Microsoft 365 Information Protection and Compliance Training Course

11 – 15 July 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Microsoft 365 Information Protection and Compliance Training Course

Ref: 1650_221899 **Date:** 11 – 15 July 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Microsoft 365 Information Protection and Compliance Training Course is a one-week professional programme for Microsoft 365, security, compliance, records, privacy, and information-governance administrators, who leave with a Purview Control Deployment Plan. It addresses fragmented protection and compliance settings through data discovery, sensitivity labels, data loss prevention, retention, records, eDiscovery, audit, insider-risk workflows, least-privilege roles, staged testing, monitoring, and governance. Agile Leaders Training Center develops practical Microsoft 365 information protection capability.

Who Should Attend

- Microsoft 365 teams responsible for tenant protection and compliance settings
- Security functions responsible for sensitive-data controls and investigations
- Records teams responsible for retention and disposition processes
- Legal and privacy operations responsible for eDiscovery and case workflows
- Information-governance teams responsible for classifications and ownership
- Assurance teams responsible for audit evidence and control monitoring

The course assumes participants administer Microsoft 365 or related governance processes and leaves out certification preparation, legal advice, and advanced scripting.

Departments and Industries

The course supports organisations that use Microsoft 365 and need controlled, auditable handling of sensitive information.

- Information technology, cloud administration, and digital workplace teams
- Cybersecurity, data protection, privacy, and compliance operations
- Legal, records management, audit, and information governance
- Banking, insurance, professional services, and telecommunications
- Healthcare, education, retail, and manufacturing
- Public, nonprofit, and regulated service organisations

Learning Objectives

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

- Analyze information-protection and compliance requirements
- Build label taxonomies, policies, roles, and deployment controls
- Apply Microsoft Purview sensitivity labels and protection settings
- Use Microsoft Purview data loss prevention and monitoring
- Configure retention, records, audit, and case workflows
- Evaluate testing evidence, alerts, risks, and control performance

Course Agenda

Day 1: Purview Foundations and Governance

- Microsoft Purview Compliance Administration Landscape
- Data Security, Risk, Compliance, and Governance Boundaries
- Licensing, Supported Locations, and Current Documentation
- Role Groups, Least Privilege, and Separation of Duties
- Protection and Compliance Requirements Map

Day 2: Information Protection and Labels

- Data Discovery and Sensitive Information Types
- Microsoft Purview Sensitivity Labels and Taxonomy
- Scopes, Priority, Encryption, and Content Markings
- Label Policies, Defaults, Mandatory and Automatic Labelling
- Pilot, Propagation, User Experience, and Adoption

Day 3: Data Loss Prevention

- Microsoft Purview Data Loss Prevention Architecture
- Locations, Conditions, Exceptions, and Actions
- Policy Tips, Alerts, Incidents, and User Justification
- Endpoint and Collaboration Control Scenarios
- Test Mode, False Positives, Tuning, and Rollout

Day 4: Retention, Records, and Cases

- Retention Policies, Retention Labels, and Adaptive Scope
- Microsoft Purview Records Management and Disposition
- eDiscovery Roles, Cases, Collections, and Review
- Audit Search, Evidence Preservation, and Export Controls
- Insider Risk Principles, Privacy, and Case Handling

AGILE LEADERS
Training Center

Day 5: Operations and Capstone

- Content Explorer, Activity Explorer, Alerts, and Reports
- Control Testing and Operational Acceptance
- Change, Exception, Incident, and Escalation Workflows
- Current-Feature Review and Governance Cadence
- Capstone: Purview Control Deployment Plan

Practical Exercises

Suggested activities turn information-handling requirements into testable administration decisions.

- Suggested activity: design a sensitivity-label taxonomy and publication model
- Suggested activity: build and test a DLP scenario with exceptions and alert handling
- Suggested activity: map retention, record, eDiscovery, and audit responsibilities
- Suggested activity: prepare a staged deployment, monitoring, and governance plan

FAQs

Who should take Microsoft 365 information protection training, and what does it assume?

It suits Microsoft 365, security, compliance, records, privacy, legal-operations, and governance practitioners and assumes working knowledge of tenant administration or information controls, not prior Microsoft certification.

How does Microsoft Purview compliance administration differ from cybersecurity operations?

Purview administration focuses on data classification, protection, retention, records, investigations, audit, and compliance workflows. Cybersecurity operations more broadly address identities, devices, applications, infrastructure, threats, detection, and response.

How should Microsoft Purview sensitivity labels be deployed?

Labels should be based on business meaning and data risk, ordered carefully, assigned suitable scopes and protection actions, published to controlled pilot groups, tested across supported locations, monitored, communicated, and expanded through governed stages.

When should Microsoft Purview data loss prevention use test mode?

Test mode should support evidence gathering before enforcement, allowing administrators to examine matches, user impact, exceptions, false positives, alerts, and process readiness before selecting proportionate restrictive actions.

Does Microsoft 365 information protection training provide Microsoft certification?

No. The course develops practical administration capability and does not provide Microsoft certification, endorsement, examination status, guaranteed compliance, or legal assurance. Product features, licences, and documentation should be verified before deployment.

Conclusion

Participants take back a Purview Control Deployment Plan containing requirements, roles, label taxonomy, DLP scenarios, retention and records decisions, case workflows, audit evidence, pilot controls, monitoring, and governance. It makes protection decisions testable and ownership visible. The plan supports staged deployment while product capabilities, licences, data risks, and organisational needs continue to change.