vce trainer



MS-101.examsforall.premium.exam.150q

MS-101

MS-101

Microsoft 365 Mobility and Security

Version 6.0

Score: 800/1000

Version:

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Implement modern device services

(39 questions)

Question 1

HOTSPOT

Your network contains an Active Directory forest named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You use Microsoft System Center Configuration Manager (Current Branch) for device management.

You have the Windows 10 devices shown in the following table.

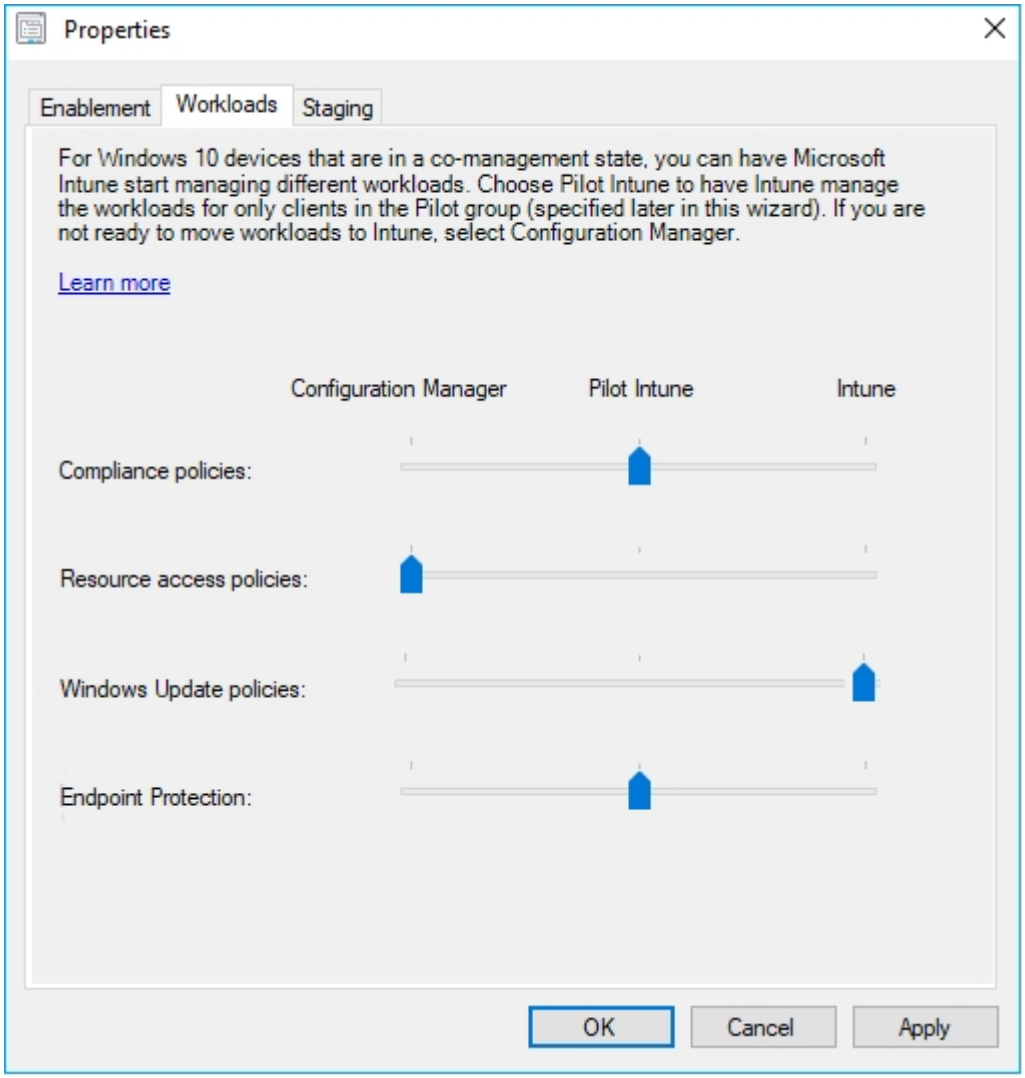
Name	Collection
Device1	Collection1
Device2	Collection2

You configure Configuration Manager co-management as follows:

Automatic enrollment in Intune: Pilot
Pilot collection: Collection2

You configure co-management workloads as shown in the following exhibit.

