key data flows between tools automatically.	Core tools are integrated via APIs. Key data flows between tools automatically.
4 - Managed	Integration is comprehensive and monitored. Failures in integration are detected and alerted. Tool integration coverage is measured.	Integration is comprehensive and monitored. Failures in integration are detected and alerted. Tool integration coverage is measured.	Integration is comprehensive and monitored. Failures in integration are detected and alerted. Tool integration coverage is measured.
5 - Optimised	Tools form a coherent data governance platform. AI toolchain is integrated with the data platform. Integration is continuously monitored.	Tools form a coherent data governance platform. AI toolchain is integrated with the data platform. Integration is continuously monitored.	Tools form a coherent data governance platform. AI toolchain is integrated with the data platform. Integration is continuously monitored.

D8.2 - Automation Level

Measure ID	Measure Name	Governs	Normative References
D8.2	Automation Level	The extent to which data quality checks, remediation workflows, and governance processes are automated rather than manual.	ISO 8000-61 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	All quality processes are manual.	All quality processes are manual.	All quality processes are manual.
1 - Ad Hoc	Some automated checks exist in specific tools. Not systematic.	Some automated checks exist in specific tools. Not systematic.	Some automated checks exist in specific tools. Not systematic.
2 - Repeatable	Automation is in place for major quality checks. Manual processes dominate.	Automation is in place for major quality checks. Manual processes dominate.	Automation is in place for major quality checks. Manual processes dominate.
3 - Defined	The majority of data quality checks and governance workflows are automated. Manual intervention is reserved for complex situations.	The majority of data quality checks and governance workflows are automated. Manual intervention is reserved for complex situations.	The majority of data quality checks and governance workflows are automated. Manual intervention is reserved for complex situations.
4 - Managed	Automation coverage is measured. Gaps are identified and addressed. Automated remediation is in place for defined issue types.	Automation coverage is measured. Gaps are identified and addressed. Automated remediation is in place for defined issue types.	Automation coverage is measured. Gaps are identified and addressed. Automated remediation is in place for defined issue types.
5 - Optimised	Governance automation is comprehensive. Manual processes are the exception. AI quality monitoring is fully automated.	Governance automation is comprehensive. Manual processes are the exception. AI quality monitoring is fully automated.	Governance automation is comprehensive. Manual processes are the exception. AI quality monitoring is fully automated.

D8.3 - Platform Fit

Measure ID	Measure Name	Governs	Normative References
D8.3	Platform Fit	How well the current tooling aligns to the organisation's data platform strategy and AI strategy.	ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No platform strategy. Tool choices are ad hoc.	No platform strategy. Tool choices are ad hoc.	No platform strategy. Tool choices are ad hoc.
1 - Ad Hoc	Platform strategy exists informally. Tool choices are not consistently aligned.	Platform strategy exists informally. Tool choices are not consistently aligned.	Platform strategy exists informally. Tool choices are not consistently aligned.
2 - Repeatable	A platform strategy exists. New tool choices consider alignment. Legacy tools are not yet addressed.	A platform strategy exists. New tool choices consider alignment. Legacy tools are not yet addressed.	A platform strategy exists. New tool choices consider alignment. Legacy tools are not yet addressed.
3 - Defined	A formal platform strategy drives tool selection. Current tooling is assessed against the strategy. A remediation plan exists for gaps.	A formal platform strategy drives tool selection. Current tooling is assessed against the strategy. A remediation plan exists for gaps.	A formal platform strategy drives tool selection. Current tooling is assessed against the strategy. A remediation plan exists for gaps.
4 - Managed	Platform fit is actively maintained. Tool assessments are conducted on a defined cycle. AI toolchain alignment to strategy is specifically assessed.	Platform fit is actively maintained. Tool assessments are conducted on a defined cycle. AI toolchain alignment to strategy is specifically assessed.	Platform fit is actively maintained. Tool assessments are conducted on a defined cycle. AI toolchain alignment to strategy is specifically assessed.
5 - Optimised	Platform strategy is a living governance document. Tool choices are governed. AI toolchain is a strategic investment with a defined roadmap.	Platform strategy is a living governance document. Tool choices are governed. AI toolchain is a strategic investment with a defined roadmap.	Platform strategy is a living governance document. Tool choices are governed. AI toolchain is a strategic investment with a defined roadmap.

D8.4 - User Accessibility

Measure ID	Measure Name	Governs	Normative References
D8.4	User Accessibility	Whether tools are accessible and usable for both technical and business user personas without requiring specialist IT support.	DAMA DMBOK Ch.12 ISO 42001 Clause 7.2
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Tools are accessible to IT only. Business users have no direct access.	Tools are accessible to IT only. Business users have no direct access.	Tools are accessible to IT only. Business users have no direct access.
1 - Ad Hoc	Some tools have basic business user interfaces. Significant IT dependency remains.	Some tools have basic business user interfaces. Significant IT dependency remains.	Some tools have basic business user interfaces. Significant IT dependency remains.
2 - Repeatable	Major tools have business-friendly interfaces. Self-service is limited.	Major tools have business-friendly interfaces. Self-service is limited.	Major tools have business-friendly interfaces. Self-service is limited.
3 - Defined	Tools are accessible to both technical and business users. Training is provided. Self-service capability exists for core use cases.	Tools are accessible to both technical and business users. Training is provided. Self-service capability exists for core use cases.	Tools are accessible to both technical and business users. Training is provided. Self-service capability exists for core use cases.
4 - Managed	Business user adoption is measured. Tool usability is regularly assessed. Feedback drives product improvement.	Business user adoption is measured. Tool usability is regularly assessed. Feedback drives product improvement.	Business user adoption is measured. Tool usability is regularly assessed. Feedback drives product improvement.
5 - Optimised	Tools support genuine self-service governance. Business users can discover data, assess quality, and request access without IT intermediation.	Tools support genuine self-service governance. Business users can discover data, assess quality, and request access without IT intermediation.	Tools support genuine self-service governance. Business users can discover data, assess quality, and request access without IT intermediation.

D8.5 - API Extensibility

Measure ID	Measure Name	Governs	Normative References
D8.5	API Extensibility	Whether tools expose APIs and SDKs that enable integration, customisation, and extension.	ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Tools do not expose APIs. Integration requires bespoke development.	Tools do not expose APIs. Integration requires bespoke development.	Tools do not expose APIs. Integration requires bespoke development.
1 - Ad Hoc	Some tools expose basic APIs. Not consistently used.	Some tools expose basic APIs. Not consistently used.	Some tools expose basic APIs. Not consistently used.
2 - Repeatable	Core tools expose APIs. Integration is in place for some use cases.	Core tools expose APIs. Integration is in place for some use cases.	Core tools expose APIs. Integration is in place for some use cases.
3 - Defined	All core tools expose APIs. APIs are used for tool integration and automation. API documentation is maintained.	All core tools expose APIs. APIs are used for tool integration and automation. API documentation is maintained.	All core tools expose APIs. APIs are used for tool integration and automation. API documentation is maintained.
4 - Managed	APIs are used for all tool integration. API usage is monitored. Deprecation of API versions is managed.	APIs are used for all tool integration. API usage is monitored. Deprecation of API versions is managed.	APIs are used for all tool integration. API usage is monitored. Deprecation of API versions is managed.
5 - Optimised	API-first design governs tool selection. All governance processes are API-accessible. AI toolchain APIs enable end-to-end automation.	API-first design governs tool selection. All governance processes are API-accessible. AI toolchain APIs enable end-to-end automation.	API-first design governs tool selection. All governance processes are API-accessible. AI toolchain APIs enable end-to-end automation.

D8.6 - Cloud-Native Alignment

Measure ID	Measure Name	Governs	Normative References
D8.6	Cloud-Native Alignment	Whether tooling is cloud-native or well-architected for the chosen cloud environment, enabling scalability and operational efficiency.	ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	All tooling is on-premise with no cloud strategy.	All tooling is on-premise with no cloud strategy.	All tooling is on-premise with no cloud strategy.
1 - Ad Hoc	Cloud adoption is nascent. Some tools are cloud-hosted but not cloud-native.	Cloud adoption is nascent. Some tools are cloud-hosted but not cloud-native.	Cloud adoption is nascent. Some tools are cloud-hosted but not cloud-native.
2 - Repeatable	Core tools are cloud-hosted. Cloud-native architecture is emerging.	Core tools are cloud-hosted. Cloud-native architecture is emerging.	Core tools are cloud-hosted. Cloud-native architecture is emerging.
3 - Defined	Majority of tooling is cloud-native or well-architected for cloud. A cloud governance framework exists.	Majority of tooling is cloud-native or well-architected for cloud. A cloud governance framework exists.	Majority of tooling is cloud-native or well-architected for cloud. A cloud governance framework exists.
4 - Managed	Cloud-native adoption is actively managed. Total cost and performance are monitored. AI tools are cloud-native.	Cloud-native adoption is actively managed. Total cost and performance are monitored. AI tools are cloud-native.	Cloud-native adoption is actively managed. Total cost and performance are monitored. AI tools are cloud-native.
5 - Optimised	Tooling is fully cloud-native. Cloud governance is automated. AI model serving and training infrastructure is cloud-native and governed.	Tooling is fully cloud-native. Cloud governance is automated. AI model serving and training infrastructure is cloud-native and governed.	Tooling is fully cloud-native. Cloud governance is automated. AI model serving and training infrastructure is cloud-native and governed.

D8.7 - AI Toolchain Readiness

Measure ID	Measure Name	Governs	Normative References
D8.7	AI Toolchain Readiness	Whether the toolchain includes AI/ML pipeline management, feature stores, model registries, and experiment tracking.	ISO 42001 Clause 8 EU AI Act Art.9,12
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No AI-specific tooling. AI initiatives use ad hoc approaches.	No AI-specific tooling. AI initiatives use ad hoc approaches.	No AI-specific tooling. AI initiatives use ad hoc approaches.
1 - Ad Hoc	Basic AI tooling exists. No feature store, model registry, or experiment tracking.	Basic AI tooling exists. No feature store, model registry, or experiment tracking.	Basic AI tooling exists. No feature store, model registry, or experiment tracking.
2 - Repeatable	Some AI tooling is in place. Feature store or model registry may exist. Not integrated.	Some AI tooling is in place. Feature store or model registry may exist. Not integrated.	Some AI tooling is in place. Feature store or model registry may exist. Not integrated.
3 - Defined	AI toolchain includes pipeline management, feature store, and model registry. Tools are integrated. Governance coverage is partial.	AI toolchain includes pipeline management, feature store, and model registry. Tools are integrated. Governance coverage is partial.	AI toolchain includes pipeline management, feature store, and model registry. Tools are integrated. Governance coverage is partial.
4 - Managed	AI toolchain is comprehensive and well-integrated. Experiment tracking and model lineage are in place. AI governance policies are enforced through tooling.	AI toolchain is comprehensive and well-integrated. Experiment tracking and model lineage are in place. AI governance policies are enforced through tooling.	AI toolchain is comprehensive and well-integrated. Experiment tracking and model lineage are in place. AI governance policies are enforced through tooling.
5 - Optimised	AI toolchain is a governed platform. All AI development and deployment uses the toolchain. Toolchain enforces governance standards automatically.	AI toolchain is a governed platform. All AI development and deployment uses the toolchain. Toolchain enforces governance standards automatically.	AI toolchain is a governed platform. All AI development and deployment uses the toolchain. Toolchain enforces governance standards automatically.

