Generic Data Governance Policy Framework

A modular, decision-driven template — core essentials plus optional extensions, built to adapt to your organization's context.

Consumer Data Domain – Data Governance Project

Grounded in DAMA-DMBOK2, DCAM, and ISO 8000, and informed by a structured benchmark review of 17 published data governance policies and frameworks (Appendix B), plus the author's own AI Governance and Data Governance practice playbooks.

Prepared: 5 August 2026

Preamble — Four Ways to Approach Data Governance

Before defining a single role or policy, an organization has to decide how it wants to govern in the first place. Four recognizable approaches recur across the benchmark reviewed for this framework (Appendix B) and across the wider governance literature. Most organizations are not a pure example of one — they blend two, and the blend shifts as the program matures. Naming the starting point deliberately, rather than defaulting to it by accident, is the first decision this framework asks you to make. The self-assessment questionnaire referenced at the end of this preamble is designed to help make that choice explicit.

The Four Approaches

Command-and-Control. Roles and rules are created at the top of the organization; managers and supervisors are assigned to delegate and enforce each data task. Governance is imposed, not negotiated.

Formalized. A comprehensive, systematic program: documented roles, training curricula, performance reviews, and a full policy/standard/guideline/procedure stack. Governance is built, not discovered.

Non-Invasive. Existing roles and responsibilities are identified and formalized for governance purposes, rather than new positions being created. Governance recognizes, rather than reorganizes (Robert Seiner's Non-Invasive Data Governance).

Adaptive. A flexible approach that integrates governance practice into daily work as it becomes useful, and evolves the operating model as needs change. Governance is iterated, not fixed.

These four are not mutually exclusive: an organization commonly runs Command-and-Control for regulatory-critical domains while running Non-Invasive or Adaptive for lower-risk ones. The point of naming them is to make that mix a deliberate design choice, not a default.

Comparative View

	Command-and-Control	Formalized	Non-Invasive	Adaptive
Governance model	Centralized, top-down	Structured, systematic	Recognizes existing structure	Iterative, evolving
Enforcement style	Directive, audited	Procedural, documented	Collaborative, light-touch	Contextual, negotiated
Speed to first result	Fast to mandate, slow to adopt	Slow — significant upfront build	Fast — reuses what exists	Fast, in small increments
Documentation weight	Rules communicated, not co-authored	Exhaustive (policy → procedure)	Minimal — reflects current practice	Living documents, updated per sprint

	Command-and-Control	Formalized	Non-Invasive	Adaptive
Main risk	Low field buy-in, seen as policing	Upfront cost; risk of "shelf-ware"	Enforcement can lack teeth	Harder to audit; inconsistency across domains
Aligned named frameworks	COBIT; EDM Council DCAM (regulated/audit contexts)	DAMA-DMBOK2 (11 knowledge areas); DGI Framework (10 components)	Non-Invasive Data Governance (Seiner); McKinsey 3-tier DMO model	Agile Data Governance movement
Best suited when	Heavy regulatory exposure; audit-critical; low trust requiring firm control	Building a data management program from scratch; need a shared vocabulary across a large or complex org	Governance maturity is low; need quick wins; culture resists top-down mandates	Fast-changing environment (e.g. AI/ML); scaling domain by domain; continuous adaptation required
Observed in benchmark	Institutional/government policies (Oklahoma, UNLV, McGill, New Hampshire, UNSW)	DAMA-referencing policies (Oklahoma); DGI Framework; comprehensive vendor guides (Profisee)	Author's Data Governance Brochure; Seiner-referencing guidance (Twilio)	Author's AI Governance Framework; Agile-rollout guidance (Section 6)

Where DCAM, COBIT, and DAMA-DMBOK2 fit

This framework does not ask you to choose one named methodology over another — it asks you to choose an approach (above), then borrow the named framework that fits it. If your context is regulated and audit-critical, EDM Council's DCAM (a capability maturity model widely used in financial services) or COBIT (IT controls and audit alignment) pair naturally with a Command-and-Control or Formalized approach. If you are building a data management capability from scratch and need a shared vocabulary, DAMA-DMBOK2's eleven knowledge areas (Appendix A) or the DGI Framework's ten components pair with Formalized. Where data quality specifically is in scope, ISO 8000 provides a vendor-neutral standard for data quality and exchange, applicable regardless of which of the four approaches you choose (Section 3.4).