Licensed to Berend Post berend.post@it-university.nl



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	○	○
Configuration Manager manages the Windows Update policies for Device1.	○	○
Microsoft Intune manages Endpoint Protection for Device2.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 2

Your company has a Microsoft 365 subscription that contains the domains shown in the following table.

Name	Can enroll devices to Microsoft Intune by using auto-discovery
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

The company plans to add a custom domain named fabrikam.com to the subscription and then to enable enrollment of devices to Intune by using auto-discovery for fabrikam.com.

You need to add a DNS record to the fabrikam.com zone.

Which record type should you use for the new record?

- ☐ PTR
- ☐ SRV
- ☐ CNAME
- ☐ TXT

Question 3

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.

What should you do from the Security & Compliance admin center?

- ☐ Create a data loss prevention (DLP) policy that has a Content is shared condition.
- ☐ Modify the default safe links policy.
- ☐ Create a data loss prevention (DLP) policy that has a Content contains condition.
- ☐ Create a new safe links policy.

Licensed to Berend Post berend.post@it-university.nl

Question 4

HOTSPOT

You have several devices enrolled in Microsoft Intune.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	*None*

The device type restrictions in Intune are configured as shown in the following table.

Priority	Member of	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	*None*
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You add User3 as a device enrollment manager in Intune.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Intune.	○	○
User2 can enroll Android devices in Intune.	○	○
User3 can enroll iOS devices in Intune.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 5

HOTSPOT

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group2, Group3
Device3	Windows 10	Group2, Group3

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Assigned
Policy1	Windows 10 and later	Yes
Policy2	Android	No
Policy3	Windows 10 and later	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Policy1 applies to Device3.	◯	◯
Policy2 applies to Device2.	◯	◯

Licensed to Berend Post berend.post@it-university.nl

Question 6

Your company uses Microsoft System Center Configuration Manager (Current Branch) and Microsoft Intune to co-manage devices.

Which two actions can be performed only from Intune? Each correct answer presents a complete solution.

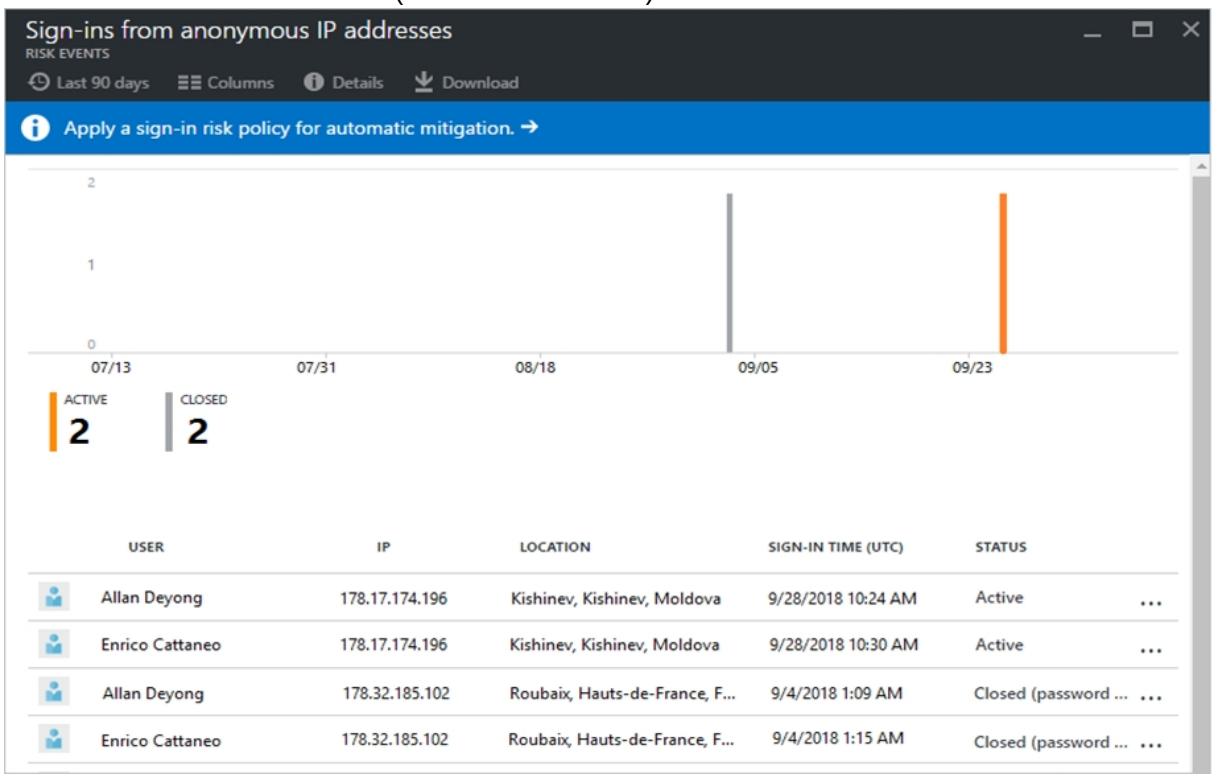
NOTE: Each correct selection is worth one point.