D8.8 - Tooling Debt

Measure ID	Measure Name	Governs	Normative References
D8.8	Tooling Debt	Whether there is a managed process to identify, prioritise, and retire legacy or redundant tooling.	ISO 8000-61
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Tooling debt is unmanaged. Legacy tools accumulate.	Tooling debt is unmanaged. Legacy tools accumulate.	Tooling debt is unmanaged. Legacy tools accumulate.
1 - Ad Hoc	Tooling debt is recognised but not formally tracked.	Tooling debt is recognised but not formally tracked.	Tooling debt is recognised but not formally tracked.
2 - Repeatable	Major legacy tools are identified. A retirement plan exists in principle.	Major legacy tools are identified. A retirement plan exists in principle.	Major legacy tools are identified. A retirement plan exists in principle.
3 - Defined	Tooling debt is formally tracked. A prioritised retirement roadmap exists. Retirement follows a defined process.	Tooling debt is formally tracked. A prioritised retirement roadmap exists. Retirement follows a defined process.	Tooling debt is formally tracked. A prioritised retirement roadmap exists. Retirement follows a defined process.
4 - Managed	Tooling debt is managed on a rolling basis. Retirement progress is reported. New tool adoption requires retirement of displaced tools.	Tooling debt is managed on a rolling basis. Retirement progress is reported. New tool adoption requires retirement of displaced tools.	Tooling debt is managed on a rolling basis. Retirement progress is reported. New tool adoption requires retirement of displaced tools.
5 - Optimised	Tooling governance is comprehensive. Technical debt is continuously identified and managed. AI tooling debt is separately tracked given its governance implications.	Tooling governance is comprehensive. Technical debt is continuously identified and managed. AI tooling debt is separately tracked given its governance implications.	Tooling governance is comprehensive. Technical debt is continuously identified and managed. AI tooling debt is separately tracked given its governance implications.

10. Domain D9: Transparency & Access

Domain	Transparency & Access
Domain ID	D9
Weighting	8.33%
Measures	8
Purpose	Governance that is invisible to its consumers is governance that fails. Data consumers need to find data, understand its quality, know when it changes, and trust that the AI outputs they rely on are based on reliable foundations. This domain governs data discoverability, quality transparency, access governance, and the transparency requirements specific to AI systems. Strong performance means data consumers across the organisation can make better decisions because they understand the provenance and quality of the data behind those decisions.
Regulatory Context	EU AI Act Articles 13, 52 (transparency and provision of information to users). GDPR Article 5(1)(a) (lawfulness, fairness, transparency). ISO 42001 Clause 8 (AI system transparency requirements).

D9.1 - Data Discoverability

Measure ID	Measure Name	Governs	Normative References
D9.1	Data Discoverability	Whether users can find datasets with full context including quality, lineage, and ownership without requiring IT assistance.	ISO 8000-8 DAMA DMBOK Ch.12
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Data discovery requires contacting individual data owners or IT staff.	Data discovery requires contacting individual data owners or IT staff.	Data discovery requires contacting individual data owners or IT staff.
1 - Ad Hoc	A basic inventory of datasets exists. Quality and lineage information is absent.	A basic inventory of datasets exists. Quality and lineage information is absent.	A basic inventory of datasets exists. Quality and lineage information is absent.
2 - Repeatable	A data catalog provides basic discovery. Quality information is limited. IT assistance is frequently required.	A data catalog provides basic discovery. Quality information is limited. IT assistance is frequently required.	A data catalog provides basic discovery. Quality information is limited. IT assistance is frequently required.
3 - Defined	A governed data catalog provides discovery with quality scores, lineage, and ownership for all critical assets. Self-service discovery is possible.	A governed data catalog provides discovery with quality scores, lineage, and ownership for all critical assets. Self-service discovery is possible.	A governed data catalog provides discovery with quality scores, lineage, and ownership for all critical assets. Self-service discovery is possible.
4 - Managed	Data catalog completeness is measured. All new assets are catalogued before production use. Discovery satisfaction is tracked.	Data catalog completeness is measured. All new assets are catalogued before production use. Discovery satisfaction is tracked.	Data catalog completeness is measured. All new assets are catalogued before production use. Discovery satisfaction is tracked.
5 - Optimised	Data discovery is fully self-service. The catalog is the authoritative reference. AI model metadata including training data references is discoverable.	Data discovery is fully self-service. The catalog is the authoritative reference. AI model metadata including training data references is discoverable.	Data discovery is fully self-service. The catalog is the authoritative reference. AI model metadata including training data references is discoverable.

D9.2 - Quality Visibility

Measure ID	Measure Name	Governs	Normative References
D9.2	Quality Visibility	Whether data quality metrics are visible to data consumers at the point of use in dashboards, reports, and data products.	ISO 8000-8 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Quality is not visible to data consumers. Consumers cannot assess data trustworthiness.	Quality is not visible to data consumers. Consumers cannot assess data trustworthiness.	Quality is not visible to data consumers. Consumers cannot assess data trustworthiness.
1 - Ad Hoc	Quality information is available on request from the data team.	Quality information is available on request from the data team.	Quality information is available on request from the data team.
2 - Repeatable	Quality metrics are visible in some dashboards. Not at the point of use in data products.	Quality metrics are visible in some dashboards. Not at the point of use in data products.	Quality metrics are visible in some dashboards. Not at the point of use in data products.
3 - Defined	Quality scores and freshness indicators are visible to consumers in dashboards and data products. Consumer-facing quality is defined and maintained.	Quality scores and freshness indicators are visible to consumers in dashboards and data products. Consumer-facing quality is defined and maintained.	Quality scores and freshness indicators are visible to consumers in dashboards and data products. Consumer-facing quality is defined and maintained.
4 - Managed	Quality visibility covers all critical data products. Consumers can assess data quality before use. Quality trends are visible.	Quality visibility covers all critical data products. Consumers can assess data quality before use. Quality trends are visible.	Quality visibility covers all critical data products. Consumers can assess data quality before use. Quality trends are visible.
5 - Optimised	Quality is embedded in every data product as a standard property. Consumers can see quality history, trends, and alerts. AI output quality indicators are visible to AI users.	Quality is embedded in every data product as a standard property. Consumers can see quality history, trends, and alerts. AI output quality indicators are visible to AI users.	Quality is embedded in every data product as a standard property. Consumers can see quality history, trends, and alerts. AI output quality indicators are visible to AI users.

D9.3 - Access Controls

Measure ID	Measure Name	Governs	Normative References
D9.3	Access Controls	Whether access controls are risk-based, streamlined for legitimate users, and fully auditable.	GDPR Art.25,32 EU AI Act Art.15
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Access controls are absent or applied uniformly without risk differentiation.	Access controls are absent or applied uniformly without risk differentiation.	Access controls are absent or applied uniformly without risk differentiation.
1 - Ad Hoc	Access controls exist but are not risk-based. Access approval is slow.	Access controls exist but are not risk-based. Access approval is slow.	Access controls exist but are not risk-based. Access approval is slow.
2 - Repeatable	Risk-based access controls exist for major systems. Approval processes are partially streamlined.	Risk-based access controls exist for major systems. Approval processes are partially streamlined.	Risk-based access controls exist for major systems. Approval processes are partially streamlined.
3 - Defined	Access controls are risk-based and streamlined for legitimate users. Access requests and approvals are auditable.	Access controls are risk-based and streamlined for legitimate users. Access requests and approvals are auditable.	Access controls are risk-based and streamlined for legitimate users. Access requests and approvals are auditable.
4 - Managed	Access control effectiveness is measured. Denied access patterns are analysed. Access governance is reviewed periodically.	Access control effectiveness is measured. Denied access patterns are analysed. Access governance is reviewed periodically.	Access control effectiveness is measured. Denied access patterns are analysed. Access governance is reviewed periodically.
5 - Optimised	Access governance is automated and risk-based. Just-in-time access is available for sensitive assets. Access patterns are continuously monitored.	Access governance is automated and risk-based. Just-in-time access is available for sensitive assets. Access patterns are continuously monitored.	Access governance is automated and risk-based. Just-in-time access is available for sensitive assets. Access patterns are continuously monitored.

D9.4 - Self-Service Capability

Measure ID	Measure Name	Governs	Normative References
D9.4	Self-Service Capability	Whether analysts and business users can self-serve with governed data including lineage, quality information, and approved templates.	DAMA DMBOK Ch.12 ISO 42001 Clause 7.2
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No self-service. All data access and analysis requires IT involvement.	No self-service. All data access and analysis requires IT involvement.	No self-service. All data access and analysis requires IT involvement.
1 - Ad Hoc	Very limited self-service. Users access pre-approved extracts only.	Very limited self-service. Users access pre-approved extracts only.	Very limited self-service. Users access pre-approved extracts only.
2 - Repeatable	Basic self-service analytics exists for some user groups. Governed data access is limited.	Basic self-service analytics exists for some user groups. Governed data access is limited.	Basic self-service analytics exists for some user groups. Governed data access is limited.
3 - Defined	Governed self-service is available for all authorised users. Data includes lineage and quality information. Templates and governed datasets are provided.	Governed self-service is available for all authorised users. Data includes lineage and quality information. Templates and governed datasets are provided.	Governed self-service is available for all authorised users. Data includes lineage and quality information. Templates and governed datasets are provided.
4 - Managed	Self-service adoption is measured. User feedback drives improvement. Self-service expands as governance matures.	Self-service adoption is measured. User feedback drives improvement. Self-service expands as governance matures.	Self-service adoption is measured. User feedback drives improvement. Self-service expands as governance matures.
5 - Optimised	Self-service is the default mode for data consumption. Governed data products are available on demand. Self-service includes AI model outputs with appropriate transparency information.	Self-service is the default mode for data consumption. Governed data products are available on demand. Self-service includes AI model outputs with appropriate transparency information.	Self-service is the default mode for data consumption. Governed data products are available on demand. Self-service includes AI model outputs with appropriate transparency information.

