



Information Governance and Records Risk Control Training Course

21 – 25 December 2026
Milan

Information Governance and Records Risk Control Training Course

Ref: 759_157765 **Date:** 21 – 25 December 2026 **Location:** Milan **Fees:** 5700 Euro

Overview

Information Governance and Records Risk Control Training Course is a five-day intermediate course for governance, records, legal, compliance, risk, cybersecurity, and assurance functions who leave with an Information Governance and Records Risk Control Portfolio. Participants connect information ownership, ISO 15489-1:2016 records principles, cyber risk, legal obligations, retention, disposition, access, and evidence traceability. The course turns fragmented controls into coordinated lifecycle decisions and assurance evidence. Agile Leaders Training Center develops information governance and records risk control practice.

Who Should Attend

- Information governance functions responsible for ownership, policy, and lifecycle decisions
- Records functions responsible for capture, classification, retention, access, and disposition
- Legal and compliance functions responsible for obligations, holds, evidence, and assurance
- Cybersecurity governance functions responsible for information risk and protective controls
- Risk and internal assurance functions responsible for control evaluation and reporting

The course assumes participants influence information, records, legal-risk, security, compliance, or assurance decisions, and leaves out system configuration, litigation advice, certification preparation, and technical incident response.

Departments and Industries

The course supports departments and industries that govern information value, obligations, security, and evidence.

- Information governance, records management, legal operations, and compliance
- Cybersecurity governance, enterprise risk, internal audit, and assurance
- Financial services and healthcare
- Energy, industrial operations, and telecommunications
- Public services, education, and professional services

Learning Objectives

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



- Apply ISO 15489-1:2016 principles to records lifecycle decisions
- Analyze information ownership, authority, obligation, and cyber-risk dependencies
- Build classification, retention, access, and disposition controls
- Evaluate legal holds, exceptions, control evidence, and residual risk
- Use cross-functional assurance and issue-escalation methods
- Build an Information Governance and Records Risk Control Portfolio

Course Agenda

Day 1: Establish Information Governance Direction

- ARMA Information Governance Implementation Model Stakeholder Map
- Information Ownership and Accountability Matrix
- Business Context and Information Obligation Register
- Cyber, Legal, Compliance, and Records Dependency Map
- Information Governance Charter and Decision Rights Template

Day 2: Design Records Lifecycle Controls

- ISO 15489-1:2016 Concepts and Principles Review
- Record Creation and Capture Control Checklist
- Metadata, Classification, and File Plan Design
- Retention Schedule and Disposition Authority Matrix
- Records Access, Use, and Transfer Control Map

Day 3: Integrate Cyber and Legal Risk

- Information Asset and Threat Exposure Register
- ISO/IEC 27001:2022 Risk-Control Alignment Worksheet
- Legal Obligation and Records Requirement Traceability Matrix
- Legal Hold, Preservation, and Disposition Suspension Procedure
- Third-Party Information Custody Risk Assessment

Day 4: Assure Controls and Evidence

- Records Control Design and Operating Evidence Catalogue
- Access, Retention, and Disposition Exception Log
- Control Gap, Root Cause, and Remediation Tracker
- Audit Sampling and Evidence Traceability Worksheet
- Cross-Functional Assurance and Escalation Dashboard



Day 5: Practice Governance Decisions

- Exercise: Assign Information Ownership and Decision Rights
- Exercise: Resolve a Retention and Legal Hold Conflict
- Exercise: Evaluate Cyber Risk in a Records Process
- Exercise: Present Control Evidence and Remediation Priorities
- Capstone: Information Governance and Records Risk Control Portfolio

Practical Exercises

The course uses suggested activities based on healthcare, financial services, energy, telecommunications, and professional services.

- Suggested activity: map information owners, records responsibilities, legal obligations, and security dependencies for a business process.
- Suggested activity: challenge a retention and disposition decision affected by a legal hold and cyber exposure.
- Suggested activity: trace a control requirement through policy, process, evidence, exception, and remediation records.
- Suggested activity: present an assurance dashboard and prioritized control treatment plan to cross-functional stakeholders.

FAQs

Who suits information governance and records risk training, and what does it assume?

Governance, records, legal, compliance, risk, cybersecurity, and assurance functions suit the course; it assumes influence over information lifecycle, control, obligation, risk, or evidence decisions.

How does information governance and records risk differ from document control training?

Information governance and records risk coordinates ownership, obligations, lifecycle controls, cyber exposure, and assurance, while document control training focuses more narrowly on document creation, review, approval, versioning, distribution, and retrieval.

How should records retention and disposition decisions be governed?

Records retention and disposition decisions should connect business purpose, documented requirements, ownership, classification, approved authority, legal holds, security risk, exceptions, evidence, and accountable approval.



How does cyber risk affect records controls?

Cyber risk affects records controls through access, integrity, availability, transfer, third-party custody, preservation, and disposal exposures that must be assessed across the information lifecycle.

What evidence supports records risk assurance?

Records risk assurance uses approved policies, ownership records, control designs, capture and access logs, retention authorities, disposition evidence, exception records, sampling results, remediation actions, and traceability to requirements.

Conclusion

Participants take back an Information Governance and Records Risk Control Portfolio connecting ownership, lifecycle controls, cyber exposure, legal obligations, assurance evidence, and remediation. It changes disconnected policies and records activities into coordinated, traceable decisions. The portfolio supports defensible retention, controlled disposition, accountable access, cross-functional assurance, and prioritized treatment of information risk.