- ☐ Deploy applications to Windows 10 devices.
- ☐ Deploy VPN profiles to iOS devices.
- ☐ Deploy VPN profiles to Windows 10 devices.
- ☐ Publish applications to Android devices.

Licensed to Berend Post berend.post@it-university.nl

Question 7

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)



You need to reduce the likelihood that the sign-ins are identified at risky.

What should you do?

- ☐ From the Security & Compliance admin center, create a classification label.
- ☐ From the Security & Compliance admin center, add the users to the Security Readers role group.
- ☐ From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
- ☐ From the Conditional access blade in the Azure Active Directory admin center, create named locations.

Licensed to Berend Post berend.post@it-university.nl

Question 8

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices.

Your company uses the following types of devices:
Windows 10
Windows 8.1
Android
iOS

Which devices can be managed by using co-management?

- ☐ Windows 10 and Windows 8.1 only
- ☐ Windows 10, Android, and iOS only
- ☐ Windows 10 only
- ☐ Windows 10, Windows 8.1, Android, and iOS

Licensed to Berend Post berend.post@it-university.nl

Question 9

HOTSPOT

You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

The device type restrictions are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

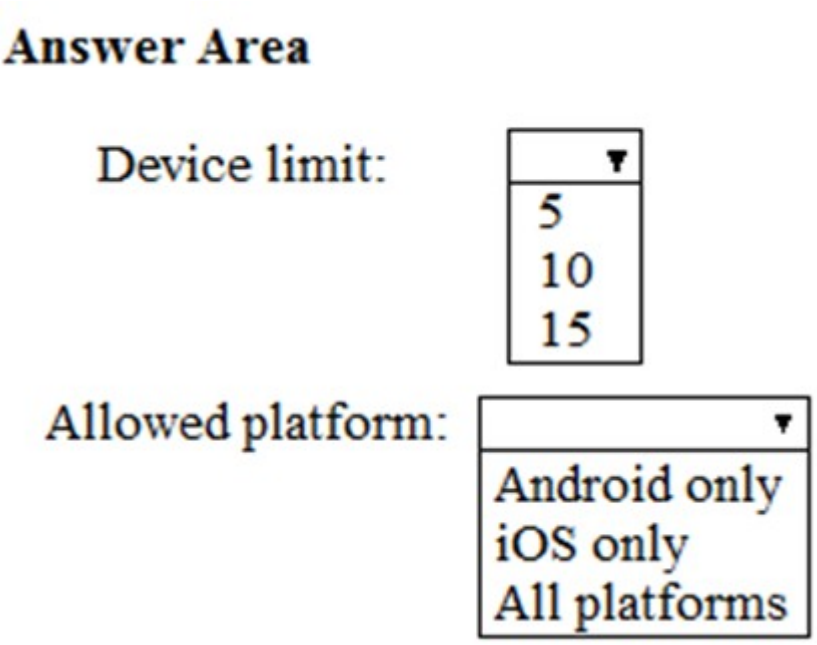
The device limit restrictions are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	Wet Region	5	Engineering
Default	All users	10	All users