D9.5 - Change Communication

Measure ID	Measure Name	Governs	Normative References
D9.5	Change Communication	Whether upstream data changes are communicated proactively to downstream consumers with sufficient notice and impact assessment.	ISO 8000-61 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Data changes are not communicated. Consumers discover changes when their systems break.	Data changes are not communicated. Consumers discover changes when their systems break.	Data changes are not communicated. Consumers discover changes when their systems break.
1 - Ad Hoc	Changes are communicated informally to known consumers.	Changes are communicated informally to known consumers.	Changes are communicated informally to known consumers.
2 - Repeatable	Major data changes are communicated in advance. Impact assessment is informal.	Major data changes are communicated in advance. Impact assessment is informal.	Major data changes are communicated in advance. Impact assessment is informal.
3 - Defined	All critical data changes are communicated proactively with impact assessment. Communication follows a defined process with defined timescales.	All critical data changes are communicated proactively with impact assessment. Communication follows a defined process with defined timescales.	All critical data changes are communicated proactively with impact assessment. Communication follows a defined process with defined timescales.
4 - Managed	Change communication includes downstream impact analysis. Consumer acknowledgement is tracked. Emergency changes follow an expedited process.	Change communication includes downstream impact analysis. Consumer acknowledgement is tracked. Emergency changes follow an expedited process.	Change communication includes downstream impact analysis. Consumer acknowledgement is tracked. Emergency changes follow an expedited process.
5 - Optimised	Change communication is automated for all data assets. Data contracts define change notification requirements. AI model re-evaluation is triggered by upstream data changes.	Change communication is automated for all data assets. Data contracts define change notification requirements. AI model re-evaluation is triggered by upstream data changes.	Change communication is automated for all data assets. Data contracts define change notification requirements. AI model re-evaluation is triggered by upstream data changes.

D9.6 - Trust Metrics

Measure ID	Measure Name	Governs	Normative References
D9.6	Trust Metrics	Whether the organisation measures data product trust through adoption rates, consumer satisfaction, and mean time to resolve quality incidents.	ISO 8000-8 DAMA DMBOK Ch.1
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Trust metrics are not defined or measured.	Trust metrics are not defined or measured.	Trust metrics are not defined or measured.
1 - Ad Hoc	Trust is assessed informally through conversations with consumers.	Trust is assessed informally through conversations with consumers.	Trust is assessed informally through conversations with consumers.
2 - Repeatable	Some satisfaction measurement occurs. Not linked to formal trust metrics.	Some satisfaction measurement occurs. Not linked to formal trust metrics.	Some satisfaction measurement occurs. Not linked to formal trust metrics.
3 - Defined	Formal trust metrics are defined and measured for critical data products. Metrics include adoption, satisfaction, and incident resolution time.	Formal trust metrics are defined and measured for critical data products. Metrics include adoption, satisfaction, and incident resolution time.	Formal trust metrics are defined and measured for critical data products. Metrics include adoption, satisfaction, and incident resolution time.
4 - Managed	Trust metrics trend over time. Poor trust scores trigger investigation. Trust metrics are published to data consumers.	Trust metrics trend over time. Poor trust scores trigger investigation. Trust metrics are published to data consumers.	Trust metrics trend over time. Poor trust scores trigger investigation. Trust metrics are published to data consumers.
5 - Optimised	Trust is a primary data product quality metric. Trust scores drive product roadmap decisions. AI output trust is separately measured and published.	Trust is a primary data product quality metric. Trust scores drive product roadmap decisions. AI output trust is separately measured and published.	Trust is a primary data product quality metric. Trust scores drive product roadmap decisions. AI output trust is separately measured and published.

D9.7 - AI Output Transparency

Measure ID	Measure Name	Governs	Normative References
D9.7	AI Output Transparency	Whether AI model outputs are accompanied by sufficient context for consumers to assess their reliability and limitations.	EU AI Act Art.13,52 ISO 42001 Clause 8.5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	AI outputs are presented without any context, confidence information, or limitation disclosure.	AI outputs are presented without any context, confidence information, or limitation disclosure.	AI outputs are presented without any context, confidence information, or limitation disclosure.
1 - Ad Hoc	Confidence scores are available for some AI outputs. Limitations are not documented.	Confidence scores are available for some AI outputs. Limitations are not documented.	Confidence scores are available for some AI outputs. Limitations are not documented.
2 - Repeatable	Confidence information is provided for major AI systems. Limitation documentation is partial.	Confidence information is provided for major AI systems. Limitation documentation is partial.	Confidence information is provided for major AI systems. Limitation documentation is partial.
3 - Defined	All production AI system outputs are accompanied by confidence scores, key limitations, and guidance for appropriate use. Documentation is maintained.	All production AI system outputs are accompanied by confidence scores, key limitations, and guidance for appropriate use. Documentation is maintained.	All production AI system outputs are accompanied by confidence scores, key limitations, and guidance for appropriate use. Documentation is maintained.
4 - Managed	AI transparency documentation is reviewed and updated when models are updated. Consumer understanding of AI limitations is assessed.	AI transparency documentation is reviewed and updated when models are updated. Consumer understanding of AI limitations is assessed.	AI transparency documentation is reviewed and updated when models are updated. Consumer understanding of AI limitations is assessed.
5 - Optimised	AI transparency is embedded in the AI governance framework. All AI outputs meet EU AI Act transparency requirements. Transparency documentation is version-controlled.	AI transparency is embedded in the AI governance framework. All AI outputs meet EU AI Act transparency requirements. Transparency documentation is version-controlled.	AI transparency is embedded in the AI governance framework. All AI outputs meet EU AI Act transparency requirements. Transparency documentation is version-controlled.

D9.8 - Data Contract Adoption

Measure ID	Measure Name	Governs	Normative References
D9.8	Data Contract Adoption	Whether formal data contracts are in place between data producers and consumers, defining quality SLAs, freshness requirements, and change notification obligations.	ISO 8000-61 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No data contracts. Producer and consumer expectations are misaligned.	No data contracts. Producer and consumer expectations are misaligned.	No data contracts. Producer and consumer expectations are misaligned.
1 - Ad Hoc	Informal agreements exist between some producers and consumers.	Informal agreements exist between some producers and consumers.	Informal agreements exist between some producers and consumers.
2 - Repeatable	Data contracts exist for major data products. Not universally applied.	Data contracts exist for major data products. Not universally applied.	Data contracts exist for major data products. Not universally applied.
3 - Defined	Formal data contracts are in place for all critical data products. Contracts define quality SLAs, freshness, access terms, and change notification.	Formal data contracts are in place for all critical data products. Contracts define quality SLAs, freshness, access terms, and change notification.	Formal data contracts are in place for all critical data products. Contracts define quality SLAs, freshness, access terms, and change notification.
4 - Managed	Contract compliance is monitored. SLA breaches trigger defined responses. Contracts are reviewed when data products change.	Contract compliance is monitored. SLA breaches trigger defined responses. Contracts are reviewed when data products change.	Contract compliance is monitored. SLA breaches trigger defined responses. Contracts are reviewed when data products change.
5 - Optimised	Data contracts are the standard mechanism for data product governance. Contract compliance is automated. AI training data contracts define quality and provenance requirements.	Data contracts are the standard mechanism for data product governance. Contract compliance is automated. AI training data contracts define quality and provenance requirements.	Data contracts are the standard mechanism for data product governance. Contract compliance is automated. AI training data contracts define quality and provenance requirements.

11. Domain D10: Lifecycle & Retention

Domain	Lifecycle & Retention
Domain ID	D10
Weighting	8.33%
Measures	8
Purpose	Data that is retained beyond its purpose is a liability. Data that is deleted before it is needed is a loss. Governance of the full data lifecycle - from creation through active use to archival, deletion, and decommissioning - is fundamental to GDPR compliance, AI audit readiness, and operational efficiency. This domain is particularly critical for AI systems: the datasets used to train models must be retained for audit purposes, but personal data used in training must also be managed within consent and purpose limitation frameworks. These obligations create tension that only deliberate lifecycle governance can resolve.
Regulatory Context	GDPR Articles 5(1)(e), 17 (storage limitation, right to erasure). EU AI Act Article 12 (logging and record-keeping). ISO 42001 Clause 7.5 (documented information). Multiple jurisdiction-specific data retention regulations.

D10.1 - Retention Policy

Measure ID	Measure Name	Governs	Normative References
D10.1	Retention Policy	Whether data retention policies are defined for all critical data classes and whether those policies are enforced.	GDPR Art.5(1)(e) EU AI Act Art.12 ISO 42001 Clause 7.5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No retention policies. Data is retained indefinitely by default.	No retention policies. Data is retained indefinitely by default.	No retention policies. Data is retained indefinitely by default.
1 - Ad Hoc	Retention is discussed informally. Policy exists for regulated data only.	Retention is discussed informally. Policy exists for regulated data only.	Retention is discussed informally. Policy exists for regulated data only.
2 - Repeatable	Retention policies exist for major data classes. Enforcement is inconsistent.	Retention policies exist for major data classes. Enforcement is inconsistent.	Retention policies exist for major data classes. Enforcement is inconsistent.
3 - Defined	Formal retention policies cover all critical data classes. Policies are enforced through process and tooling. Retention periods are aligned to regulatory requirements.	Formal retention policies cover all critical data classes. Policies are enforced through process and tooling. Retention periods are aligned to regulatory requirements.	Formal retention policies cover all critical data classes. Policies are enforced through process and tooling. Retention periods are aligned to regulatory requirements.
4 - Managed	Policy compliance is monitored and audited. Retention periods are reviewed when regulations change. AI training data retention is specifically governed.	Policy compliance is monitored and audited. Retention periods are reviewed when regulations change. AI training data retention is specifically governed.	Policy compliance is monitored and audited. Retention periods are reviewed when regulations change. AI training data retention is specifically governed.
5 - Optimised	Retention governance is automated. Data cannot be retained beyond its policy period without a formal extension approval. AI data retention is part of the AI lifecycle governance.	Retention governance is automated. Data cannot be retained beyond its policy period without a formal extension approval. AI data retention is part of the AI lifecycle governance.	Retention governance is automated. Data cannot be retained beyond its policy period without a formal extension approval. AI data retention is part of the AI lifecycle governance.

D10.2 - Archival Process

Measure ID	Measure Name	Governs	Normative References
D10.2	Archival Process	Whether a governed archival process exists with defined criteria for when and how data is moved from active to archived state.	GDPR Art.5(1)(e) ISO 42001 Clause 7.5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No archival process. Data is either in active use or deleted.	No archival process. Data is either in active use or deleted.	No archival process. Data is either in active use or deleted.
1 - Ad Hoc	Archival is managed informally on a case-by-case basis.	Archival is managed informally on a case-by-case basis.	Archival is managed informally on a case-by-case basis.
2 - Repeatable	An archival process exists for major data classes. Criteria are informal.	An archival process exists for major data classes. Criteria are informal.	An archival process exists for major data classes. Criteria are informal.
3 - Defined	A formal archival process with defined criteria covers all critical data classes. Archived data is accessible to authorised parties. Archival events are logged.	A formal archival process with defined criteria covers all critical data classes. Archived data is accessible to authorised parties. Archival events are logged.	A formal archival process with defined criteria covers all critical data classes. Archived data is accessible to authorised parties. Archival events are logged.
4 - Managed	Archival processes are automated where possible. Archived data retrieval SLAs are defined. Archive integrity is verified.	Archival processes are automated where possible. Archived data retrieval SLAs are defined. Archive integrity is verified.	Archival processes are automated where possible. Archived data retrieval SLAs are defined. Archive integrity is verified.
5 - Optimised	Archival governance is fully automated. Data lifecycle transitions are logged and auditable. AI training data archival is governed as part of the AI lifecycle.	Archival governance is fully automated. Data lifecycle transitions are logged and auditable. AI training data archival is governed as part of the AI lifecycle.	Archival governance is fully automated. Data lifecycle transitions are logged and auditable. AI training data archival is governed as part of the AI lifecycle.

