Microsoft

SC-400T00 – Microsoft Information Protection and Compliance Administrator

ASSESSMENT GUIDE

Overview

This document provides information and guidance on how to develop formative and summative assessments for SC-400T00 Microsoft Information Protection and Compliance Administrator. It is split into two main sections:

- **Section 1: Learning path questions** provides guidance for assessing student mastery as they progress through the course. This section includes a set of items for each course learning path that you can use throughout the course to monitor student progress and inform your instruction; the assessment items may include multiple-choice questions and/or open-ended questions.

This guide is intended to be a reference and starting point for instructors as you plan how to assess your students. As you read through the guide, you may choose to tailor the assessment strategies, including the assessment items and rubric, for your classroom.

Table of Contents

Section 1: Learning path questions

Introduction

This section includes multiple choice and/or open-ended questions that are aligned to the course learning paths for SC-400T00 Microsoft Information Protection and Compliance Administrator.

You can use the questions as they are presented or modify them as appropriate for your learners. The questions do not appear in any other course materials and are designed to supplement the formative assessment opportunities that are integrated directly into Microsoft Learn and the Microsoft Official Course, such as Knowledge Checks, "Try-It" activities, Exercises, Walkthroughs, Labs, and Demos.

Questions are designed to allow for easy integration into an online quiz through Microsoft Forms or through your institution's Learning Management System (LMS). If you aren't familiar with the Microsoft Forms short support videos are available. As a best practice, create new quizzes and delete old quizzes each class to keep the response URLs from being circulated and responses continuing to come in after class.

Assigning the module questions to students as an independent activity will enable you to collect data about individual student progress. However, we recommend that you set aside class time to review answers and address any common student misconceptions, as later modules depend on knowledge and understanding gained earlier in the course.

Overview of multiple-choice questions

The multiple-choice questions require one or more answer responses and will include plausible distractors. These are set at a level slightly lower than the multiple-choice questions in the SC-400 Administering Information Protection and Compliance in Microsoft 365 certification exam.

Overview of open-ended questions

The open-ended questions present challenges beyond single answer responses and include scenario-based questions. These questions give students the opportunity to demonstrate critical thinking through their responses.

For their responses, encourage students to explore multiple Microsoft Purview product solutions and adopt a design-first approach before settling on a potential solution. Exploring the official Microsoft Purview risk and compliance documentation is a great place for students to research and investigate the different Microsoft Purview risk and compliance products and services that are available.

Learning Path 1: Implement Information Protection in Microsoft 365

Multiple choice questions

1. Use this simple quiz to check knowledge for the Implement Information Protection in Microsoft 365 topic area of the SC-400 Microsoft Information Protection Administrator training.

   a. Retention label

   b. Sensitive information types (SIT) (correct answer)

   c. Sensitivity label

   d. Keyword list

2. Which of the following lets you classify and protect data while making sure user productivity isn't hindered?

   a. Sensitivity label (correct answer)

   b. Document fingerprint

   c. Retention label

   d. Sensitive Information Type

3. Where should your data be stored to seed and train a trainable classifier?

   a. **In a SharePoint Online document library or folder (correct answer)**

   b. On an Azure SQL database

   c. In a dedicated folder in OneDrive

   d. In an Azure Blob storage account

4. Why would an automatic sensitivity label be important to an organization?

   a. Users would train to be experts in your policies before applying sensitivity labels.

   b. Users need to be trained on when to use each of the classifications.

   c. Users don't need to be relied upon to classify all content correctly. (correct answer)

5. What service needs to be activated on your Microsoft 365 tenant to implement Microsoft Purview Message Encryption?

   a. Exchange Admin Center (EAC)

   b. Office 365 Message Encryption (OME)

   c. Information Rights Management (IRM)

   d. Microsoft Azure Rights Management (Azure RMS) (correct answer)

Open-ended questions

1. Describe a sensitive information type. Be sure to discuss the different types of sensitive information available in Microsoft 365.

Answer: (Sensitive information types are pattern-based classifiers. They are used to detect sensitive information like driver's license, credit card, and bank account numbers. Microsoft provides built in sensitive information types. If preconfigured sensitive information types do not suit business needs, custom sensitive information types can be created that is fully defined on your own or based on a copy of a built-in sensitive information type. Exact data match (EDM) sensitive information types are created from scratch and are used to detect the exact values that have been defined in a database of sensitive information.)