What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Licensed to Berend Post berend.post@it-university.nl

Question 10

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 11

A user receives the following message when attempting to sign in to https://myapps.microsoft.com:

"Your sign-in was blocked. We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin."

Which configuration prevents the users from signing in?

- ☐ Microsoft Azure Active Directory (Azure AD) Identity Protection policies
- ☐ Microsoft Azure Active Directory (Azure AD) conditional access policies
- ☐ Security & Compliance supervision policies
- ☐ Security & Compliance data loss prevention (DLP) policies

Licensed to Berend Post berend.post@it-university.nl

Question 12

HOTSPOT

Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).

You have Windows 10 and Windows 8.1 devices.

You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First action to perform:

- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- Create a Microsoft Azure Log Analytics workspace.
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

- Configure all the devices to have a commercial ID.
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- Configure and restart the Windows Update service on all the devices.

Licensed to Berend Post berend.post@it-university.nl

Question 13

HOTSPOT

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 14

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 15

HOTSPOT

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Quality updates:
- 14 days
- 30 days
- 60 days
- 120 days

Feature updates:
- 60 days
- 180 days
- 365 days
- 540 days

Licensed to Berend Post berend.post@it-university.nl

Question 16

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.

The company recently hired four new users who have the devices shown in the following table.

Name	Operating system
User1	Windows 8
User2	Windows 10
User3	Android 8.0
User4	iOS 11

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Intune automatically.

Which users have a device that can enroll in Microsoft Intune automatically?

- ☐ User1, User2, User3, and User4
- ☐ User2 only
- ☐ User1 and User2 only
- ☐ User1, User2, and User3 only

Question 17

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You add your user account as a device enrollment manager.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 18

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You unjoin Device1 from the Active Directory domain.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 19

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices.

You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices.

You need to recommend a Windows 10 deployment method.

What should you recommend?

- ☐ a provisioning package
- ☐ an in-place upgrade
- ☐ wipe and load refresh
- ☐ Windows Autopilot

Licensed to Berend Post berend.post@it-university.nl

Question 20

Your company has a Microsoft 365 subscription. The subscription contains 500 devices that run Windows 10 and 100 devices that run iOS.

You need to create Microsoft Intune device configuration profiles to meet the following requirements:

Configure Wi-Fi connectivity to a secured network named ContosoNet.
Require passwords of at least six characters to lock the devices.

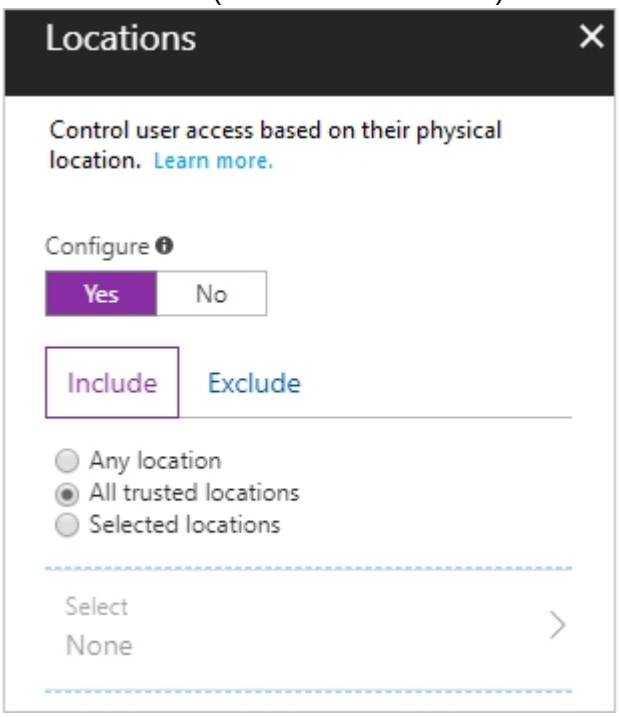
What is the minimum number of device configuration profiles that you should create?