D10.3 - Deletion & Right to Erasure

Measure ID	Measure Name	Governs	Normative References
D10.3	Deletion & Right to Erasure	Whether processes are in place to fulfil data subject deletion requests within regulatory timescales, including deletion from AI training data and models.	GDPR Art.17 EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No deletion process. Data subject requests cannot be fulfilled.	No deletion process. Data subject requests cannot be fulfilled.	No deletion process. Data subject requests cannot be fulfilled.
1 - Ad Hoc	Deletion requests are managed manually and informally.	Deletion requests are managed manually and informally.	Deletion requests are managed manually and informally.
2 - Repeatable	A deletion process exists for structured personal data. AI training data and models are not addressed.	A deletion process exists for structured personal data. AI training data and models are not addressed.	A deletion process exists for structured personal data. AI training data and models are not addressed.
3 - Defined	A formal deletion process covers structured and unstructured personal data. Timescales are defined and met. AI training data deletion is addressed in policy.	A formal deletion process covers structured and unstructured personal data. Timescales are defined and met. AI training data deletion is addressed in policy.	A formal deletion process covers structured and unstructured personal data. Timescales are defined and met. AI training data deletion is addressed in policy.
4 - Managed	Deletion processes are tested regularly. Timescale compliance is measured. AI model retraining following data deletion is governed.	Deletion processes are tested regularly. Timescale compliance is measured. AI model retraining following data deletion is governed.	Deletion processes are tested regularly. Timescale compliance is measured. AI model retraining following data deletion is governed.
5 - Optimised	Deletion is automated where technically feasible. AI model deletion implications are formally assessed. Right to erasure obligations are embedded in data product design.	Deletion is automated where technically feasible. AI model deletion implications are formally assessed. Right to erasure obligations are embedded in data product design.	Deletion is automated where technically feasible. AI model deletion implications are formally assessed. Right to erasure obligations are embedded in data product design.

D10.4 - End-of-Life Governance

Measure ID	Measure Name	Governs	Normative References
D10.4	End-of-Life Governance	Whether a formal process exists for decommissioning data assets at the end of their useful life.	ISO 8000-8 ISO 42001 Clause 7.5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No decommissioning process. Systems and datasets are retired informally.	No decommissioning process. Systems and datasets are retired informally.	No decommissioning process. Systems and datasets are retired informally.
1 - Ad Hoc	Decommissioning is handled case-by-case. No defined process.	Decommissioning is handled case-by-case. No defined process.	Decommissioning is handled case-by-case. No defined process.
2 - Repeatable	A decommissioning process exists for major systems. Data assets are not specifically addressed.	A decommissioning process exists for major systems. Data assets are not specifically addressed.	A decommissioning process exists for major systems. Data assets are not specifically addressed.
3 - Defined	A formal data asset decommissioning process covers all critical assets. Decommissioning includes dependency assessment, consumer notification, and final deletion or archival.	A formal data asset decommissioning process covers all critical assets. Decommissioning includes dependency assessment, consumer notification, and final deletion or archival.	A formal data asset decommissioning process covers all critical assets. Decommissioning includes dependency assessment, consumer notification, and final deletion or archival.
4 - Managed	Decommissioning events are logged and auditable. Consumer impact is assessed before decommissioning. AI model retirement follows a formal process.	Decommissioning events are logged and auditable. Consumer impact is assessed before decommissioning. AI model retirement follows a formal process.	Decommissioning events are logged and auditable. Consumer impact is assessed before decommissioning. AI model retirement follows a formal process.
5 - Optimised	End-of-life governance is embedded in the data asset lifecycle. Decommissioning records are maintained. AI model retirement is governed and documented.	End-of-life governance is embedded in the data asset lifecycle. Decommissioning records are maintained. AI model retirement is governed and documented.	End-of-life governance is embedded in the data asset lifecycle. Decommissioning records are maintained. AI model retirement is governed and documented.

D10.5 - AI Training Data Retention

Measure ID	Measure Name	Governs	Normative References
D10.5	AI Training Data Retention	Whether datasets used for AI training are retained and accessible for audit for periods aligned to model lifecycle and regulatory obligations.	EU AI Act Art.12 ISO 42001 Clause 7.5 GDPR Art.5(1)(e)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	AI training data is not retained after model deployment.	AI training data is not retained after model deployment.	AI training data is not retained after model deployment.
1 - Ad Hoc	Retention is informal. Training data may exist on local developer systems.	Retention is informal. Training data may exist on local developer systems.	Retention is informal. Training data may exist on local developer systems.
2 - Repeatable	Retention policy exists for some AI training datasets. Versioning is absent.	Retention policy exists for some AI training datasets. Versioning is absent.	Retention policy exists for some AI training datasets. Versioning is absent.
3 - Defined	AI training datasets are formally retained and versioned for defined periods. Retention is aligned to model lifecycle and regulatory requirements. Datasets are accessible to authorised parties.	AI training datasets are formally retained and versioned for defined periods. Retention is aligned to model lifecycle and regulatory requirements. Datasets are accessible to authorised parties.	AI training datasets are formally retained and versioned for defined periods. Retention is aligned to model lifecycle and regulatory requirements. Datasets are accessible to authorised parties.
4 - Managed	Retention is systematically managed. Dataset accessibility is verified periodically. Retention periods are reviewed when regulatory requirements change.	Retention is systematically managed. Dataset accessibility is verified periodically. Retention periods are reviewed when regulatory requirements change.	Retention is systematically managed. Dataset accessibility is verified periodically. Retention periods are reviewed when regulatory requirements change.
5 - Optimised	AI training data retention is governed as part of the AI lifecycle. Retained datasets are stored in governed, auditable storage. Retention records form part of the AI audit trail.	AI training data retention is governed as part of the AI lifecycle. Retained datasets are stored in governed, auditable storage. Retention records form part of the AI audit trail.	AI training data retention is governed as part of the AI lifecycle. Retained datasets are stored in governed, auditable storage. Retention records form part of the AI audit trail.

D10.6 - Regulatory Retention Alignment

Measure ID	Measure Name	Governs	Normative References
D10.6	Regulatory Retention Alignment	Whether retention schedules are explicitly aligned to regulatory requirements across all applicable jurisdictions.	GDPR Art.5(1)(e) EU AI Act Art.12 multiple jurisdictions
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Retention schedules are not aligned to regulatory requirements.	Retention schedules are not aligned to regulatory requirements.	Retention schedules are not aligned to regulatory requirements.
1 - Ad Hoc	Key regulatory retention requirements are informally known.	Key regulatory retention requirements are informally known.	Key regulatory retention requirements are informally known.
2 - Repeatable	Retention schedules are aligned to major regulations. Multi-jurisdiction requirements are not fully addressed.	Retention schedules are aligned to major regulations. Multi-jurisdiction requirements are not fully addressed.	Retention schedules are aligned to major regulations. Multi-jurisdiction requirements are not fully addressed.
3 - Defined	Retention schedules are formally aligned to all applicable regulatory requirements. Multi-jurisdiction obligations are documented and managed.	Retention schedules are formally aligned to all applicable regulatory requirements. Multi-jurisdiction obligations are documented and managed.	Retention schedules are formally aligned to all applicable regulatory requirements. Multi-jurisdiction obligations are documented and managed.
4 - Managed	Regulatory alignment is reviewed on a defined cycle. Regulatory changes trigger retention schedule review. Multi-jurisdiction conflicts are formally resolved.	Regulatory alignment is reviewed on a defined cycle. Regulatory changes trigger retention schedule review. Multi-jurisdiction conflicts are formally resolved.	Regulatory alignment is reviewed on a defined cycle. Regulatory changes trigger retention schedule review. Multi-jurisdiction conflicts are formally resolved.
5 - Optimised	Regulatory retention alignment is continuously maintained. A regulatory horizon-scanning process identifies upcoming changes. Retention schedules are automatically updated when regulations change.	Regulatory retention alignment is continuously maintained. A regulatory horizon-scanning process identifies upcoming changes. Retention schedules are automatically updated when regulations change.	Regulatory retention alignment is continuously maintained. A regulatory horizon-scanning process identifies upcoming changes. Retention schedules are automatically updated when regulations change.

D10.7 - Data Minimisation

Measure ID	Measure Name	Governs	Normative References
D10.7	Data Minimisation	Whether data is collected and retained only to the extent necessary for its documented purpose.	GDPR Art.5(1)(c) EU AI Act Art.10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Data is collected and retained without consideration of minimisation.	Data is collected and retained without consideration of minimisation.	Data is collected and retained without consideration of minimisation.
1 - Ad Hoc	Minimisation is considered informally for some data collections.	Minimisation is considered informally for some data collections.	Minimisation is considered informally for some data collections.
2 - Repeatable	Data minimisation is applied to personal data. Other data types are not addressed.	Data minimisation is applied to personal data. Other data types are not addressed.	Data minimisation is applied to personal data. Other data types are not addressed.
3 - Defined	Data minimisation is applied to all critical data collections. New data collections require documented justification for each data element.	Data minimisation is applied to all critical data collections. New data collections require documented justification for each data element.	Data minimisation is applied to all critical data collections. New data collections require documented justification for each data element.
4 - Managed	Minimisation assessments are conducted periodically for existing data assets. Over-collection is identified and remediated.	Minimisation assessments are conducted periodically for existing data assets. Over-collection is identified and remediated.	Minimisation assessments are conducted periodically for existing data assets. Over-collection is identified and remediated.
5 - Optimised	Data minimisation is embedded in data product design. New data collections cannot proceed without a minimisation assessment. AI training data minimisation is governed.	Data minimisation is embedded in data product design. New data collections cannot proceed without a minimisation assessment. AI training data minimisation is governed.	Data minimisation is embedded in data product design. New data collections cannot proceed without a minimisation assessment. AI training data minimisation is governed.