2. Describe data loss prevention (DLP) and its importance in an organization.

   Answer: (To comply with business standards and industry regulations, organizations must protect sensitive information and prevent inadvertent disclosure. Sensitive information can include financial data or personal information, such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across your environment.)

3. Describe trainable classifiers and how trainable classifiers identify items.

   Answer: (A Microsoft Purview trainable classifier is a tool you can train to recognize various types of content by giving it samples to look at. Once trained, you can use it to identify items for sensitivity labels, communications compliance policies, and retention policies. Trainable classifiers are useful when content is not easily identified using pattern matching. Trainable classifiers apply artificial intelligence (AI) and machine learning (ML) to find data to track, protect, and govern.)

4. Describe Microsoft Purview Message Encryption and its implementation.

   Answer: (Microsoft Purview Message Encryption allows organizations to share protected email with anyone on any device. Users can exchange protected messages with other Microsoft 365 organizations, as well as third-parties using Outlook.com and other email services. To activate Purview Message Encryption, Azure Rights Management (Azure RMS) and Information Rights Management (IRM) capabilities must be activated on your tenant. The next step is to define a mail flow rule which determines under what condition email messages should be encrypted, as well as conditions for removing that encryption.)

5. Describe the necessary steps for configuring sensitivity labels.

   Answer: (Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied, automatically or by the user, the content or site is protected based on the settings you choose. To configure a sensitivity label, you need to set the Name and Description for the sensitivity label. Next set the Encryption to either none, to apply encryption, or remove existing encryption. The next step is to configure the option for Content marking for either a watermark, header, or footer. From there you have the option to set Site and group settings. In the next step you have the option to configure auto-labeling, and from there you review your settings.)

Learning Path 2: Implement Data Loss Prevention

Multiple choice questions

1. The customer service manager for a bank is concerned about his team sharing personally identifiable information (PII) through Microsoft Teams. What tool can you recommend to prevent the sharing of this sensitive information through Microsoft Teams?

   a. Document fingerprint

   b. Insider Risk Management

   c. Data Loss Prevention (DLP) (correct answer)

   d. Retention label

2. Which of the following is best practice when creating DLP policies?

   a. Test your DLP policies before turning them on (correct answer)

   b. Turn them on right away and modify based on DLP false positive reports

   c. Always avoid templates and create custom policies

3. What is required to onboard Windows devices for DLP activity monitoring?

   a. A supported version of Microsoft Office installed and up to date. (correct answer)

   b. Ensure the device is on Windows 8.1 or later.

   c. The device is not joined to Azure Active Directory (Azure AD)

   d. The account onboarding the device must have the Compliance Manager Administrator role.

4. The manager of the finance department is wanting to know when files are being shared from the organization's OneDrive account to non-Microsoft cloud apps. Which of the tools below would you recommend?

   a. A connector in Power Platform

   b. A file policy within Microsoft 365 Defender (correct answer)

   c. A sensitivity label

   d. Document fingerprinting

5. You have created DLP policies for a healthcare organization. Members of the security team are receiving excessive alerts from false positives. How can you ensure the team only receives relevant alerts to help prevent alert fatigue in the department?

   a. Use keyword dictionaries based on the organization's needs.

b. Modify the DLP policies to adjust how the policy behaves. (correct answer)

c. Delete the DLP policy and recreate it to the department's specifications.

Open-ended questions

1. What are methods for identifying sensitive data that should be protected by DLP?

   Answer: (Content explorer identifies the email and documents in your organization that contain sensitive information. Content explorer uses the built-in sensitive info types included in Microsoft Purview and any custom sensitive info types you define to identify the content. If only using built-in sensitive info types, no configuration is needed to allow you to understand the data you might want to protect.

   Activity explorer includes information on activity related to content that contains sensitive information, which can also inform what should be protected by DLP policies. Like content explorer, much of the data generated by activity explorer requires little or no configuration.)

2. What is Endpoint DLP and what deployment options are available through device onboard?

   Answer: (Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items on Windows devices. Once devices are onboarded into the Microsoft Purview compliance portal, the information about what activities (like copying to USB devices or printing) users perform on sensitive items is visible to those who have access to activity explorer in the Microsoft Purview compliance portal. You can also take the extra step of auditing or restricting those activities via data loss prevention policies. Devices can be onboarded via local script, group policy, Microsoft Endpoint Configuration Manager, Mobile Device Management/Microsoft Intune or VDI onboarding scripts for non-persistent machines.)