Finding Your Organization's Profile

A 20-question self-assessment questionnaire accompanies this framework (distributed separately as a short survey). Each question offers four answers, one aligned to each approach above; tallying the responses produces a profile — typically a dominant approach and a secondary one — rather than a single fixed label, in the same spirit as a behavioral-style assessment. Use the result as a starting point for Section 0's Decision Checklist, not as a verdict: the profile describes where the organization tends to sit today, and the framework is designed to accommodate a deliberate shift over time (Section 8).

0. How to Use This Framework

This document is not a policy to adopt as-is. It is a modular template with two layers:

- CORE — the elements that appeared in the large majority of the 17 benchmark policies reviewed (Appendix B) and that DAMA-DMBOK2 treats as foundational. Define these regardless of your organization's size, sector, or maturity.
- EXTENSIONS — optional modules to activate based on decisions specific to your situation: regulatory exposure, data sensitivity, organizational maturity, whether AI/ML is in scope, or whether data spans multiple entities or countries.

Work through the decision checklist below before you start drafting — it tells you which extensions to activate. Treat the resulting policy as a lifecycle, not a one-time launch: revisit the checklist and the policy itself at least annually (Section 8).

Decision Checklist

Question	If yes → activate / strengthen
Are you subject to sector-specific or multi-jurisdiction regulation (e.g. GDPR, sector laws)?	Strengthen Legal, Regulatory & Compliance (3.1); activate Data Sharing & Third-Party (5.3)
Do you use, or plan to use, AI/ML systems — including AI embedded in SaaS tools?	Activate the AI Governance Extension (5.6)
Do multiple business units, brands, or countries share the same data domains?	Activate Master & Reference Data (5.2); strengthen Data Access & Classification (3.2)
Is this a first-time governance program, or is organizational maturity low?	Start with Core only (Sections 2–4); defer extensions to later sprints (Section 8)
Do you already operate, or plan to operate, a data catalog or metadata tool?	Activate Metadata & Data Catalog (5.1)
Is data volume, criticality, or external scrutiny high enough to warrant formal risk scoring?	Activate Risk Management (5.5)
Are data and records/information management already converged under one function?	Activate Records & Information Governance convergence (5.7)

1. Guiding Principles

Five principles observed across the strongest benchmark policies and consistent with the Agile Data Governance movement (minimum viable policy over upfront documentation, decentralized stewardship, a shift from policing to enabling):

Governance clarifies; it rarely invents. Map the people who already do data work before drawing an org chart. Most organizations already have an informal 80/20 owner and steward pattern — governance recognizes and structures it rather than imposing a new system on top.

Be non-invasive by default. Following Robert Seiner's Non-Invasive Data Governance approach: formalize existing accountability first; add new roles or committees only where a genuine gap exists.

Bottom-up, or it doesn't stick. A top-down mandate dropped on a busy team creates friction, not compliance. Start with the Sponsor and Data/Business Owner conversations (Section 8, Step 0) before writing policy.

Policy cascades; it doesn't dictate. A Policy states intent. Standards, Guidelines, and Procedures carry the operational detail (Section 4). Keep the Policy layer short and stable; let the lower layers absorb day-to-day change.

Treat it as a lifecycle, not a launch. Every policy domain, role, and RACI assignment should be reviewed on a fixed cadence (at minimum annually) and re-scoped when the business, technology, or regulatory context changes (Section 8, Step 5).

2. Essential — Governance Roles & Responsibilities

Explicit roles and responsibilities appeared in 15 of the 17 benchmark documents reviewed (88%), and role/committee structures of some kind in 16 of 17 (94%) — see Appendix B. This is the single most consistent element across every framework examined, and it is the starting point DAMA-DMBOK2 and DCAM both require before any policy content is drafted.