D10.8 - Lifecycle Audit Trail

Measure ID	Measure Name	Governs	Normative References
D10.8	Lifecycle Audit Trail	Whether an auditable record of data asset lifecycle events is maintained, including creation, change, transfer, archival, and deletion.	ISO 42001 Clause 7.5 EU AI Act Art.12 GDPR Art.5(2)
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No lifecycle audit trail. Asset history is unknown.	No lifecycle audit trail. Asset history is unknown.	No lifecycle audit trail. Asset history is unknown.
1 - Ad Hoc	Lifecycle events are partially recorded in system logs.	Lifecycle events are partially recorded in system logs.	Lifecycle events are partially recorded in system logs.
2 - Repeatable	Lifecycle events are recorded for major data assets. Not comprehensive.	Lifecycle events are recorded for major data assets. Not comprehensive.	Lifecycle events are recorded for major data assets. Not comprehensive.
3 - Defined	A formal lifecycle audit trail records all key events for critical data assets. Records are tamper-evident and retained for defined periods.	A formal lifecycle audit trail records all key events for critical data assets. Records are tamper-evident and retained for defined periods.	A formal lifecycle audit trail records all key events for critical data assets. Records are tamper-evident and retained for defined periods.
4 - Managed	Audit trail completeness is monitored. Events trigger automated notifications to data owners. Trails are reviewed periodically.	Audit trail completeness is monitored. Events trigger automated notifications to data owners. Trails are reviewed periodically.	Audit trail completeness is monitored. Events trigger automated notifications to data owners. Trails are reviewed periodically.
5 - Optimised	Lifecycle audit trails are comprehensive and automated. AI data asset lifecycle events are included. Trails support regulatory examination and internal assurance.	Lifecycle audit trails are comprehensive and automated. AI data asset lifecycle events are included. Trails support regulatory examination and internal assurance.	Lifecycle audit trails are comprehensive and automated. AI data asset lifecycle events are included. Trails support regulatory examination and internal assurance.

12. Domain D11: Organisational Readiness

Domain	Organisational Readiness
Domain ID	D11
Weighting	8.33%
Measures	10
Purpose	Technical governance controls fail without organisational capability to design, implement, and sustain them. This domain governs the human side of data and AI governance: data literacy, AI literacy, change management capability, training programmes, executive commitment, and the cultural conditions that make governance stick. Organisations that score highly in technical domains but poorly here are typically running governance on the effort of a small expert team with limited organisational penetration. That model does not scale and does not survive personnel change.
Regulatory Context	EU AI Act Article 4 (AI literacy - operators and providers must ensure sufficient AI literacy for their staff). ISO 42001 Clause 7 (support: competence, awareness, communication). ISO 8000-8 Clause 7.

D11.1 - Data Literacy

Measure ID	Measure Name	Governs	Normative References
D11.1	Data Literacy	Whether data literacy is assessed across the organisation and whether a structured programme is in place to improve it.	ISO 8000-8 Clause 7 ISO 42001 Clause 7.2
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Data literacy is not considered. Staff use data without understanding quality or governance.	Data literacy is not considered. Staff use data without understanding quality or governance.	Data literacy is not considered. Staff use data without understanding quality or governance.
1 - Ad Hoc	Data literacy is recognised as a gap. No assessment or programme.	Data literacy is recognised as a gap. No assessment or programme.	Data literacy is recognised as a gap. No assessment or programme.
2 - Repeatable	Data literacy is assessed informally for some roles. Improvement is ad hoc.	Data literacy is assessed informally for some roles. Improvement is ad hoc.	Data literacy is assessed informally for some roles. Improvement is ad hoc.
3 - Defined	Data literacy is formally assessed across the organisation. A structured improvement programme is in place with defined learning pathways.	Data literacy is formally assessed across the organisation. A structured improvement programme is in place with defined learning pathways.	Data literacy is formally assessed across the organisation. A structured improvement programme is in place with defined learning pathways.
4 - Managed	Literacy levels are tracked over time. Programme effectiveness is measured. Literacy requirements are built into role profiles.	Literacy levels are tracked over time. Programme effectiveness is measured. Literacy requirements are built into role profiles.	Literacy levels are tracked over time. Programme effectiveness is measured. Literacy requirements are built into role profiles.
5 - Optimised	Data literacy is embedded in the organisational talent framework. Literacy levels are monitored continuously. The programme is benchmarked against peer organisations.	Data literacy is embedded in the organisational talent framework. Literacy levels are monitored continuously. The programme is benchmarked against peer organisations.	Data literacy is embedded in the organisational talent framework. Literacy levels are monitored continuously. The programme is benchmarked against peer organisations.

D11.2 - AI Literacy

Measure ID	Measure Name	Governs	Normative References
D11.2	AI Literacy	Whether staff understand AI capabilities, limitations, and risks sufficiently to use AI outputs responsibly and to govern AI systems appropriately.	EU AI Act Art.4 ISO 42001 Clause 7.2
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No AI literacy. Staff use AI outputs without understanding limitations or risks.	No AI literacy. Staff use AI outputs without understanding limitations or risks.	No AI literacy. Staff use AI outputs without understanding limitations or risks.
1 - Ad Hoc	AI literacy is recognised as a need. No structured programme.	AI literacy is recognised as a need. No structured programme.	AI literacy is recognised as a need. No structured programme.
2 - Repeatable	Basic AI awareness training is available. Coverage and depth are insufficient.	Basic AI awareness training is available. Coverage and depth are insufficient.	Basic AI awareness training is available. Coverage and depth are insufficient.
3 - Defined	A structured AI literacy programme is in place, differentiated by role. Coverage is measured. EU AI Act literacy requirements are addressed.	A structured AI literacy programme is in place, differentiated by role. Coverage is measured. EU AI Act literacy requirements are addressed.	A structured AI literacy programme is in place, differentiated by role. Coverage is measured. EU AI Act literacy requirements are addressed.
4 - Managed	AI literacy levels are assessed and tracked. Programme content is updated as AI capabilities and regulations evolve.	AI literacy levels are assessed and tracked. Programme content is updated as AI capabilities and regulations evolve.	AI literacy levels are assessed and tracked. Programme content is updated as AI capabilities and regulations evolve.
5 - Optimised	AI literacy is embedded in the organisational learning framework. AI literacy assessment is part of role onboarding. The programme meets and exceeds EU AI Act Article 4 requirements.	AI literacy is embedded in the organisational learning framework. AI literacy assessment is part of role onboarding. The programme meets and exceeds EU AI Act Article 4 requirements.	AI literacy is embedded in the organisational learning framework. AI literacy assessment is part of role onboarding. The programme meets and exceeds EU AI Act Article 4 requirements.

D11.3 - Change Management Capability

Measure ID	Measure Name	Governs	Normative References
D11.3	Change Management Capability	Whether the organisation has demonstrated capability to plan and deliver data and AI governance change programmes.	ISO 8000-8 Clause 8 ISO 42001 Clause 8
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No change management capability for governance programmes.	No change management capability for governance programmes.	No change management capability for governance programmes.
1 - Ad Hoc	Change is managed informally. Governance initiatives frequently stall.	Change is managed informally. Governance initiatives frequently stall.	Change is managed informally. Governance initiatives frequently stall.
2 - Repeatable	Basic change management is applied to governance initiatives. Track record is mixed.	Basic change management is applied to governance initiatives. Track record is mixed.	Basic change management is applied to governance initiatives. Track record is mixed.
3 - Defined	A structured change management approach is applied to all governance programmes. Stakeholder engagement and communication are planned.	A structured change management approach is applied to all governance programmes. Stakeholder engagement and communication are planned.	A structured change management approach is applied to all governance programmes. Stakeholder engagement and communication are planned.
4 - Managed	Change management effectiveness is measured. Lessons from past programmes inform future ones. Governance change is embedded in programme governance.	Change management effectiveness is measured. Lessons from past programmes inform future ones. Governance change is embedded in programme governance.	Change management effectiveness is measured. Lessons from past programmes inform future ones. Governance change is embedded in programme governance.
5 - Optimised	Change management is a core organisational capability. Governance programmes deliver to plan. The organisation has a track record of sustained governance improvement.	Change management is a core organisational capability. Governance programmes deliver to plan. The organisation has a track record of sustained governance improvement.	Change management is a core organisational capability. Governance programmes deliver to plan. The organisation has a track record of sustained governance improvement.

D11.4 - Training Programme

Measure ID	Measure Name	Governs	Normative References
D11.4	Training Programme	Whether a structured, role-appropriate training programme for data and AI governance exists and is actively maintained.	ISO 8000-8 Clause 7 ISO 42001 Clause 7.2 EU AI Act Art.4
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No formal training programme for data or AI governance.	No formal training programme for data or AI governance.	No formal training programme for data or AI governance.
1 - Ad Hoc	Training is ad hoc. Individuals find their own development resources.	Training is ad hoc. Individuals find their own development resources.	Training is ad hoc. Individuals find their own development resources.
2 - Repeatable	Some training is available but not structured or role-differentiated.	Some training is available but not structured or role-differentiated.	Some training is available but not structured or role-differentiated.
3 - Defined	A structured training programme covers data governance and AI governance. Content is role-differentiated. Completion is tracked.	A structured training programme covers data governance and AI governance. Content is role-differentiated. Completion is tracked.	A structured training programme covers data governance and AI governance. Content is role-differentiated. Completion is tracked.
4 - Managed	Training effectiveness is assessed. Content is updated when the DQI Standard or regulations change. Training completion is a governance KPI.	Training effectiveness is assessed. Content is updated when the DQI Standard or regulations change. Training completion is a governance KPI.	Training effectiveness is assessed. Content is updated when the DQI Standard or regulations change. Training completion is a governance KPI.
5 - Optimised	Training is delivered through a governed LMS. Completion is mandatory for key roles. Training aligns to the DQI education pathway and certification requirements.	Training is delivered through a governed LMS. Completion is mandatory for key roles. Training aligns to the DQI education pathway and certification requirements.	Training is delivered through a governed LMS. Completion is mandatory for key roles. Training aligns to the DQI education pathway and certification requirements.

D11.5 - Executive Commitment

Measure ID	Measure Name	Governs	Normative References
D11.5	Executive Commitment	Whether executive commitment to data and AI governance is demonstrated through investment decisions and visible leadership.	ISO 8000-8 Clause 5 ISO 42001 Clause 5.1
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No executive commitment. Governance is a bottom-up initiative without senior support.	No executive commitment. Governance is a bottom-up initiative without senior support.	No executive commitment. Governance is a bottom-up initiative without senior support.
1 - Ad Hoc	Executive support is verbal. No investment or visible leadership.	Executive support is verbal. No investment or visible leadership.	Executive support is verbal. No investment or visible leadership.
2 - Repeatable	An executive champion exists. Engagement is periodic. Investment is limited.	An executive champion exists. Engagement is periodic. Investment is limited.	An executive champion exists. Engagement is periodic. Investment is limited.
3 - Defined	Executive commitment is demonstrated through named sponsorship, approved investment, and visible engagement. Governance is an ExCo agenda item.	Executive commitment is demonstrated through named sponsorship, approved investment, and visible engagement. Governance is an ExCo agenda item.	Executive commitment is demonstrated through named sponsorship, approved investment, and visible engagement. Governance is an ExCo agenda item.
4 - Managed	Board-level visibility of governance maturity. Investment tracks governance roadmap. Executive performance includes governance KPIs.	Board-level visibility of governance maturity. Investment tracks governance roadmap. Executive performance includes governance KPIs.	Board-level visibility of governance maturity. Investment tracks governance roadmap. Executive performance includes governance KPIs.
5 - Optimised	Governance is a board-level strategic priority. The board receives regular maturity reporting. Governance investment is treated as strategic infrastructure.	Governance is a board-level strategic priority. The board receives regular maturity reporting. Governance investment is treated as strategic infrastructure.	Governance is a board-level strategic priority. The board receives regular maturity reporting. Governance investment is treated as strategic infrastructure.