3. Describe DLP policies for Power Platform and the groups that can be used to categorize connectors.

   Answer: (While DLP policies in the Microsoft Purview compliance portal protect data in Microsoft 365 services from being shared, DLP policies in Power Platform are used to restrict communication between connectors. A connector in Power Platform is a wrapper or an API that allows predefined triggers and actions to access the data behind it. DLP policies enforce rules for which connectors can be used together by classifying connectors as either Business or Non-Business. If you put a connector in the Business group, it can only be used with other connectors from that group in any given app or flow. Sometimes you might want to block the usage of certain connectors altogether by classifying them as Blocked.)

4. Describe DLP integration in Microsoft 365 Defender.

   Answer: (Data loss prevention polices can be used for non-Microsoft cloud apps. You can use DLP policies for non-Microsoft cloud apps to monitor and detect when sensitive data is used and shared with non-Microsoft Cloud apps. File policies allow you to control the actions you can execute in Microsoft 365 Defender. To integrate DLP with Microsoft 365 Defender, file policies must be enabled in Microsoft 365 Defender. To do this, navigate to the Microsoft 365 Defender, select Settings, then select Settings again. Select Files from the Information Protection section, then check Enable file monitoring if not already selected, then select Save.)

5. Describe the different DLP reports and when you would use each report**.**

Answer: (In the Microsoft Purview Compliance portal you have options to view the DLP policy matches, DLP incidents, and DLP false positives and overrides reports. DLP policy matches is a detailed report that shows the count of DLP policy matches over time. This report is often used to tune or refine your DLP policies. The DLP incidents report also shows policy matches over time, but this report shows matches at a rule level. For example, if an email matched three different rules, the policy matches report shows three different line items while the incidents report would show a single line item for that piece of content. The DLP false positives and overrides reports shows a count of user reported false positives and overrides over time.)

Learning Path 3: SC-400: Implement Data Lifecycle and Records Management

Multiple choice questions

1. You work for a company that requires content in SharePoint Online, OneDrive, and mailboxes are retained for no longer than two years after creation. Which of the following tools would help you implement based on this requirement? (Select two)

   a. Retention polices (correct answer)

   b. Regulatory records

   c. Retention labels (correct answer)

   d. Trainable classifiers

   e. Mailbox archives

2. Which of the following actions are allowed when content is declared a regulatory record in OneDrive?

   a. Open/read documents (correct answer)

   b. Delete files

   c. Edit documents

   d. Rename files

3. Which of the following is a feature of retention labels but not retention policies?

   a. The capability to retain and delete content.

   b. The capability to apply event-based retention. (correct answer)

   c. The capability to apply retention automatically.

4. Which of the following file formats is supported by file plans?

   a. XML

   b. CVS (correct answer)

   c. HTML

   d. RTF

5. You work for an office that needs a tool that enables preservation of mailboxes for legal purposes on an as needed basis. This tool needs to include the following capabilities:

- The need to preserve all mailbox items including deleted items, modified items, and archived items.

- The tool needs to support individual mailbox holds.

Which of the following would you recommend for this requirement?

   a. Retention policies

   b. Retention labels

   c. eDiscovery hold (correct answer)

   d. Litigation hold

Open-ended questions

1. Describe the principles of retention.

   Answer: (You may run into situations where content has several retention labels and policies applied. The policies may have different actions or different retention periods. The principles of retention explain what takes precedence in these situations.

   - **Retention wins over deletion. If your content has one policy that states to retain content for three years, but another retention policy states to delete it after one, in this case the retention policy wins, and the content is retained for three years.**
   - **Longest period of retention wins. If one retention policy states to keep content for five years, but another retention policy states to keep the same content for three years, the content will be retained for five years.**
   - **Explicit wins over implicit. If content has a retention label that is manually assigned to retain content for five years, and a retention policy assigned at a mailbox, site, or document library level is assigned to retain content for three years, the content will be retained for five years. The label that was manually assigned was explicitly assigned to be retained for five years. The retention policy is implicitly applied.**
   - **Shortest deletion period wins. If content has two different retention policies applied with one retention policy with a deletion action for 10 years after creation while another retention**

policy has a delete action for 7 years after creation, the content will be deleted after 7 years because that's the shortest deletion period between the two policies.)