- ☐ 4
- ☐ 2
- ☐ 1

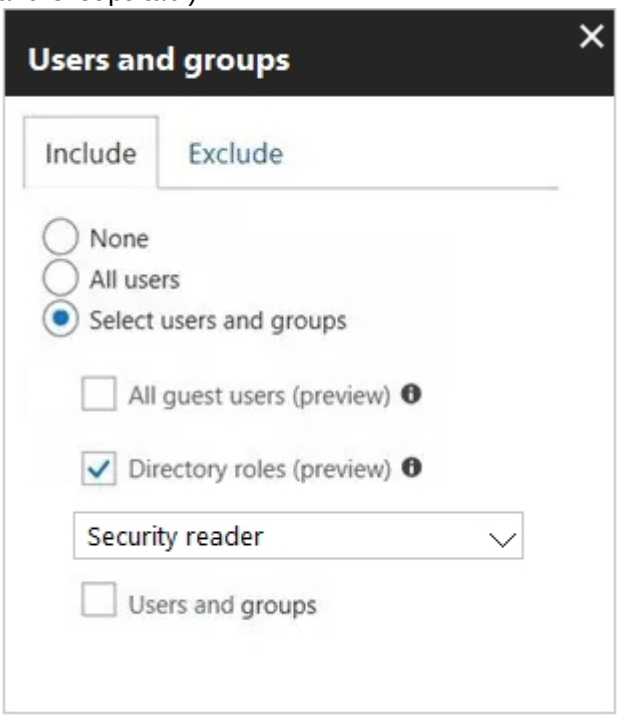
Licensed to Berend Post berend.post@it-university.nl

Question 21

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)



The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

Licensed to Berend Post berend.post@it-university.nl

What should you do?

- ☐ From the conditional access policy, configure the device state.
- ☐ From the Azure Active Directory admin center, create a custom control.
- ☐ From the Device Management admin center, create a device compliance policy.
- ☐ From the Azure Active Directory admin center, create a named location.

Question 22

You have Windows 10 Pro devices that are joined to an Active Directory domain.

You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business for SSO to Microsoft 365 services.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☐ computers that have biometric hardware features
- ☐ Microsoft Intune enrollment
- ☐ Microsoft Azure Active Directory (Azure AD)
- ☐ smartcards
- ☐ TPM-enabled devices

Licensed to Berend Post berend.post@it-university.nl

Question 23

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to a Configuration Manager device collection.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 24

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 25

You have computers that run Windows 10 Enterprise and are joined to the domain.

You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.

You need to prevent Windows from being updated for the next 30 days.

Which two Group Policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ Select when Quality Updates are received
- ☐ Select when Preview Builds and Feature Updates are received
- ☐ Turn off auto-restart for updates during active hours
- ☐ Manage preview builds
- ☐ Automatic updates detection frequency

Licensed to Berend Post berend.post@it-university.nl

Question 26

HOTSPOT

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

The device compliance policies in Intune are configured as shown in the following table.

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Non configured	15	Yes

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy2	Group2
Policy3	Group3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 27

Your company has 10 offices.

The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.

You discover that one of the offices has the following:

Computers that have several preinstalled applications
Computers that use nonstandard computer names
Computers that have Windows 10 preinstalled
Computers that are in a workgroup

You must configure the computers to meet the following corporate requirements:

All the computers must be joined to the domain.
All the computers must have computer names that use a prefix of CONTOSO.
All the computers must only have approved corporate applications installed.

