Data Governance and Protection Strategy Training Course

7 – 11 December 2026
Madrid

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Data Governance and Protection Strategy Training Course

Ref: 807_172213 **Date:** 7 – 11 December 2026 **Location:** Madrid **Fees:** 5700 Euro

Overview

Data Governance and Protection Strategy Training Course is a one-week professional course for governance, privacy, compliance, security, data ownership, and assurance functions who leave with a Data Governance and Protection Strategy Pack. Participants connect the governance operating model, decision rights, data ownership and stewardship, data classification, integrity controls, privacy risk, compliance mapping, policy architecture, accountability, monitoring, incident response, and assurance evidence. The course turns fragmented controls into traceable operating decisions. Agile Leaders Training Center develops data governance and protection strategy capability.

Who Should Attend

- Governance functions responsible for decision rights, policy ownership, oversight forums, and operating-model design
- Data ownership functions responsible for business definitions, access decisions, critical data, and control accountability
- Stewardship functions responsible for metadata, classification, quality issues, lineage, and remediation coordination
- Privacy and compliance functions responsible for requirements, risk mapping, evidence, and control monitoring
- Information security functions responsible for protection measures, incident coordination, and control assurance
- Audit and assurance functions responsible for testing evidence, reporting gaps, and tracking corrective actions

The course assumes participants can map business processes, data assets, and control responsibilities, and leaves out technical data engineering, security-tool configuration, legal advice, and certification preparation.

Departments and Industries

The course supports departments and industries that need accountable use, integrity, privacy, and protection of enterprise data.

- Data offices, governance, risk, compliance, privacy, information security, audit, and legal departments
- Banking, insurance, financial services, and professional services
- Healthcare, education, research, and public-service organizations
- Manufacturing, energy, utilities, logistics, and telecommunications
- Retail, hospitality, digital platforms, and customer-service operations

AGILE LEADERS
Training Center

Learning Objectives

By the end of this course, participants will be able to:

- Build a governance operating model with decision rights and accountable forums
- Apply ownership, stewardship, classification, and critical-data controls
- Analyze privacy, protection, integrity, and compliance risks across data lifecycles
- Map requirements to policies, controls, evidence, and accountable roles
- Evaluate monitoring indicators, incidents, exceptions, and corrective actions
- Build an assurance plan and sequenced implementation roadmap

Course Agenda

Day 1: Frame Data Governance

- Data Governance Mandate and Value-Outcome Map
- Governance Operating Model Canvas
- Decision-Rights and Escalation Matrix
- Data Owner, Steward, and Custodian Accountability Register
- Governance Forum Charter and Issue-Intake Workflow

Day 2: Classify and Control Data

- Enterprise Data Inventory and Lifecycle Map
- Data Classification and Handling Scheme
- Critical Data Element Identification Scorecard
- Data Integrity Control and Validation Matrix
- Metadata, Lineage, and Evidence Traceability Register

Day 3: Map Protection and Compliance

- Privacy Risk and Data-Processing Assessment Worksheet
- Protection Requirement and Control Mapping Table
- Policy Architecture and Standard Hierarchy
- Third-Party Data Sharing and Accountability Checklist
- Requirement-to-Evidence Compliance Traceability Map

Day 4: Monitor and Assure Governance

- Governance Indicator and Control-Effectiveness Dashboard
- Data Issue, Exception, and Remediation Register
- Data Incident Triage and Response Workflow
- Control Testing and Assurance Evidence Plan
- Governance Reporting and Management Review Pack

Day 5: Practice Strategy Design

- Exercise: Diagnose Operating-Model and Decision-Right Gaps
- Exercise: Classify Data and Assign Integrity Controls
- Exercise: Map Privacy and Protection Requirements to Evidence
- Exercise: Evaluate Indicators, Incidents, and Assurance Findings
- Capstone: Data Governance and Protection Strategy Pack

Practical Exercises

The course uses suggested activities based on financial services, healthcare, manufacturing, and digital-service scenarios.

- Suggested activity: map data domains, decision rights, owners, stewards, forums, and escalation routes for a cross-functional process.
- Suggested activity: classify data assets, identify critical elements, and connect integrity and handling controls to lifecycle stages.
- Suggested activity: convert privacy and protection requirements into policies, control owners, evidence, and monitoring indicators.
- Suggested activity: review an incident and assurance finding, prioritize remediation, and build a sequenced implementation roadmap.

FAQs

Who suits data governance and protection strategy training, and what does it assume?

Governance, privacy, compliance, security, data ownership, stewardship, and assurance functions suit the training; it assumes participants can map business processes, data assets, and control responsibilities.

How does data governance and protection strategy differ from general cybersecurity training?

Data governance and protection strategy defines decision rights, accountability, classification, integrity, privacy, policy, evidence, and oversight across the data lifecycle, while general cybersecurity training focuses more broadly on threats, systems, and technical safeguards.

What roles belong in a data governance operating model?

A data governance operating model assigns governing forums, accountable owners, operational stewards, technical custodians, privacy and security advisers, control performers, assurance reviewers, and escalation authorities to defined decisions and evidence.

How should data integrity controls be documented?

Data integrity controls should link critical data elements, validation rules, source and lineage, responsible roles, execution frequency, exceptions, remediation, approvals, and retained evidence in one traceable record.

What evidence supports data governance assurance?

Governance assurance uses approved policies, decision records, ownership registers, inventories, classification evidence, control results, issue logs, incident records, indicators, testing workpapers, corrective actions, and management reviews.

Conclusion

Participants take back a Data Governance and Protection Strategy Pack containing the operating model, accountability registers, classification scheme, integrity controls, risk maps, policy architecture, monitoring dashboard, incident workflow, assurance plan, and roadmap. It changes disconnected governance tasks into a traceable operating system. The pack connects decisions, roles, data, controls, evidence, exceptions, and improvement priorities.