2. Describe the difference between a retention label and a retention policy.

   Answer: (Retention labels are assigned at the item level while retention polices are assigned at the site or mailbox level. Retention labels support the features below while retention policies do not:

   - **When using retention labels, retention settings travel with the content if it's moved to a different location within your Microsoft 365 tenant.**
   - **Retention labels support the use of event-based retention.**
   - **You can use trainable classifiers to identify content to label.**
   - **You can apply a default label for SharePoint items or Exchange messages.**
   - **At the end of the retention period, retention labels support disposition review to review content before it's permanently deleted as well as the ability to automatically apply another retention label.**
   - **Retention labels support marking the content as a label as part of the label settings, and always having proof of disposition when content is deleted at the end of its retention period.)**

3. Describe the mailbox hold features available on Exchange Online.

   Answer: (Exchange online provides a feature called holds to prevent mailbox content from being deleted. This feature is applied on single mailbox level. There are two types of holds available in Exchange online. The litigation hold prevents all content within a mailbox from being deleted. The eDiscovery hold prevents only mailbox content that matches specific search criteria from being changed or deleted.)

4. Describe a file plan and its capabilities.

   (Answer: File plans from Records management in the Microsoft Purview compliance portal have the following capabilities:

   - **Bulk-create retention labels from a spreadsheet**
   - **Export information from existing retention labels for analysis and offline collaboration**
   - **More information about retention labels is displayed to make it easier to see into and across the settings of all your retention labels from one view**
   - **File plane descriptors support additional and optional information for each label)**

5. Describe event driven retention and its requirements.

   Answer: (When you retain content, the retention period is often based on the age of the content. You can also create retention labels based on events. The event triggers the start of the retention

period, and all content with a retention label applied for that type of event get the label's retention actions enforced on them. Event-based retention requires retention settings that:

- **Retain the content.**
- **Delete the content automatically or trigger a disposition review at the end of the retention period.)**

Learning Path 4: SC-400: Monitor and investigate data and activities by using Microsoft Purview

Multiple choice questions

1. What does Microsoft Purview Compliance Manager help organizations with?

    a. Understanding their current state of compliance and highlighting areas for improvement (correct answer)

    b. Assigning compliance permissions

    c. Enabling auditing for the organization

    d. Creating policies to alert potential compliance issues

2. How does Compliance Manager calculate the overall compliance score?

    a. By assigning scores to improvement actions, controls, and assessments

    b. By averaging the scores of all completed improvement actions

    c. By summing the scores of all Microsoft actions and improvement actions (correct answer)

    d. By considering the risk level and type of each action

3. Which step in the eDiscovery (Standard) workflow involves copying the results of a search to a Microsoft-provided Azure Storage location?

    a. Create an eDiscovery hold

    b. Search for content

    c. Export and download search results (correct answer)

    d. Download the exported data

4. Which auditing solution in Microsoft Purview provides the ability to log and search for audited activities and is turned on by default for organizations with the appropriate subscription?

a. Office 365 Management Activity API

b. Audit (Premium)

c. Audit log retention policies

d. Audit (Standard) (correct answer)

5. Which auditing action in Microsoft 365 helps investigators better understand email data breaches and identify the scope of compromises to specific mail items?

a. MailItemsAccessed (correct answer)

b. Mailbox audit log

c. Sync access

d. Bind access

Open-ended questions

1. What steps should organizations complete when planning for security and compliance in Microsoft 365?

Answer:

- **Familiarize yourself with information protection capabilities in Microsoft 365.**
- **After setting up your Microsoft 365 subscription, take note of your starting score within the Microsoft Secure Score tool. Secure Score provides configuration suggestions that an organization can take to increase its score. The goal is to be aware of opportunities that you can take to protect your environment without negatively affecting your users' productivity.**
- **Plan access protection for identity and devices. Organizations can defend against cyber-attacks and guard against data loss by protecting access to data and services and securing email policies and configurations.**
- **Plan data protection based on data sensitivity.**
- **Use the Microsoft Purview compliance portal to provide a single view into the controls needed to manage the spectrum of Microsoft 365 data governance.**
- **Use recommended configurations as a starting point for enterprise scale or sophisticated access security scenarios.**