You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.

What should you recommend?

- ☐ a provisioning package
- ☐ wipe and load refresh
- ☐ Windows Autopilot
- ☐ an in-place upgrade

Question 28

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You have a Microsoft 365 subscription.

You need to ensure that administrators can manage the configuration settings for all the Windows 10 devices in your organization.

What should you configure?

- ☐ the Enrollment restrictions
- ☐ the mobile device management (MDM) authority
- ☐ the Exchange on-premises access settings
- ☐ the Windows enrollment settings

Licensed to Berend Post berend.post@it-university.nl

Question 29

You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Intune automatically.

What should you configure?

- ☐ Enrollment restrictions from the Intune admin center
- ☐ device enrollment managers from the Intune admin center
- ☐ MAM User scope from the Azure Active Directory admin center
- ☐ MDM User scope from the Azure Active Directory admin center

Question 30

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You create the Mobility (MDM and MAM) settings.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 31

HOTSPOT

You have several devices enrolled in Microsoft Intune.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	Group A
User2	Intune administrator	Group B
User3	*None*	*None*

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	Group A
2	Policy2	10	Group B
Default	All users	5	All users

You add User3 as a device enrollment manager in Intune.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Intune.	○	○
User2 can enroll a maximum of 10 devices in Intune.	○	○
User3 can enroll an unlimited number of devices in Intune.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 32

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to an Active Directory group.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 33

HOTSPOT

You have the Microsoft Azure Active Directory (Azure AD) users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

The device compliance policies in Intune are configured as shown in the following table.

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

You create a conditional access policy that has the following settings:

The Assignments settings are configured as follows:
Users and groups: Group1
Cloud apps: Microsoft Office 365 Exchange Online
Conditions: Include All device state, exclude Device marked as compliant
Access controls is set to Block access.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	◯	◯
User1 can access Microsoft Exchange Online from Device2.	◯	◯
User2 can access Microsoft Exchange Online from Device2.	◯	◯

Licensed to Berend Post berend.post@it-university.nl

Question 34

HOTSPOT

You create two device compliance policies for Android devices as shown in the following table.

Policy	Configuration	Action	Assigned to
Policy1	Require encryption of the data storage on the device.	Mark as noncompliant immediately.	Group1
Policy2	Require Google Play services.	Mark as noncompliant immediately.	Group2

You have the Android devices shown in the following table.

Name	User	Configuration
Android1	User1	Not encrypted
Android2	User2	Google Play services not configured
Android3	User3	Not encrypted Google Play services configured

The users belong to the groups shown in the following table.

User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The users enroll their device in Microsoft Intune.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The device of User1 is compliant.	○	○
The device of User2 is compliant.	○	○
The device of User3 is compliant.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 35

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.

Which role should you assign to the user?

- ☐ Cloud application administrator
- ☐ Application administrator
- ☐ Global administrator
- ☐ Service administrator

Question 36

You have a Microsoft 365 tenant.

You have a line-of-business application named App1 that users access by using the My Apps portal.

After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.

You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.

What should you do?

- ☐ From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.
- ☐ From Microsoft Cloud App Security, modify the impossible travel alert policy.
- ☐ From Microsoft Cloud App Security, create an app discovery policy.
- ☐ From the Azure Active Directory admin center, modify the conditional access policy.

Licensed to Berend Post berend.post@it-university.nl

Question 37

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Mobility (MDM and MAM) settings.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 38

Your company has a Microsoft 365 E3 subscription.

All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).

You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.

What should you use?

- ☐ Windows Autopilot
- ☐ Windows Update
- ☐ Subscription Activation
- ☐ an in-place upgrade

Licensed to Berend Post berend.post@it-university.nl

Question 39

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You create an Apple Configurator enrollment profile.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Case Study (7 questions)

Case Study
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Licensed to Berend Post berend.post@it-university.nl

Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements
Planned Changes

Contoso plans to implement the following changes:

Implement Microsoft 365.
Manage devices by using Microsoft Intune.
Implement Azure Advanced Threat Protection (ATP).
Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
User1 must be able to enroll all the New York office mobile devices in Intune.
Azure ATP sensors must be installed and must NOT use port mirroring.
Whenever possible, the principle of least privilege must be used.
A Microsoft Store for Business must be created.
Compliance Requirements

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question 40

HOTSPOT

You need to meet the technical requirements and planned changes for Intune.