D11.6 - Culture of Data Quality

Measure ID	Measure Name	Governs	Normative References
D11.6	Culture of Data Quality	Whether data quality is treated as a shared organisational responsibility rather than the exclusive concern of the data team.	ISO 8000-8 Clause 5 ISO 42001 Clause 5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Data quality is seen as an IT or data team problem. Business teams feel no responsibility.	Data quality is seen as an IT or data team problem. Business teams feel no responsibility.	Data quality is seen as an IT or data team problem. Business teams feel no responsibility.
1 - Ad Hoc	Some business teams engage with data quality when it affects their operations.	Some business teams engage with data quality when it affects their operations.	Some business teams engage with data quality when it affects their operations.
2 - Repeatable	A growing number of business teams see data quality as a shared concern. Culture is uneven.	A growing number of business teams see data quality as a shared concern. Culture is uneven.	A growing number of business teams see data quality as a shared concern. Culture is uneven.
3 - Defined	Data quality is recognised as a shared responsibility across the organisation. Business teams actively participate in governance.	Data quality is recognised as a shared responsibility across the organisation. Business teams actively participate in governance.	Data quality is recognised as a shared responsibility across the organisation. Business teams actively participate in governance.
4 - Managed	Data quality culture is embedded and measurable. Business teams proactively identify and report quality issues. Culture surveys track progress.	Data quality culture is embedded and measurable. Business teams proactively identify and report quality issues. Culture surveys track progress.	Data quality culture is embedded and measurable. Business teams proactively identify and report quality issues. Culture surveys track progress.
5 - Optimised	Data quality culture is a strategic organisational value. It is embedded in induction, performance management, and leadership communication.	Data quality culture is a strategic organisational value. It is embedded in induction, performance management, and leadership communication.	Data quality culture is a strategic organisational value. It is embedded in induction, performance management, and leadership communication.

D11.7 - Incentive Alignment

Measure ID	Measure Name	Governs	Normative References
D11.7	Incentive Alignment	Whether staff performance objectives are aligned to data quality and governance outcomes.	ISO 8000-8 Clause 5 ISO 42001 Clause 5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No performance objectives linked to data quality or governance.	No performance objectives linked to data quality or governance.	No performance objectives linked to data quality or governance.
1 - Ad Hoc	Data quality mentioned in some role profiles without measurement.	Data quality mentioned in some role profiles without measurement.	Data quality mentioned in some role profiles without measurement.
2 - Repeatable	Data quality objectives exist for data team roles. Not extended to business roles.	Data quality objectives exist for data team roles. Not extended to business roles.	Data quality objectives exist for data team roles. Not extended to business roles.
3 - Defined	Performance objectives linked to data governance outcomes are in place for data owners, stewards, and key business roles.	Performance objectives linked to data governance outcomes are in place for data owners, stewards, and key business roles.	Performance objectives linked to data governance outcomes are in place for data owners, stewards, and key business roles.
4 - Managed	Data governance performance objectives are reviewed annually. Incentives are aligned to governance priorities. Poor governance performance is addressed.	Data governance performance objectives are reviewed annually. Incentives are aligned to governance priorities. Poor governance performance is addressed.	Data governance performance objectives are reviewed annually. Incentives are aligned to governance priorities. Poor governance performance is addressed.
5 - Optimised	Governance outcomes are embedded across all relevant role profiles. Incentive alignment is reviewed when governance priorities change.	Governance outcomes are embedded across all relevant role profiles. Incentive alignment is reviewed when governance priorities change.	Governance outcomes are embedded across all relevant role profiles. Incentive alignment is reviewed when governance priorities change.

D11.8 - Cross-Functional Collaboration

Measure ID	Measure Name	Governs	Normative References
D11.8	Cross-Functional Collaboration	Whether business and technology teams collaborate effectively on governance initiatives rather than operating in silos.	ISO 8000-8 Clause 5 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Business and technology teams operate in silos on governance. Collaboration is absent.	Business and technology teams operate in silos on governance. Collaboration is absent.	Business and technology teams operate in silos on governance. Collaboration is absent.
1 - Ad Hoc	Collaboration occurs on specific projects. Not embedded in governance.	Collaboration occurs on specific projects. Not embedded in governance.	Collaboration occurs on specific projects. Not embedded in governance.
2 - Repeatable	A cross-functional data governance forum exists. Collaboration is improving.	A cross-functional data governance forum exists. Collaboration is improving.	A cross-functional data governance forum exists. Collaboration is improving.
3 - Defined	Business and technology teams collaborate actively on governance initiatives through formal mechanisms. Joint working groups operate on defined topics.	Business and technology teams collaborate actively on governance initiatives through formal mechanisms. Joint working groups operate on defined topics.	Business and technology teams collaborate actively on governance initiatives through formal mechanisms. Joint working groups operate on defined topics.
4 - Managed	Cross-functional collaboration is embedded in governance programme design. Joint working group outcomes are tracked and reported.	Cross-functional collaboration is embedded in governance programme design. Joint working group outcomes are tracked and reported.	Cross-functional collaboration is embedded in governance programme design. Joint working group outcomes are tracked and reported.
5 - Optimised	Collaboration is the default mode for governance. Business-technology joint teams own governance domains. Collaboration is a measured organisational capability.	Collaboration is the default mode for governance. Business-technology joint teams own governance domains. Collaboration is a measured organisational capability.	Collaboration is the default mode for governance. Business-technology joint teams own governance domains. Collaboration is a measured organisational capability.

D11.9 - Governance Maturity Roadmap

Measure ID	Measure Name	Governs	Normative References
D11.9	Governance Maturity Roadmap	Whether the organisation has a documented, active, and executive-sponsored governance maturity roadmap.	ISO 8000-8 Clause 6 ISO 42001 Clause 6
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No maturity roadmap. Governance is reactive.	No maturity roadmap. Governance is reactive.	No maturity roadmap. Governance is reactive.
1 - Ad Hoc	Improvement areas are informally identified but not documented as a roadmap.	Improvement areas are informally identified but not documented as a roadmap.	Improvement areas are informally identified but not documented as a roadmap.
2 - Repeatable	A roadmap exists but is not formally sponsored or actively managed.	A roadmap exists but is not formally sponsored or actively managed.	A roadmap exists but is not formally sponsored or actively managed.
3 - Defined	A formal governance maturity roadmap is documented, executive-sponsored, and actively managed. Progress is reviewed quarterly.	A formal governance maturity roadmap is documented, executive-sponsored, and actively managed. Progress is reviewed quarterly.	A formal governance maturity roadmap is documented, executive-sponsored, and actively managed. Progress is reviewed quarterly.
4 - Managed	The roadmap is used to prioritise investment. Progress is reported to executive leadership and the board. The roadmap is updated when priorities change.	The roadmap is used to prioritise investment. Progress is reported to executive leadership and the board. The roadmap is updated when priorities change.	The roadmap is used to prioritise investment. Progress is reported to executive leadership and the board. The roadmap is updated when priorities change.
5 - Optimised	The roadmap is a strategic governance instrument. It is integrated with business planning. Progress is publicly reported where appropriate. The roadmap references the DQI target maturity levels.	The roadmap is a strategic governance instrument. It is integrated with business planning. Progress is publicly reported where appropriate. The roadmap references the DQI target maturity levels.	The roadmap is a strategic governance instrument. It is integrated with business planning. Progress is publicly reported where appropriate. The roadmap references the DQI target maturity levels.

D11.10 - External Benchmarking

Measure ID	Measure Name	Governs	Normative References
D11.10	External Benchmarking	Whether the organisation actively benchmarks its governance maturity against peer organisations and industry standards.	ISO 8000-8 Clause 9 ISO 42001 Clause 9.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No benchmarking. The organisation has no external reference point.	No benchmarking. The organisation has no external reference point.	No benchmarking. The organisation has no external reference point.
1 - Ad Hoc	External benchmarking is discussed. No structured approach.	External benchmarking is discussed. No structured approach.	External benchmarking is discussed. No structured approach.
2 - Repeatable	Informal benchmarking occurs through industry events or peer conversations.	Informal benchmarking occurs through industry events or peer conversations.	Informal benchmarking occurs through industry events or peer conversations.
3 - Defined	Formal benchmarking is conducted using a recognised framework. Results inform the governance roadmap.	Formal benchmarking is conducted using a recognised framework. Results inform the governance roadmap.	Formal benchmarking is conducted using a recognised framework. Results inform the governance roadmap.
4 - Managed	Benchmarking is conducted on a defined cycle. Results are compared over time. The organisation contributes to benchmark datasets.	Benchmarking is conducted on a defined cycle. Results are compared over time. The organisation contributes to benchmark datasets.	Benchmarking is conducted on a defined cycle. Results are compared over time. The organisation contributes to benchmark datasets.
5 - Optimised	The organisation is a benchmark contributor and uses benchmark data to set and validate governance targets. DQI assessment results are used as the primary benchmark instrument.	The organisation is a benchmark contributor and uses benchmark data to set and validate governance targets. DQI assessment results are used as the primary benchmark instrument.	The organisation is a benchmark contributor and uses benchmark data to set and validate governance targets. DQI assessment results are used as the primary benchmark instrument.

13. Domain D12: Sustainable & Maintainable

Domain	Sustainable & Maintainable
Domain ID	D12
Weighting	8.33%
Measures	8
Purpose	Governance that depends on heroic individual effort is governance waiting to fail. This domain governs the sustainability and maintainability of the data and AI governance programme itself: whether assets, processes, and AI models are documented, whether technical debt is managed, whether knowledge is retained when people leave, and whether there is a mechanism for continuous improvement. Organisations that perform well in Domains 1-11 but poorly here are typically building on foundations that will degrade as teams change and complexity grows.
Regulatory Context	ISO 8000-8 Clause 7 (documented information). ISO 42001 Clause 7.5 (documented information). EU AI Act Article 11 (technical documentation requirements for high-risk AI systems).