2. What are the three eDiscovery solutions provided by Microsoft Purview and how do they differ from each other?

Answer: Microsoft Purview provides three eDiscovery solutions: Content search, eDiscovery (Standard), and eDiscovery (Premium). Content search is a basic search and export functionality that can be used to search for content across Microsoft 365 data sources and export the search results to a local computer. eDiscovery (Standard) builds on the basic search and export functionality of Content search by enabling organizations to create eDiscovery cases and assign eDiscovery

managers to specific cases. eDiscovery managers can only access the cases of which they're members. eDiscovery (Standard) also lets an organization associate searches and exports with a case. It also lets an organization place an eDiscovery holds on content locations relevant to cases. eDiscovery (Premium) builds on the existing case management, preservation, search, and export capabilities in eDiscovery (Standard). eDiscovery (Premium) provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to an organization's internal and external investigations. It lets legal teams manage custodians and the legal hold notification workflow to communicate with custodians involved in a case. It also enables an organization to collect and copy data from the live service into review sets. From there, the organization can filter, search, and tag content to cull non-relevant content from further review. By doing so, an organization's workflow can identify and focus on content that's most relevant. eDiscovery (Premium) provides analytics and machine learning-based predictive coding models. These features enable an organization to further narrow the scope of an investigation to the most relevant content.

3. What are the key capabilities of Microsoft Purview eDiscovery (Premium) and how does it differ from other eDiscovery solutions?

Answer: Microsoft Purview eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export content that's responsive to an organization's internal and external investigations. It also lets legal teams manage the entire legal hold notification workflow to communicate with custodians involved in a case. The key capabilities of eDiscovery (Premium) include managing eDiscovery workflows by identifying persons of interest and their data sources, applying holds to preserve data, and managing the legal hold communication process. eDiscovery (Premium) also enables organizations to discover data where it lives by collecting data from the source, reducing large volumes of data to a relevant data set using intelligent, machine learning capabilities such as deep indexing, email threading, and near duplicate detection. Unlike traditional eDiscovery solutions that require copying large volumes of data out of Microsoft 365 to process and host duplicate data, eDiscovery (Premium) enables organizations to discover data at the source and stay within their Microsoft 365 security and compliance boundary. It also provides a streamlined, end-to-end workflow, all of which occurs within Microsoft 365, helping organizations reduce the number of eDiscovery solutions they need to rely on. Finally, eDiscovery (Premium) aligns with the eDiscovery process outlined by the Electronic Discovery Reference Model (EDRM), providing a built-in workflow that supports the EDRM.

4. What are the differences between Microsoft Purview Audit (Standard) and Audit (Premium)?

Answer: Microsoft Purview provides two auditing solutions: Audit (Standard) and Audit (Premium). Audit (Standard) provides organizations with the ability to log and search for audited activities. It also enables an organization to power its forensic, IT, compliance, and legal investigations. Audit (Premium) builds on the capabilities of Audit (Standard) by providing audit log retention policies, longer retention of audit records, high-value crucial events, and higher bandwidth access to the Office 365 Management Activity API. With Audit (Premium), organizations can create customized audit log retention policies to retain audit records for up to one year (and up to 10 years for users

with required add-on license). Organizations can create log retention policies to retain audit records based on the service where the audited activities occurred, specific audited activities, or the user who performed an audited activity. Exchange, SharePoint, and Azure Active Directory audit records are retained for one year by default. Audit records for all other activities are retained for 90 days by default.

5. What are the steps to set up and use Microsoft Purview Audit (Premium)?

Answer: To set up and use Microsoft Purview Audit (Premium) capabilities, an organization should:

1. **Assign appropriate E5 licenses to users and enable the Advanced Auditing app.**
2. **Enable "SearchQueryInitiatedExchange" and "SearchQueryInitiatedSharePoint" events for users in Exchange Online and SharePoint Online.**
3. **Set up audit retention policies based on security and compliance needs.**
4. **Use the audit log to search for Audit (Premium) events during forensic investigations.**

Learning Path 5: Manage Insider and Privacy Risk in Microsoft 365

Multiple choice questions

1. What is the purpose of Microsoft Purview Communication Compliance?

a. To monitor and identify code of conduct policy violations in company communications channels (correct answer)

b. To manage insider risk and supervise employee communications

c. To detect and remediate violations of regulatory compliance requirements

d. To provide interactive dashboards for auditing support

2. What is the purpose of the *Review percentage* setting in a communication compliance policy?

a. It determines the percentage of communications that will be reviewed by supervisors. (correct answer)

b. It sets the threshold for sensitive information detection in communications.

c. It defines the number of reviewers assigned to review communications.

d. It specifies the percentage of users who will be subject to the policy.

