Administering Information Protection and Compliance in Microsoft 365

Content

Module 1: Introduction to Information Protection and Data Lifecycle Management in Microsoft Purview

- Discuss the importance of information protection and data lifecycle management.
- Describe Microsoft's approach to these areas.
- Define key terms associated with Microsoft's information protection and data lifecycle management solutions.
- Identify the solutions offered by Microsoft Purview for information and data lifecycle management.

Module 2: Classify Data for Protection and Governance

- List components of the Data Classification solution.
- Identify cards available on the Data Classification overview tab.
- Explain the Content explorer and Activity explorer.
- Describe how to use sensitive information types and trainable classifiers.

Module 3: Create and Manage Sensitive Information Types

- Recognize differences between built-in and custom sensitivity labels.
- Configure sensitive information types with exact data match-based classification.
- Implement document fingerprinting and create custom keyword dictionaries.

Module 4: Understand Microsoft 365 Encryption

- Explain how encryption mitigates unauthorized data disclosure risks.
- Describe Microsoft data-at-rest and data-in-transit encryption solutions.
- Understand service encryption at the application layer and the differences between Microsoft managed keys and customer managed keys.

Module 5: Deploy Microsoft Purview Message Encryption

- Configure Microsoft Purview Message Encryption for end users.
- Implement Microsoft Purview Advanced Message Encryption.

Module 6: Protect Information in Microsoft Purview

- Discuss the information protection solution and its benefits.
- List customer scenarios addressed by the information protection solution.
- Describe the configuration process and user experience of the solution.
- Articulate deployment and adoption best practices.

Module 7: Apply and Manage Sensitivity Labels

- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites.
- Monitor label usage using label analytics.
- Configure on-premises labeling and manage protection settings and marking for applied sensitivity labels.
- Apply protections and restrictions to email and files.

Module 8: Prevent Data Loss in Microsoft Purview

- Discuss the benefits of the data loss prevention (DLP) solution.
- Describe the DLP configuration process.
- Explain user experiences with the implemented solution.

Module 9: Configure DLP Policies for Microsoft Defender for Cloud Apps and Power Platform

- Describe DLP integration with Microsoft Defender for Cloud Apps.
- Configure DLP policies in Microsoft Defender for Cloud Apps.

Module 10: Manage Data Loss Prevention Policies and Reports in Microsoft 365

- Review and analyze DLP reports.
- Manage permissions for DLP reports.
- Identify and mitigate DLP policy violations.
- Mitigate DLP violations in Microsoft Defender for Cloud Apps.

Module 11: Manage the Data Lifecycle in Microsoft Purview

- Discuss the Data Lifecycle Management solution and its benefits.
- List customer scenarios addressed by the Data Lifecycle Management solution.
- Describe the configuration process and user experience.
- Articulate deployment and adoption best practices.

Module 12: Manage Data Retention in Microsoft 365 Workloads

- Describe retention features in Microsoft 365 workloads.
- Configure retention settings in Teams, Yammer, and SharePoint Online.
- Recover content protected by retention settings and regain items from Exchange Mailboxes.

Module 13: Manage Records in Microsoft Purview

- Discuss the Microsoft Purview Records Management solution and its benefits.
- List customer scenarios addressed by the solution.
- Describe the configuration process and user experience.
- Articulate deployment and adoption best practices.

Module 14: Explore Compliance in Microsoft 365

- Describe how Microsoft 365 helps manage risks, protect data, and meet regulatory compliance.
- Plan compliance tasks in Microsoft Purview.
- Manage compliance requirements with Compliance Manager and use the Compliance Manager dashboard to improve compliance posture.

Module 15: Search for Content in the Microsoft Purview Compliance Portal

- Describe how to use content search in the Purview compliance portal.
- Design, create, and preview content searches.
- View search statistics, export search results, and configure search permission filtering.

Module 16: Manage Microsoft Purview eDiscovery (Standard)

- Describe how eDiscovery (Standard) builds on basic search and export functionalities.
- Create eDiscovery cases and holds.
- Search for content in cases and export it.
- Close, reopen, and delete cases.

Module 17: Manage Microsoft Purview eDiscovery (Premium)

- Describe how eDiscovery (Premium) builds on eDiscovery (Standard).
- Create and manage cases, custodians, and non-custodial data sources.
- Analyze case content and use analytical tools to reduce search result sets.

Module 18: Manage Microsoft Purview Audit (Standard)

- Describe differences between Audit (Standard) and Audit (Premium).
- Identify core features of the Audit (Standard) solution.
- Set up and implement audit log searching.
- Export, configure, view audit log records, and use searching to troubleshoot issues.

Module 19: Prepare Microsoft Purview Communication Compliance

- List enhancements in communication compliance over Office 365 Supervision policies.
- Identify and remediate code-of-conduct policy violations.
- Describe prerequisites for creating communication compliance policies.
- Explore built-in, pre-defined policy templates.

Module 20: Manage Insider Risk in Microsoft Purview

- Explain how Insider Risk Management helps prevent, detect, and contain internal risks.
- Describe built-in, pre-defined policy templates and prerequisites for insider risk policies.
- Explain actions taken on insider risk management cases.

Module 21: Implement Microsoft Purview Information Barriers

- Describe how information barriers restrict or allow communication and collaboration among groups.
- Explain components and configuration of information barriers.
- Understand how information barriers help manage user access to Teams, OneDrive, and SharePoint.

Module 22: Manage Regulatory and Privacy Requirements with Microsoft Priva

- Create and manage risk management policies for data overexposure, transfer, and minimization.
- Investigate and remediate risk alerts.
- Manage Subject Rights Requests, including estimation, retrieval, review, and reporting.

Module 23: Implement Privileged Access Management

- Explain the difference between privileged access management and privileged identity management.
- Describe the process flow and configuration of privileged access management.

Module 24: Manage Customer Lockbox

- Describe the Customer Lockbox workflow.
- Approve or deny Customer Lockbox requests.
- Audit actions performed by Microsoft engineers when access requests are approved.