What should you do? To answer, select the appropriate options is the answer area.

NOTE: Each correct selection is worth one point.

Licensed to Berend Post berend.post@it-university.nl

Answer Area

Settings to configure in Azure AD:	**Device settings** **Mobility (MDM and MAM)** **Organizational relationships** **User settings**
Settings to configure in Intune:	**Device compliance** **Device configuration** **Device enrollment** **Mobile Device Management Authority**

Licensed to Berend Post berend.post@it-university.nl

Question 41

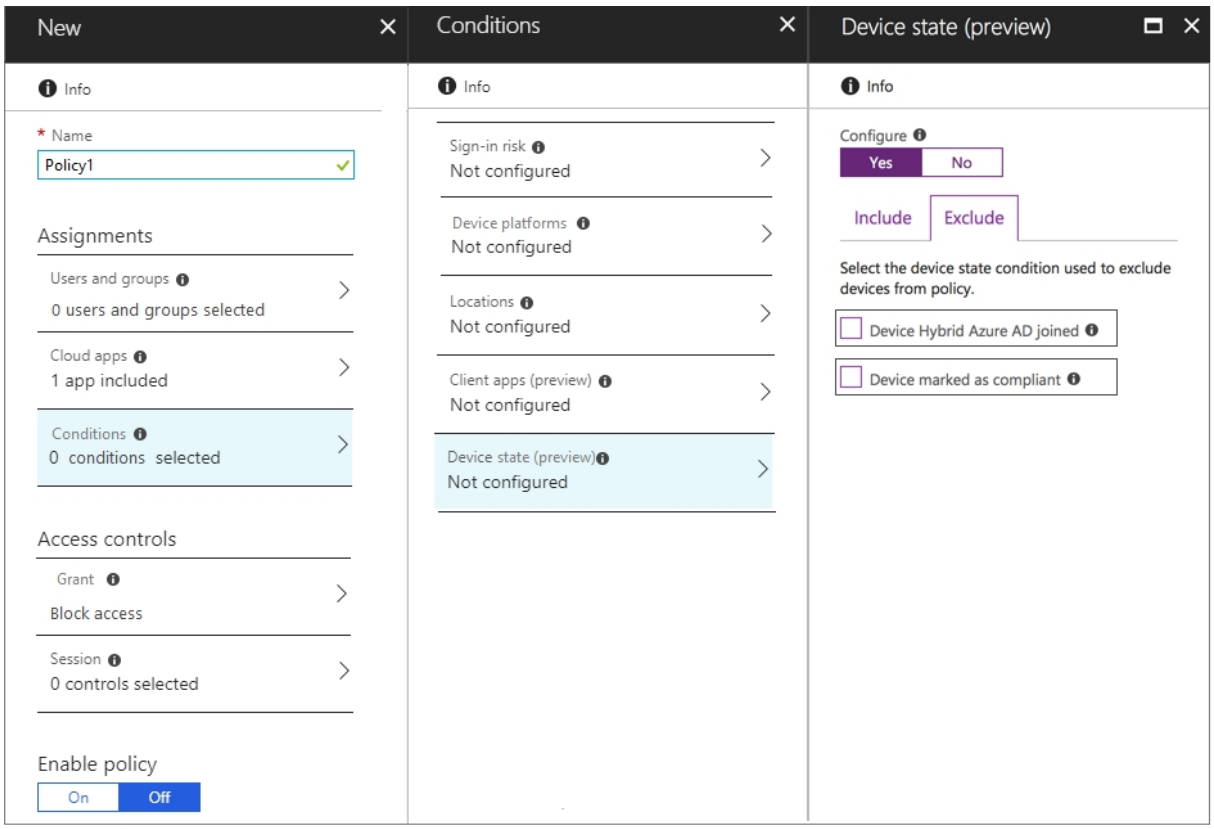
HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements.

