SC-400: Microsoft Information Protection Administrator Associate

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 and solutions for these areas.
- Define key terms and identify Microsoft Purview solutions.

Module 2: Classify Data for Protection and Governance

- List components of the Data Classification solution.
- Understand Data Classification overview, Content explorer, and Activity explorer.
- Utilize sensitive information types and trainable classifiers.

Module 3: Create and Manage Sensitive Information Types

- Differentiate between built-in and custom sensitivity labels.
- Configure exact data match-based classification and implement document fingerprinting.
- Create custom keyword dictionaries.

Module 4: Understand Microsoft 365 Encryption

- Explain encryption's role in preventing unauthorized data disclosure.
- Describe encryption solutions for data-at-rest and data-in-transit.
- Understand service encryption and key management options.

Module 5: Deploy Microsoft Purview Message Encryption

- Configure and implement Microsoft Purview Message Encryption and Advanced Message Encryption.

Module 6: Protect Information in Microsoft Purview

- Discuss benefits and scenarios of the information protection solution.
- Describe configuration, user experience, and best practices for deployment.

Module 7: Apply and Manage Sensitivity Labels

- Apply sensitivity labels across Microsoft Teams, groups, and SharePoint sites.
- Monitor and manage label usage and protection settings for emails and files.

Module 8: Prevent Data Loss in Microsoft Purview

SPIRETEC
INNOVATIONS THROUGH IMAGINATION

- Discuss data loss prevention solutions and benefits.
- Describe configuration processes and user experiences.

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

- Integrate and configure DLP policies in Microsoft Defender for Cloud Apps.

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

- Review, analyze, and manage DLP policies and reports.
- Mitigate policy violations and manage permissions.

Module 11: Manage the Data Lifecycle in Microsoft Purview

- Discuss Data Lifecycle Management benefits and scenarios.
- Describe configuration processes and user experiences.

Module 12: Manage Data Retention in Microsoft 365 Workloads

- Describe and configure retention settings for Microsoft Teams, Yammer, SharePoint Online, and Exchange Mailboxes.

Module 13: Manage Records in Microsoft Purview

- Discuss the benefits and scenarios of Microsoft Purview Records Management.
- Describe configuration processes and user experiences.

Module 14: Explore Compliance in Microsoft 365

- Manage risks, protect data, and ensure compliance with Microsoft 365.
- Use Compliance Manager for compliance management and score assessment.

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

- Use content search functionalities, design searches, preview results, and export reports.

Module 16: Manage Microsoft Purview eDiscovery (Standard)

- Describe the eDiscovery (Standard) workflow and functionalities.
- Create cases, holds, search, and export content.

Module 17: Manage Microsoft Purview eDiscovery (Premium)

- Build on eDiscovery (Standard) with advanced case management and analysis tools.

Module 18: Manage Microsoft Purview Audit (Standard)

- Understand Audit (Standard) features and set up audit log searching and troubleshooting.

Module 19: Prepare Microsoft Purview Communication Compliance

- Identify enhancements over Office 365 Supervision policies and create communication compliance policies.

Module 20: Manage Insider Risk in Microsoft Purview

- Prevent, detect, and contain internal risks with Microsoft Purview Insider Risk Management.
- Create and manage insider risk policies and actions.

Module 21: Implement Microsoft Purview Information Barriers

- Restrict or allow communication and collaboration using information barriers.
- Understand components and configurations of information barriers.

Module 22: Manage Regulatory and Privacy Requirements with Microsoft Priva

- Manage risk policies for data overexposure, transfer, and minimization.
- Handle Subject Rights Requests and related privacy tasks.

Module 23: Implement Privileged Access Management

- Differentiate between privileged access management and identity management.
- Configure and enable privileged access management.

Module 24: Manage Customer Lockbox

- Describe the Customer Lockbox workflow, approval process, and auditing of actions.