3. What is the purpose of assigning alerts to a case in insider risk management?

a. To review the individual signals and conduct a detailed investigation (correct answer)

b. To send a notice to the offending employee

c. To escalate the case for further investigation

d. To resolve the case as either benign or a confirmed policy violation

4. What action can be taken on a case after reviewing and investigating the alerts?

a. Escalate the case for legal review

b. Send a notice to the employee

c. Access the eDiscovery (Premium) case for further analysis

d. Resolve the case with a classification and change the status to Closed (correct answer)

5. How are segments used in Microsoft Purview Information Barriers?

a. Segments are used to define policies for different groups of users

b. Segments are used to create logical groupings of users based on job function or department (correct answer)

c. Segments are used to manage access to SharePoint Online and OneDrive

d. Segments are used to enable communication and collaboration between teams

Open-ended questions

1. What are some common scenarios where communication compliance policies can be useful?

Answer: Communication compliance policies can be useful in common scenarios, such as corporate policies where you can scan employee communications in your organization for potential human resources concerns such as harassment or the use of inappropriate or offensive language, risk management where you can scan messages in your organization for unauthorized communications about confidential projects such as upcoming acquisitions, mergers, earnings disclosures, reorganizations, or leadership team changes, and regulatory compliance when organizations are required to implement some type of supervisory or oversight process for messaging that is appropriate for their industry.

2. What are the components of an insider risk management policy in Microsoft Purview, and how can they be configured?

Answer: Insider risk management policies in Microsoft Purview are created using pre-defined templates and policy conditions, which define the risk indicators that correspond to particular risk activities that can be identified and examined in Microsoft Purview feature areas. These conditions also include the users added to the policy, which services are prioritized, and the monitoring time period. The Policy dashboard allows you to quickly see the policies in your organization and the

current status of alerts associated with each policy. Insider risk management templates contain pre-defined policy conditions that define the types of risk indicators monitored by a policy. Insider risk settings apply to all insider risk management policies, regardless of the template you chose when creating a policy. To define the indicators that are enabled in all policies, navigate to Settings> Indicators and select one or more indicators.

3. What are information barriers and how can they help organizations avoid conflicts of interest and safeguard internal information between users and organizational areas?

Answer: Microsoft Purview Information Barriers is a compliance solution that allows organizations to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. It enables organizations to set up policies that control access to sensitive data and prevent certain users or groups from accessing that data. This feature can be useful in scenarios where there are regulatory requirements around data access and privacy, or where there are concerns about conflicts of interest. By creating logical groupings of users and applying policies based on those groupings, organizations can manage and control access to sensitive data.

4. What are some of the benefits of using Privacy Risk Management policies in Microsoft Purview, and how can organizations get started with creating and managing these policies?

Answer: Privacy Risk Management policies in Microsoft Purview can help organizations address risk scenarios that are important to their business, and foster sound data handling practices. By using policy templates with default settings, organizations can create new policies for data overexposure, data transfers, and data minimization, or customize these templates to suit their specific needs. Alerts and email notifications can help administrators and users stay informed about policy matches and privacy risks and take immediate action to address these issues. To get started with creating and managing Privacy Risk Management policies, organizations can use the policy creation wizard in the Microsoft Purview compliance portal, and follow the guided process to choose all settings, including the type of policy, data to monitor, users and groups, locations, conditions, outcomes, alerts, and mode. By regularly reviewing and updating these policies, organizations can help minimize risks and maintain compliance with regulatory requirements around data access and privacy.

5. What are the different types of requests that Priva Subject Rights Requests supports, and how can users create a request using a template with default settings?

Answer: Priva Subject Rights Requests supports three different types of requests: Access, Export, and Tagged list for follow up. Users can create a request from a template, which is a quick "out-of-box" option that uses tailored default settings. The three templates correspond to the three request types: Data access, Data export, and Data tagged for further action. Each template allows users to select the type of relationship between the data subject and their organization, which in turn determines default settings. To create a request from a template, users can select the type of request they want to create, and then select Get started.