Administering Information Protection and Compliance in Microsoft 365 – Intensive Training («SC400»)

Learn how to protect information in your Microsoft 365 deployment. This course focuses on data governance and information protection within your organization.

Duration: 3 days
Price: 2'550.–
Course documents: Official Microsoft Courseware and Microsoft Learn
Vendor code: SC-400

Content

The content of this intensive training is derived from the exam «SC-400: Administering Information Protection and Compliance in Microsoft 365». Start preparing for the course on Microsoft Learn now and use the Learning Support if you have any questions. During the intensive training days with the instructor you will work with the official Microsoft course material (more information under «Methodology & didactics»).

Course outline:

Module 1: Implement Information Protection in Microsoft 365
Organizations require information protection solutions to protect their data against theft and accidental loss. Learn how to protect your sensitive information. Learn how Microsoft 365 information protection and governance solutions help you protect and govern your data, throughout its lifecycle – wherever it lives, or wherever it travels. Learn about the information available to help you understand your data landscape and know your data. Learn how to use sensitive information types to support your information protection strategy. Learn about how sensitivity labels are used to classify and protect business data while making sure that user productivity and their ability to collaborate are not hindered.
Lessons:

- Introduction to information protection and governance in Microsoft 365
- Classify data for protection and governance
- Create and manage sensitive information types
- Describe Microsoft 365 encryption
- Deploy message encryption in Office 365
- Configure sensitivity labels
- Apply and manage sensitivity labels

Lab: Implement Information Protection

- Assign permissions for compliance
- Manage Office 365 message encryption
- Manage Sensitive Information Types
- Manage Trainable Classifiers
- Manage Sensitivity Labels

Module 2: Implement Data Loss Prevention (DLP) in Microsoft 365
In this module we discuss how to implement data loss prevention techniques to secure your Microsoft 365 data. Learn how to discover, classify, and protect sensitive and business-critical content throughout its lifecycle across your organization. Learn how to configure and implement data loss prevention policies and integrate them with Microsoft Cloud App Security. Learn how to respond to and mitigate data loss policy violations.
Lessons:

- Prevent Data loss in Microsoft 365
- Implement Endpoint data loss prevention
- Configure DLP policies for Microsoft Cloud App Security and Power Platform
- Manage DLP policies and reports in Microsoft 365

Lab: Implement Data Loss Prevention

- Manage DLP policies
- Mange Endpoint DLP
- Test DLP policies
- Mange DLP reports

Module 3: Implement Information Governance in Microsoft 365
In this module you will learn how to plan and implement information governance strategies for an organization. Learn how to manage your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. Learn how to manage retention for Microsoft 365, and how retention solutions are implemented in the individual Microsoft 365 services. Learn how to use intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business-critical records in your organization.
Lessons:

- Govern information in Microsoft 365
- Manage data retention in Microsoft 365 workloads
- Manage records in Microsoft 365

Lab: Implement Information Governance

- Configure Retention Labels
- Implement Retention Labels
- Configure Service-based Retention
- Use eDiscovery for Recovery
- Configure Records Management

Key Learnings

- Explaining and using sensitivity labels
- Configuring Data Loss Prevention policies
- Securing messages in Office 365
- Describing the information governance configuration process
- Defining key terms associated with Microsoft's information protection and governance solutions
- Explaining the Content explorer and Activity explorer
- Describing how to use sensitive information types and trainable classifiers
- Reviewing and analyzing DLP reports
- Identifying and mitigating DLP policy violations
- Describing the integration of DLP with Microsoft Cloud App Security (MCAS)
- Deploying Endpoint DLP
- Describing records management
- Configuring event driven retention
- Importing a file plan
- Configuring retention policies and labels
- Creating custom keyword dictionaries
- Implementing document fingerprinting

Methodology & didactics

Digicomp Flexible Learning Approach:

- **Training modality:** During a period of 4 weeks, 6-8 half-day (3h each) virtual live sessions with our Azure MCT experts will take place. The sessions are already planned and can be easily combined with the daily work routine. Between the sessions there is enough time to process the learned knowledge.
- **Detailed Session Plan:** Click «**Timetable**» at the bottom of the page where you select your desired date.

Target audience

The Information Protection Administrator plans and implements controls that meet organizational compliance needs. This person is responsible for translating requirements and compliance controls into technical implementation. They assist organizational control owners to become and stay compliant. They work with information technology (IT) personnel, business application owners, human resources, and legal stakeholders to implement technology that supports policies and controls necessary to sufficiently address regulatory requirements for their organization. They also work with the compliance and security leadership such as a Chief Compliance Officer and Security Officer to evaluate the full breadth of associated enterprise risk and partner to develop those policies. This person defines applicable requirements and tests IT processes and operations against those policies and controls. They are responsible for creating policies and rules for content classification, data loss prevention, governance, and protection.

Requirements

- Foundational knowledge of Microsoft security and compliance technologies
- Basic knowledge of information protection concepts
- Understanding of cloud computing concepts
- Understanding of Microsoft 365 products and services

Basic knowledge gained in the following course is recommended:

- Microsoft Security, Compliance, and Identity Fundamentals – Intensive Training («SC900»)
- Microsoft Security, Compliance, and Identity Fundamentals – Flexible Training («SC900V»)

Certification

This intensive training prepares you for:

- **Exam:** «SC-400: Administering Information Protection and Compliance in Microsoft 365» for the
- **Certification:** «Microsoft Certified: Information Protection Administrator Associate»

Additional information

The workshop SC-5003: Implement Information Protection and Data Loss Prevention by Using Microsoft Purview is integrated into this course.

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-digital-transformation-technologies/cloud/cloud-security/course-administering-information-protection-and-compliance-in-microsoft-365-intensive-training-sc-400