D12.1 - Documentation

Measure ID	Measure Name	Governs	Normative References
D12.1	Documentation	Whether data assets, pipelines, governance rules, and AI models are fully and currently documented.	ISO 8000-8 Clause 7.5 ISO 42001 Clause 7.5 EU AI Act Art.11
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Documentation is absent. Knowledge exists only in people's heads.	Documentation is absent. Knowledge exists only in people's heads.	Documentation is absent. Knowledge exists only in people's heads.
1 - Ad Hoc	Documentation is sparse and informal. Out of date.	Documentation is sparse and informal. Out of date.	Documentation is sparse and informal. Out of date.
2 - Repeatable	Documentation exists for major assets. Currency and completeness are inconsistent.	Documentation exists for major assets. Currency and completeness are inconsistent.	Documentation exists for major assets. Currency and completeness are inconsistent.
3 - Defined	All critical data assets, pipelines, and AI models are documented. Documentation is kept current. A documentation standard exists.	All critical data assets, pipelines, and AI models are documented. Documentation is kept current. A documentation standard exists.	All critical data assets, pipelines, and AI models are documented. Documentation is kept current. A documentation standard exists.
4 - Managed	Documentation completeness is measured and tracked. Updates are triggered by changes. Documentation quality is reviewed periodically.	Documentation completeness is measured and tracked. Updates are triggered by changes. Documentation quality is reviewed periodically.	Documentation completeness is measured and tracked. Updates are triggered by changes. Documentation quality is reviewed periodically.
5 - Optimised	Documentation is comprehensive and automatically maintained where possible. AI model documentation meets EU AI Act Article 11 requirements. Documentation is version-controlled.	Documentation is comprehensive and automatically maintained where possible. AI model documentation meets EU AI Act Article 11 requirements. Documentation is version-controlled.	Documentation is comprehensive and automatically maintained where possible. AI model documentation meets EU AI Act Article 11 requirements. Documentation is version-controlled.

D12.2 - Technical Debt Management

Measure ID	Measure Name	Governs	Normative References
D12.2	Technical Debt Management	Whether a process exists to identify, prioritise, and systematically reduce data and AI technical debt.	ISO 8000-61 ISO 42001 Clause 10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Technical debt is unmanaged and untracked.	Technical debt is unmanaged and untracked.	Technical debt is unmanaged and untracked.
1 - Ad Hoc	Technical debt is recognised informally. No formal process.	Technical debt is recognised informally. No formal process.	Technical debt is recognised informally. No formal process.
2 - Repeatable	Major technical debt items are identified. A remediation plan exists in principle.	Major technical debt items are identified. A remediation plan exists in principle.	Major technical debt items are identified. A remediation plan exists in principle.
3 - Defined	Technical debt is formally tracked in a register. A prioritised reduction programme is active. Debt reduction progress is reported.	Technical debt is formally tracked in a register. A prioritised reduction programme is active. Debt reduction progress is reported.	Technical debt is formally tracked in a register. A prioritised reduction programme is active. Debt reduction progress is reported.
4 - Managed	Debt reduction is a governance priority. Investment is allocated. Progress is measured. New debt introduction requires approval.	Debt reduction is a governance priority. Investment is allocated. Progress is measured. New debt introduction requires approval.	Debt reduction is a governance priority. Investment is allocated. Progress is measured. New debt introduction requires approval.
5 - Optimised	Technical debt is managed as a governance risk. Debt levels are reported to leadership. AI-specific technical debt (model staleness, ungoverned features) is separately tracked.	Technical debt is managed as a governance risk. Debt levels are reported to leadership. AI-specific technical debt (model staleness, ungoverned features) is separately tracked.	Technical debt is managed as a governance risk. Debt levels are reported to leadership. AI-specific technical debt (model staleness, ungoverned features) is separately tracked.

D12.3 - Onboarding Efficiency

Measure ID	Measure Name	Governs	Normative References
D12.3	Onboarding Efficiency	Whether new team members can become productive within 30 days using existing documentation and onboarding processes.	ISO 8000-8 Clause 7 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	Onboarding relies entirely on colleagues. Documentation is absent.	Onboarding relies entirely on colleagues. Documentation is absent.	Onboarding relies entirely on colleagues. Documentation is absent.
1 - Ad Hoc	Basic onboarding exists but is largely verbal. 60+ days to productivity.	Basic onboarding exists but is largely verbal. 60+ days to productivity.	Basic onboarding exists but is largely verbal. 60+ days to productivity.
2 - Repeatable	Onboarding materials exist for some roles. 45-60 days to productivity typically.	Onboarding materials exist for some roles. 45-60 days to productivity typically.	Onboarding materials exist for some roles. 45-60 days to productivity typically.
3 - Defined	Structured onboarding exists for all data and governance roles. Documentation supports 30-day productivity. Onboarding effectiveness is measured.	Structured onboarding exists for all data and governance roles. Documentation supports 30-day productivity. Onboarding effectiveness is measured.	Structured onboarding exists for all data and governance roles. Documentation supports 30-day productivity. Onboarding effectiveness is measured.
4 - Managed	Onboarding is continuously improved based on new hire feedback. Time-to-productivity is tracked. Governance onboarding is included.	Onboarding is continuously improved based on new hire feedback. Time-to-productivity is tracked. Governance onboarding is included.	Onboarding is continuously improved based on new hire feedback. Time-to-productivity is tracked. Governance onboarding is included.
5 - Optimised	Onboarding is a governed process with defined outcomes. New hires for data and AI roles are productive within 30 days. Onboarding materials are version-controlled.	Onboarding is a governed process with defined outcomes. New hires for data and AI roles are productive within 30 days. Onboarding materials are version-controlled.	Onboarding is a governed process with defined outcomes. New hires for data and AI roles are productive within 30 days. Onboarding materials are version-controlled.

D12.4 - Runbooks & Playbooks

Measure ID	Measure Name	Governs	Normative References
D12.4	Runbooks & Playbooks	Whether runbooks and playbooks are available for all routine support, incident management, and governance tasks.	ISO 8000-61 ISO 42001 Clause 7.5
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No runbooks. Procedures exist only in people's knowledge.	No runbooks. Procedures exist only in people's knowledge.	No runbooks. Procedures exist only in people's knowledge.
1 - Ad Hoc	Some informal procedure documents exist. Not maintained.	Some informal procedure documents exist. Not maintained.	Some informal procedure documents exist. Not maintained.
2 - Repeatable	Runbooks exist for major operational tasks. Governance and AI runbooks are absent.	Runbooks exist for major operational tasks. Governance and AI runbooks are absent.	Runbooks exist for major operational tasks. Governance and AI runbooks are absent.
3 - Defined	Runbooks cover all critical operational, governance, and AI tasks. They are maintained and version-controlled. Runbook use is standard practice.	Runbooks cover all critical operational, governance, and AI tasks. They are maintained and version-controlled. Runbook use is standard practice.	Runbooks cover all critical operational, governance, and AI tasks. They are maintained and version-controlled. Runbook use is standard practice.
4 - Managed	Runbook completeness is measured. Gaps are tracked. Runbooks are tested periodically. Automation replaces runbooks where possible.	Runbook completeness is measured. Gaps are tracked. Runbooks are tested periodically. Automation replaces runbooks where possible.	Runbook completeness is measured. Gaps are tracked. Runbooks are tested periodically. Automation replaces runbooks where possible.
5 - Optimised	Runbooks are comprehensive and integrated with tooling. AI governance playbooks cover model review, incident response, and regulatory examination. Runbooks are continuously improved.	Runbooks are comprehensive and integrated with tooling. AI governance playbooks cover model review, incident response, and regulatory examination. Runbooks are continuously improved.	Runbooks are comprehensive and integrated with tooling. AI governance playbooks cover model review, incident response, and regulatory examination. Runbooks are continuously improved.

D12.5 - Total Cost of Ownership

Measure ID	Measure Name	Governs	Normative References
D12.5	Total Cost of Ownership	Whether the long-term total cost of ownership of the data and AI governance programme is understood, planned, and sustainable.	ISO 8000-8 ISO 42001 Clause 6
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	TCO is not considered. Governance costs are unplanned.	TCO is not considered. Governance costs are unplanned.	TCO is not considered. Governance costs are unplanned.
1 - Ad Hoc	TCO is estimated informally. No forward planning.	TCO is estimated informally. No forward planning.	TCO is estimated informally. No forward planning.
2 - Repeatable	TCO is estimated for major components. AI governance TCO is not addressed.	TCO is estimated for major components. AI governance TCO is not addressed.	TCO is estimated for major components. AI governance TCO is not addressed.
3 - Defined	TCO is formally assessed for the governance programme including tooling, resources, and AI governance. Sustainability is confirmed.	TCO is formally assessed for the governance programme including tooling, resources, and AI governance. Sustainability is confirmed.	TCO is formally assessed for the governance programme including tooling, resources, and AI governance. Sustainability is confirmed.
4 - Managed	TCO is tracked against forecast. Variances are investigated. TCO informs investment prioritisation.	TCO is tracked against forecast. Variances are investigated. TCO informs investment prioritisation.	TCO is tracked against forecast. Variances are investigated. TCO informs investment prioritisation.
5 - Optimised	TCO is a standing governance agenda item. Long-term sustainability is formally assessed. AI governance TCO is tracked separately as AI adoption grows.	TCO is a standing governance agenda item. Long-term sustainability is formally assessed. AI governance TCO is tracked separately as AI adoption grows.	TCO is a standing governance agenda item. Long-term sustainability is formally assessed. AI governance TCO is tracked separately as AI adoption grows.

D12.6 - Version Control

Measure ID	Measure Name	Governs	Normative References
D12.6	Version Control	Whether configurations, schemas, transformation logic, governance rules, and AI model artefacts are version-controlled.	ISO 8000-8 Clause 7.5 ISO 42001 Clause 7.5 EU AI Act Art.11
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No version control for data or governance artefacts.	No version control for data or governance artefacts.	No version control for data or governance artefacts.
1 - Ad Hoc	Version control is applied to some code. Data and governance artefacts are excluded.	Version control is applied to some code. Data and governance artefacts are excluded.	Version control is applied to some code. Data and governance artefacts are excluded.
2 - Repeatable	Version control is applied to data pipeline code. Schema and governance rules are not consistently covered.	Version control is applied to data pipeline code. Schema and governance rules are not consistently covered.	Version control is applied to data pipeline code. Schema and governance rules are not consistently covered.
3 - Defined	Version control covers all critical data pipeline code, schemas, transformation logic, and AI model artefacts. A branching strategy exists.	Version control covers all critical data pipeline code, schemas, transformation logic, and AI model artefacts. A branching strategy exists.	Version control covers all critical data pipeline code, schemas, transformation logic, and AI model artefacts. A branching strategy exists.
4 - Managed	Version control is enforced through CI/CD processes. All changes are tracked. Rollback is possible for critical artefacts.	Version control is enforced through CI/CD processes. All changes are tracked. Rollback is possible for critical artefacts.	Version control is enforced through CI/CD processes. All changes are tracked. Rollback is possible for critical artefacts.
5 - Optimised	Version control is comprehensive and automated. All data and governance artefacts are version-controlled. AI model versions are linked to training data versions in the provenance record.	Version control is comprehensive and automated. All data and governance artefacts are version-controlled. AI model versions are linked to training data versions in the provenance record.	Version control is comprehensive and automated. All data and governance artefacts are version-controlled. AI model versions are linked to training data versions in the provenance record.