2.1 Core Role List

Role	Accountable for	Typical reporting line	Layer
Executive Sponsor	Champions the program, secures funding and mandate, resolves cross-functional escalations.	CEO / Board	Core
Data Governance Council / Committee	Approves policy, arbitrates cross-domain conflicts, sets risk appetite.	Executive Sponsor	Core
Chief Data Officer / Data Governance Lead	Runs the program day-to-day, coordinates stewards, tracks KPIs.	CIO, CEO, or Governance Council	Core
Data Owner	Accountable for a data domain: approves definitions, standards, and access decisions within it.	Data Governance Council	Core
Data Steward	Carries out day-to-day governance on the Owner's behalf: definitions, standards application, issue resolution.	Data Owner	Core
Data Custodian	Operational responsibility for capture, storage, and technical maintenance of the data.	Data Steward / IT	Core
Data User	Adheres to policy when accessing and using data; first line of quality and misuse reporting.	Business line management	Core
Data Protection Officer / Privacy Officer	Oversees regulatory privacy compliance (e.g. GDPR); advises on legal basis and data subject rights.	Legal / Compliance	Extension — if regulated
Information Security Officer (CISO)	Owns the security control framework that the data security policy inherits.	CIO / Risk	Extension — if standalone security policy
Data Architect	Designs the technical structures (models, catalogs, integration patterns) that operationalize governance.	CDO / CIO	Extension — if formal architecture function exists
AI Owner / Model Steward	Accountable for a specific AI use case; monitors performance, drift, and documentation.	Data Owner (same domain) or AI Governance Board	Extension — if AI Governance activated (5.6)

2.2 Operating Model: A Matrix, Not a Reporting Line

The same accountability chain repeats for every data domain (vertical), while a small number of specialist roles cut across all domains (horizontal). This pattern is consistent between the data governance and AI governance playbooks referenced in this framework — the same matrix logic, reused per use case.

Domain →	Domain A (e.g. Customer)	Domain B (e.g. Product)	Domain C (e.g. Finance)	Cross-cutting owner
Data Owner	[Name / role]	[Name / role]	[Name / role]	→ Compliance Owner
Data Steward	[Name / role]	[Name / role]	[Name / role]	→ Data Quality Owner
Data Custodian / Tech	[Name / role]	[Name / role]	[Name / role]	→ Data Security Owner

Cross-functional designers who support every cell of the matrix without owning a domain: Data Architect, Platform Administrator, Database Administrator, Data Engineer, Software Engineer, Legal/DPO, Security Architect.

2.3 RACI

Build one RACI matrix per major governance task (e.g. Develop Strategy, Define Standards, Implement Policy, Monitor Compliance), assigning Responsible, Accountable, Consulted, and Informed across the roles in 2.1. Two ready-to-adapt RACI templates — one by governance body, one by individual role — are available in the project's Reference Material library and can be reused directly.

3. Essential — Policies to Define

The five domains below are the ones the user brief specifically called out, and independently the ones that recur most often across the 17 benchmark documents reviewed (Appendix B). Define all five for every organization; the "minimum content" column is the floor, not the ceiling.

3.1 Legal, Regulatory & Compliance Policy — Benchmark: 17 / 17 — 100%

- State the legal basis for processing each data category (e.g. GDPR Art. 6/9).
- Map applicable sector, national, and cross-border regulation.
- Define escalation path to Legal/DPO for new processing activities.
- Reference related policies: Data Protection, Records Retention, IT Acceptable Use.

Typical owner: Data Governance Council, with DPO/Legal

Template clause: *"[Organization] processes personal and business data only where a documented legal basis exists, and reviews that basis whenever the purpose of processing changes."*

3.2 Data Access & Classification Policy — Benchmark: 16 / 17 — 94%

- Define a sensitivity/classification scheme (e.g. Public, Internal, Confidential, Restricted).
- Set access-approval workflow and least-privilege principle.
- Require access reviews on a fixed cadence.
- Define handling requirements per classification tier.

Typical owner: Data Owner, implemented by Data Custodian/IT

Template clause: *"[Organization] classifies all data assets into no fewer than [N] sensitivity tiers, each with defined access, handling, and disclosure requirements."*

3.3 Data Life Cycle & Retention Policy — Benchmark: 16 / 17 — 94%

- Define stages: creation/capture, use, archival, disposal.
- Set retention periods per data category, tied to legal/regulatory minimums.
- Define secure disposal/deletion method and evidence requirement.
- Address data migration and legacy system sunset handling.

Typical owner: Data Owner, with Legal and Records Management

Template clause: *"[Organization] retains data only for as long as necessary to fulfil the purpose for which it was collected or a defined legal obligation, and disposes of it securely thereafter."*

3.4 Data Quality Policy — Benchmark: 15 / 17 — 88%

- Define quality dimensions in scope (accuracy, completeness, consistency, timeliness, validity).
- Set minimum quality thresholds/KPIs per critical data element.
- Define issue-logging and remediation workflow.
- Assign quality monitoring cadence and reporting to the Governance Council.

