Iverson Associates Sdn Bhd (303330-M)
Suite T113 – T114, 3rd Floor, Centrepoint, Lebuh Bandar Utama
Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan
Tel: 03-7726 2678 Fax: 03-7727 9737 Website: www.iverson.com.my

Module Title : MS-500T04-A: Administering Microsoft 365 Built-in Compliance
Duration : 1 day

About this course

nternal policies and external requirements for data retention and investigation may be necessary for your organization. In this course you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. Specifically, this course covers data retention policies and tags, in-place records management for SharePoint, email retention, and how to conduct content searches that support eDiscovery investigations. The course also helps your organization prepare for Global Data Protection Regulation (GDPR).

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and ensures that the solutions comply with the policies and regulations of the organization.

This role proactively secures Microsoft 365 enterprise environments. Responsibilities include responding to threats, implementing, managing and monitoring security and compliance solutions for the Microsoft 365 environment. They respond to incidents, investigations and enforcement of data governance.

The Microsoft 365 Security administrator is familiar with Microsoft 365 workloads and has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, learners should be able to:

- Plan and deploy a data archiving and retention system.
- Perform assessments in Compliance Manager.
- Manage email retention through Exchange.
- Conduct an audit log investigation.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.

Course Outline

Module 1: Archiving and Retention

This module explains concepts related to retention and archiving of data for Microsoft 365 including Exchange and SharePoint.

Lessons

- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention Policies in the Security and Compliance Center
- Archiving and Retention in Exchange
- In-place Records Management in SharePoint

Lab : Archiving and Retention

- Create and license users in your organization
- Configure Retention Tags and Policies
- MRM Retention Policies

After completing this module, you should be able to:

- Describe Data Governance in Microsoft 365.
- Describe the difference between In-Place Archive and Records Management.
- Explain how data is archived in Exchange.
- Recognize the benefits of In Place Records Management in SharePoint.
- Explain the difference between Message Records Management (MRM) in Exchange and Retention in Security and Compliance center.
- Explain how a retention policy works.
- Create a retention policy.
- Enable and disable In-Place Archiving.
- Create useful retention tags.

Module 2: Data Governance in Microsoft 365

This module focuses on data governance in Microsoft 365. The module will introduce you to Compliance Manager and discuss GDPR.

Lessons

- Planning Security and Compliance Needs
- Building Ethical Walls in Exchange Online
- Manage Retention in Email
- Troubleshooting Data Governance

- Analytics and Telemetry

After completing this module, you should be able to:

- Plan security and compliance roles.
- Describe what you need to consider for GDPR.
- Describe what an ethical wall in Exchange is and how it works.
- Work with retention tags in mailboxes
- Describe retention policies with email messages and email folders
- Explain how the retention age of elements is calculated.
- Repair retention policies that do not run as expected.

Module 3: Managing Search and Investigations

This module is focused on content searching and investigations. Specifically, it covers how to use eDiscovery to conduct advanced investigations of Microsoft 365 data. It also covers audit logs and discusses GDPR data subject requests.

Lessons

- Searching for Content in the Security and Compliance Center
- Audit Log Investigations
- Advanced eDiscovery

Lab : eDiscovery

- Create and license users in your organization
- Investigate your Microsoft 365 Data

After completing this module, you should be able to:

- Describe how to use content search.
- Designing your content search.
- Configuring search permission filtering.
- Describe what the audit log is and the permissions that are necessary to search the Office 365 audit log.
- Configure Audit Policies.
- Enter criteria for searching the audit log.
- Export search results to a CSV file.
- Describe what Advanced eDiscovery is and what requirements are needed.
- Analyze data in Advanced eDiscovery.
- Viewing the Advanced eDiscovery event log.
- Use Express Analytics.

Prerequisites

Learners should start this course already having the following skills:

- Basic conceptual understanding of Microsoft Azure
- Experience with Windows 10 devices
- Experience with Office 365
- Basic understanding of authorization and authentication
- Basic understanding of computer networks
- Working knowledge of managing mobile devices