D12.7 - Knowledge Retention

Measure ID	Measure Name	Governs	Normative References
D12.7	Knowledge Retention	Whether processes are in place to prevent critical knowledge loss through staff turnover and to transfer knowledge systematically.	ISO 8000-8 Clause 7 DAMA DMBOK Ch.3
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No knowledge management. Critical knowledge resides with individuals.	No knowledge management. Critical knowledge resides with individuals.	No knowledge management. Critical knowledge resides with individuals.
1 - Ad Hoc	Knowledge retention is discussed when staff leave. No proactive programme.	Knowledge retention is discussed when staff leave. No proactive programme.	Knowledge retention is discussed when staff leave. No proactive programme.
2 - Repeatable	Key person dependencies are identified. Some documentation exists as mitigation.	Key person dependencies are identified. Some documentation exists as mitigation.	Key person dependencies are identified. Some documentation exists as mitigation.
3 - Defined	A formal knowledge management programme identifies key person risks and mitigates them through documentation, cross-training, and succession planning.	A formal knowledge management programme identifies key person risks and mitigates them through documentation, cross-training, and succession planning.	A formal knowledge management programme identifies key person risks and mitigates them through documentation, cross-training, and succession planning.
4 - Managed	Knowledge retention is continuously managed. Key person risk is a governance metric. Cross-training is systematic.	Knowledge retention is continuously managed. Key person risk is a governance metric. Cross-training is systematic.	Knowledge retention is continuously managed. Key person risk is a governance metric. Cross-training is systematic.
5 - Optimised	Knowledge management is embedded in governance. No critical single points of knowledge failure exist. Knowledge transfer is a standard element of role transitions.	Knowledge management is embedded in governance. No critical single points of knowledge failure exist. Knowledge transfer is a standard element of role transitions.	Knowledge management is embedded in governance. No critical single points of knowledge failure exist. Knowledge transfer is a standard element of role transitions.

D12.8 - Continuous Improvement

Measure ID	Measure Name	Governs	Normative References
D12.8	Continuous Improvement	Whether a formal mechanism exists to capture lessons learned from governance activity and drive systematic improvement.	ISO 8000-8 Clause 10 ISO 42001 Clause 10
MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS	MATURITY LEVEL DESCRIPTORS
0 - Non-Existent	No improvement mechanism. Problems recur without resolution.	No improvement mechanism. Problems recur without resolution.	No improvement mechanism. Problems recur without resolution.
1 - Ad Hoc	Improvement is discussed informally after incidents.	Improvement is discussed informally after incidents.	Improvement is discussed informally after incidents.
2 - Repeatable	Retrospectives occur for major projects. Lessons are not systematically applied.	Retrospectives occur for major projects. Lessons are not systematically applied.	Retrospectives occur for major projects. Lessons are not systematically applied.
3 - Defined	A formal lessons-learned process is applied to all significant governance activities. Lessons are recorded and tracked to action.	A formal lessons-learned process is applied to all significant governance activities. Lessons are recorded and tracked to action.	A formal lessons-learned process is applied to all significant governance activities. Lessons are recorded and tracked to action.
4 - Managed	Improvement actions are prioritised and tracked. Progress is reviewed. Recurring issues trigger systemic remediation.	Improvement actions are prioritised and tracked. Progress is reviewed. Recurring issues trigger systemic remediation.	Improvement actions are prioritised and tracked. Progress is reviewed. Recurring issues trigger systemic remediation.
5 - Optimised	Continuous improvement is embedded in governance culture. Improvement metrics are tracked and reported. The DQI Standard review cycle incorporates lessons from assessment activity.	Continuous improvement is embedded in governance culture. Improvement metrics are tracked and reported. The DQI Standard review cycle incorporates lessons from assessment activity.	Continuous improvement is embedded in governance culture. Improvement metrics are tracked and reported. The DQI Standard review cycle incorporates lessons from assessment activity.

Annex A - ISO 8000 Alignment Matrix

The following table maps each DQI domain to the relevant clauses and parts of the ISO 8000 data quality standards family.

DQI Domain	Primary ISO 8000 Reference	Alignment Notes
D1 - Data Value & Alignment	ISO 8000-8 Clause 4 (context)	Alignment of data quality activity to organisational context and objectives.
D2 - Data Ownership & Stewardship	ISO 8000-8 Clause 5 (leadership)	Accountability and ownership of data assets.
D3 - Core Data Quality	ISO 8000-8 Clauses 6-8; ISO 8000-61	Core data quality dimensions and quality management operations.
D4 - Pipeline Quality & Operations	ISO 8000-61 (process reference model)	Data quality management process operations including monitoring and control.
D5 - AI Readiness & Provenance	ISO 8000-110 (provenance); ISO 8000-61	Data provenance for AI training; quality management applied to AI data.
D6 - Governance & Compliance	ISO 8000-8 Clauses 4-10	Full governance framework including policy, metadata, and compliance.
D7 - Security & Privacy	ISO 8000-8 Clause 5 (context requirements)	Security controls supporting data quality governance.
D8 - Tooling & Technology	ISO 8000-61 (operational processes)	Technology enablement of data quality management processes.
D9 - Transparency & Access	ISO 8000-8 Clause 7 (support)	Data discoverability, visibility, and access governance.
D10 - Lifecycle & Retention	ISO 8000-8 Clause 7.5 (documented information)	Data lifecycle governance including retention and deletion.
D11 - Organisational Readiness	ISO 8000-8 Clause 7 (competence, awareness)	Organisational capability and culture for data quality governance.
D12 - Sustainable & Maintainable	ISO 8000-8 Clauses 7.5, 10 (improvement)	Documentation, knowledge management, and continuous improvement.

Annex B - ISO/IEC 42001 Alignment Matrix

The following table maps DQI domains and selected measures to clauses of ISO/IEC 42001:2023 (Artificial Intelligence Management System).

ISO 42001 Clause	Clause Title	Primary DQI Alignment
Clause 4	Context of the organisation	D1 (Strategic Alignment, Use Case Linkage), D2 (Executive Sponsorship)
Clause 5	Leadership	D2 (Formalised Roles, Executive Sponsorship, Cross-Functional Council)
Clause 6	Planning	D11 (Governance Maturity Roadmap), D1 (Impact Assessment)
Clause 7	Support	D11 (Data Literacy, AI Literacy, Training Programme), D12 (Documentation)
Clause 7.5	Documented information	D12 (Documentation, Version Control, Runbooks), D10 (Lifecycle Audit Trail)
Clause 8	Operation	D5 (all measures), D4 (Pipeline Quality), D7 (Privacy by Design, AI Security)
Clause 8.4	AI system development	D5.1-D5.12 (full domain alignment), D3.12 (Fitness for Purpose)
Clause 8.5	AI system deployment	D5.6 (Input Validation), D9.7 (AI Output Transparency)
Clause 9	Performance evaluation	D2.4 (Performance Metrics), D4.3 (Monitoring), D11.10 (Benchmarking)
Clause 9.3	Management review	D11.9 (Governance Maturity Roadmap), D6.4 (Regulatory Compliance)
Clause 10	Improvement	D6.7 (Quality Issue Management), D12.8 (Continuous Improvement)

Annex C - EU AI Act Alignment Matrix

The following table maps key EU AI Act articles to the DQI measures that support compliance with those obligations. This alignment is indicative. Organisations should obtain qualified legal advice on their specific EU AI Act obligations.

EU AI Act Article	Subject	Primary DQI Measure Alignment
Article 4	AI Literacy	D11.2 (AI Literacy), D11.4 (Training Programme)
Article 6	Classification of high-risk AI systems	D6.5 (EU AI Act Alignment) - risk classification activity
Article 9	Risk management system	D5.12 (AI Readiness Gate), D6.1 (Policy Framework), D1.6 (Impact Assessment)
Article 10	Data and data governance	D5.1-D5.3 (Provenance, Quality, Bias), D3.1-D3.12 (Core Data Quality)
Article 11	Technical documentation	D12.1 (Documentation), D5.1 (Training Data Provenance), D5.5 (Feature Engineering)
Article 12	Record-keeping	D5.8 (Model-Data Traceability), D3.11 (Auditability), D10.8 (Lifecycle Audit Trail)
Article 13	Transparency and provision of information	D9.7 (AI Output Transparency), D9.1 (Data Discoverability)
Article 15	Accuracy, robustness, and cybersecurity	D7.1-D7.10 (Security & Privacy domain), D5.7 (Drift Detection)
Article 17	Quality management system	D6.1 (Policy Framework), D6.7 (Quality Issue Management), D12.8 (Continuous Improvement)
Article 25	Obligations of distributors	D7.10 (Third-Party Security), D6.9 (Third-Party Data Governance)
Article 52	Transparency obligations for certain AI systems	D9.7 (AI Output Transparency)

Annex D - GDPR Alignment Matrix

The following table maps key GDPR articles to the DQI measures that support compliance. UK GDPR alignment follows the same structure. This alignment is indicative and does not constitute legal advice.

GDPR Article	Subject	Primary DQI Measure Alignment
Article 5(1)(a)	Lawfulness, fairness, and transparency	D9.7 (AI Output Transparency), D6.1 (Policy Framework)
Article 5(1)(c)	Data minimisation	D10.7 (Data Minimisation), D3.6 (Uniqueness)
Article 5(1)(d)	Accuracy	D3.1 (Accuracy), D3.2 (Completeness)
Article 5(1)(e)	Storage limitation	D10.1 (Retention Policy), D10.6 (Regulatory Retention Alignment)
Article 5(2)	Accountability	D2.2 (Accountability Mapping), D6.10 (Governance Audit Trail)
Article 17	Right to erasure	D10.3 (Deletion & Right to Erasure)
Article 22	Automated individual decision-making	D9.7 (AI Output Transparency), D5.10 (Consent & Personal Data Provenance)
Article 24	Responsibility of the controller	D2.5 (Executive Sponsorship), D6.1 (Policy Framework)
Article 25	Data protection by design and by default	D7.8 (Privacy by Design)
Article 28	Processor obligations	D7.10 (Third-Party Security), D6.9 (Third-Party Data Governance)
Article 30	Records of processing activities	D6.10 (Governance Audit Trail), D10.8 (Lifecycle Audit Trail)
Article 32	Security of processing	D7.1-D7.3 (Encryption, Access Controls, Audit Logging)
Article 33	Notification of breach	D7.5 (Breach Response)
Article 35	Data protection impact assessment	D7.8 (Privacy by Design)

This Standard is published by Q4IT. All rights reserved. Reproduction for internal use by licensed DQI practitioners is permitted. Commercial reproduction requires written consent from Q4IT.

info@q4it.eu | www.q4it.eu | Q4IT GBR | Q4IT Canada | Q4IT Czech Republic