Typical owner: Data Steward, accountable to Data Owner

Template clause: *"[Organization] measures and reports data quality for all critical data elements against defined thresholds no less often than [quarterly], and logs and remediates exceptions through a documented workflow."*

Standards alignment: ISO 8000 provides a vendor-neutral standard for data quality and data exchange and can be cited here as the measurable basis for quality thresholds, independent of which of the four governance approaches (Preamble) the organization follows.

3.5 Data Security Policy — Benchmark: 10 / 17 explicit standalone — 59% (frequently folded into Access & Classification in the remaining benchmarks)

- Define baseline technical/organizational controls (encryption, authentication, logging).
- Define incident detection and breach-notification workflow and timelines.
- Reference vulnerability management and third-party security requirements.
- Recommended as a standalone policy where regulatory exposure or data sensitivity is high; otherwise can remain a sub-section of 3.2.

Typical owner: CISO / Information Security, with Data Owner

Template clause: *"[Organization] applies security controls proportionate to each data classification tier and notifies [DPO/regulator] of a confirmed personal data breach within [72] hours of becoming aware of it."*

4. Policy Hierarchy Convention

Keep the Policy layer short and stable; let Standards, Guidelines, and Procedures absorb operational change. This cascade — rather than a single monolithic document — is what lets the framework adapt without rewriting governance from scratch each time something changes.

Level	What it must define	Typical owner
Policy	What must be true, and why. Rarely changes.	Data Governance Council
Standard	What "good" looks like — the measurable requirement derived from policy.	Data Owner
Guideline	Recommended practice for meeting a standard — the "how," offered as guidance rather than mandated.	Data Steward
Procedure	Step-by-step instructions for day-to-day compliance with the standard.	Data Custodian / operational team

5. Optional — Extension Modules

Activate a module when the Decision Checklist (Section 0) points to it. Each module is designed to plug into the same role structure (Section 2) and hierarchy convention (Section 4) as the core.

Module	Activate if…	Benchmark frequency
5.1 Metadata & Data Catalog	You operate, or plan to operate, a data catalog or need a shared business glossary.	12 / 17 — 71%
5.2 Master & Reference Data	Multiple business units or systems share the same core entities (customer, product, vendor, chart of accounts).	6 / 17 — 35%
5.3 Data Sharing & Third-Party / External Exchange	Data is shared with external partners, vendors, or across legal entities.	6 / 17 — 35%
5.4 Training & Awareness	Near-universal good practice; formalize if adoption or audit findings show gaps. Recommended even outside strict "core."	12 / 17 — 71%
5.5 Risk Management	Data volume, criticality, or external scrutiny justifies formal risk scoring and a risk register.	8 / 17 — 47%
5.6 AI Governance Extension	AI/ML systems are in use or planned, including AI embedded in SaaS tools ("shadow AI"). See detail below — the EU AI Act creates binding obligations for many high-risk use cases.	Emerging — 1 / 17 explicit; addressed separately in the author's AI Governance Framework
5.7 Records & Information Governance convergence	Data governance and records/information management are combined under one function or one policy umbrella.	Observed in benchmark (e.g. UNSW model)

5.6 detail — AI Governance Extension

Where AI/ML is in scope, reuse the same governance discipline built for data — extended, not replaced — following the five-step continuous loop below (adapted from the author's AI Governance Framework):

1. Inventory & Evaluate — build a complete AI inventory (vendor/SaaS tools with embedded AI, internally built models, and "shadow AI"); you cannot govern what you haven't found.
2. Classify the Risk — grade against a fixed, graduated scale. The EU AI Act uses four tiers: Unacceptable (prohibited) → High-Risk (regulated, e.g. credit scoring, recruitment, biometric categorisation) → Limited Risk (transparency obligations only) → Minimal Risk (no additional requirements). Governance effort scales with the tier.
3. Define Policy & Owners — reuse the data matrix (Section 2.2) per AI use case: AI Owner (accountable), Model Steward (monitoring, documentation, drift), Technical Delegation (implementation). An AI Governance Board sets risk appetite and approval gates.
4. Document Every Application — one file per AI system, covering: Purpose & Legal Basis, Risk & Impact Assessment, Human Oversight, Training Data, Security Assessment, and Monitoring & Change Log.
5. Monitor & Reassess — this is a loop, not a launch: step 5 always feeds back into step 1, since AI systems continue to change after go-live in a way most data assets do not.

Legal grounding: Regulation (EU) 2024/1689 (the EU AI Act) is the binding reference where the organization has EU exposure; the full text (EN/FR) and an EPRS explanatory briefing are held in the project's Reference Material library, alongside the OECD and UNESCO AI principles for non-binding ethical grounding.

6. Governance Lifecycle — Agile Operating Rhythm

Run governance as a continuous loop, not a one-off documentation exercise:

Step	Action
1. Inventory & Evaluate	Find every data domain/system in use — vendor, embedded, or internally built — before governing it.
2. Classify	Grade against fixed criteria: sensitivity, risk, regulatory exposure.
3. Define Policy & Owners	Assign who decides at each level (Section 2) and which policy domains apply (Sections 3–5).
4. Document	One record per domain/system: purpose, quality standard, access rule, retention plan, security assessment.
5. Monitor & Reassess	Re-enter the loop whenever the domain, model, or use changes — this always feeds back into Step 1.

Agile rollout cadence

Train, then trust → equip people, then hand over real responsibility, not a checklist. Monthly reachable goals → not a two-year roadmap. Sprints, concrete deliverables → one or two finished things: a definition, a standard, a process. One-page sprint summary → ten minutes to build, makes the team's work visible to everyone. This lines up with the wider Agile Data Governance movement: minimum viable policies over upfront documentation, decentralized stewardship, and a shift from policing to enabling.

7. Documentation Templates

7.1 One-Page Policy Template

Use this structure for every individual policy produced from Section 3 or Section 5.

Field	Content
Policy name	[Name]
Owner	[Role — Section 2.1]
Effective date / next review	[Date] / [Date, ≤ 12 months later]
Purpose & scope	[What this policy governs, and what it explicitly excludes]
Definitions	[Key terms — see Glossary, Section 10, for the shared baseline]
Roles referenced	[Roles from Section 2.1 relevant to this policy]
Policy statements	[Numbered, testable statements — see template clauses in Section 3]
Related standards / guidelines / procedures	[Links — Section 4 hierarchy]
Enforcement & exceptions	[Consequence of non-compliance; exception approval path]

7.2 One-File-Per-Domain (or System) Template

Generalized from the AI Governance Framework's "one file per AI system" approach — the same six-section structure works for any data domain or system of record:

Section	What it covers
Purpose & legal basis	What the domain/system is for, who owns it, and the legal ground it relies on.
Quality & risk assessment	Applicable quality thresholds (3.4) and, where relevant, risk/impact classification (5.5, 5.6).
Access & classification	Sensitivity tier and access rules (3.2).
Life cycle & retention plan	Stages and retention period (3.3).
Security assessment	Controls applied, proportionate to classification (3.5).
Monitoring & change log	Ongoing checks and a record of material changes to data, scope, or use.

8. Adoption Roadmap

Step	Action
0. Two conversations first	Sponsor Conversation (why more governance, what does success look like) and Data/Business Owner Conversation (how the data organization actually works today) — before any framework is imposed.
1. Ship the Core only	Draft and approve the five essential policies (Section 3) and name the core roles (Section 2.1) for one pilot domain. Resist the urge to activate every extension on day one.
2. Name the owners	Populate the matrix (Section 2.2) for the pilot domain. One role per concern, one loop for all of them: the Owner sits down with the Steward, agrees the standard, surfaces friction, iterates.
3. Run sprints	Monthly reachable goals; one or two finished deliverables per sprint; a one-page summary each time (Section 6).
4. Scale domain by domain	Replicate the matrix for the next domain; activate extension modules (Section 5) only where the Decision Checklist (Section 0) indicates a real trigger.
5. Review annually	Re-run the Decision Checklist, refresh the RACI, and re-certify each policy's "next review" date (7.1). Treat the whole framework as a lifecycle, not a launch.

9. Decision Log / Customization Worksheet

Record every decision made when adapting this generic template to your organization's situation. This is what turns a generic framework into your framework — and gives the next review cycle a starting point.

Decision	Choice made	Rationale	Date / Owner
Extension modules activated (Section 5)	[e.g. 5.1, 5.5, 5.6]	[Link to Decision Checklist answers]	[ ]
Data classification tiers used (3.2)	[N tiers, names]	[ ]	[ ]
Retention periods by category (3.3)	[ ]	[ ]	[ ]
Quality thresholds / KPIs (3.4)	[ ]	[ ]	[ ]
Risk scoring model, if activated (5.5)	[ ]	[ ]	[ ]
AI risk tiers adopted, if activated (5.6)	[ ]	[ ]	[ ]
Review cadence	[e.g. annual]	[ ]	[ ]

10. Glossary

Term	Definition
Data Governance	The exercise of authority and control over data — setting policy, assigning accountability, ensuring quality, security, and compliance.
Data Governance Council	The senior body that approves policy, arbitrates conflicts between domains, and sponsors governance initiatives.
Data Owner	A business role accountable for a data domain — approves definitions, standards, and access decisions within it.
Data Steward	Carries out day-to-day governance work on the Owner's behalf: definitions, standards application, issue resolution.
Data Custodian	Operational, usually technical, responsibility for the capture, storage, and maintenance of data.
Policy	A high-level statement of what must be true about data — the "what," brief and rarely detailed.
Standard	A measurable requirement derived from policy — what a good outcome looks like, used to judge compliance.
Guideline	Recommended practice for meeting a standard — the "how," offered as guidance rather than mandated.
Procedure	Step-by-step instructions people actually follow, day to day, to comply with the standard.
Data Dictionary	A technical inventory of data elements — names, types, formats, business meaning.
Data Domain	A logical grouping of related data — e.g. Customer, Product, Finance — used to assign ownership and scope.
Master Data / Reference Data	Core shared entities (e.g. customer, product, vendor) or standardized code lists used consistently across systems.
Taxonomy	A hierarchical classification of concepts, parent and child categories, one relationship type.
High-Risk AI System	Under the EU AI Act, an AI system listed in Annex III or subject to Art. 6 full requirements (e.g. credit scoring, recruitment, biometric categorisation).
General-Purpose AI (GPAI)	A model trained at scale, adaptable to many downstream tasks — e.g. a foundation model.
Human Oversight	The design and operational ability for a person to understand, monitor, and — when needed — override an AI system's output.
Model Drift	The gradual decline in a model's accuracy as real-world data shifts away from what it was trained on.
Fundamental Rights Impact Assessment (FRIA)	A required assessment of how a high-risk AI deployment affects the people subject to it, under EU AI Act Art. 27.

Appendix A — DAMA-DMBOK2 Reference Wheel

This framework sits on top of DAMA-DMBOK2, the industry-standard reference where Data Governance is the discipline that ties together, and sets direction for, every other data management knowledge area:

- Data Architecture, Data Modeling & Design, Data Storage & Operations
- Data Security, Data Quality, Metadata
- Data Integration & Interoperability, Document & Content Management
- Reference & Master Data, Data Warehousing & Business Intelligence

Data Governance sits at the center of the wheel and sets policy, standards, and accountability that each of the surrounding knowledge areas implements.

Appendix B — Benchmark Source Summary

17 published data governance policies and frameworks, held in the project's Reference Material library, were scanned for the presence of 17 recurring themes. Results below; full source register with links, authors, and copyright status is maintained separately in Reference Material Register.docx.

Theme	Present in
Purpose / Scope	17 / 17 — 100%
Legal / Compliance / Privacy	17 / 17 — 100%
Governance Council / Committee	16 / 17 — 94%
Data Access / Classification	16 / 17 — 94%
Data Life Cycle / Retention	16 / 17 — 94%
Definitions / Glossary	15 / 17 — 88%
Roles & Responsibilities (explicit section)	15 / 17 — 88%
Data Quality	15 / 17 — 88%
Standards / Guidelines / Procedures hierarchy	15 / 17 — 88%
Metadata / Data Dictionary / Catalog	12 / 17 — 71%
Training / Awareness	12 / 17 — 71%
Enforcement / Exceptions	11 / 17 — 65%
Data Security (standalone)	10 / 17 — 59%
Risk Management	8 / 17 — 47%
Master / Reference Data	6 / 17 — 35%
Data Sharing / Third-Party	6 / 17 — 35%
AI / Emerging Tech	1 / 17 — 6% (emerging — see Section 5.6)

Sources scanned: Oklahoma OMES, UNLV, UK Higher-Ed College policy, FHWA Data Governance Plan Vol. 1, New Hampshire DOE, UNSW, McGill University, Textile Exchange, Atlan, Laco, Profisee (11 published policy examples); DGI Framework, OvalEdge, Sprinto, Twilio framework guides (4 framework guides); plus the author's own Data Governance Brochure and AI Governance Framework playbooks used for structure and tone.