You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Question 42

You need to create the Microsoft Store for Business.

Which user can create the store?

- ☐ User2
- ☐ User3
- ☐ User4
- ☐ User5

Licensed to Berend Post berend.post@it-university.nl

Question 43

HOTSPOT

You need to meet the Intune requirements for the Windows 10 devices.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

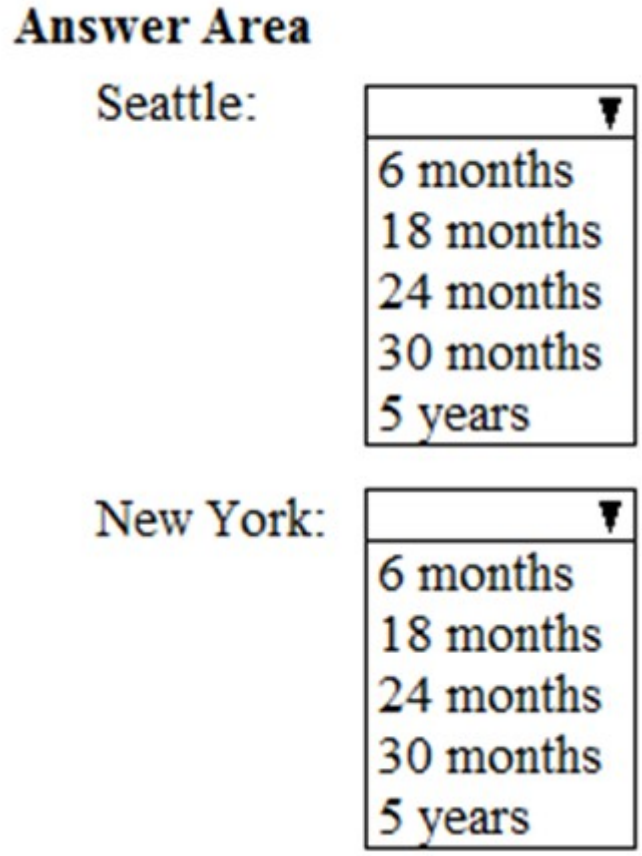
Licensed to Berend Post berend.post@it-university.nl

Question 44

HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Question 45

You need to ensure that User1 can enroll the devices to meet the technical requirements.

What should you do?

- ☐ From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- ☐ From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- ☐ From the Intune admin center, add User1 as a device enrollment manager.
- ☐ From the Intune admin center, configure the Enrollment restrictions.

Licensed to Berend Post berend.post@it-university.nl

Question 46

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

- ☐ 1
- ☐ 4
- ☐ 7
- ☐ 31

Licensed to Berend Post berend.post@it-university.nl

Case Study (1 questions)

Case Study
Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment
Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

ADatum identifies the following technical requirements:

Licensed to Berend Post berend.post@it-university.nl

Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question 47

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

- ☐ Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- ☐ Microsoft Azure Active Directory (Azure AD) Identity Protection
- ☐ Microsoft Azure Active Directory (Azure AD) conditional access policies
- ☐ Microsoft Azure Active Directory (Azure AD) authentication methods

Licensed to Berend Post berend.post@it-university.nl

Implement Microsoft 365 security and threat management

(35 questions)

Question 48

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a trusted location and a compliance policy

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 49

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 50

DRAG DROP

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Windows Defender Advanced Threat Protection (ATP). The solution must avoid installing software on the devices whenever possible.

Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Methods

- A Microsoft Azure ATP sensor
- A local script
- Microsoft Monitoring Agent

Answer Area

- Windows 8.1:
- Windows 10:
- Windows Server 2016:

Licensed to Berend Post berend.post@it-university.nl

Question 51

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

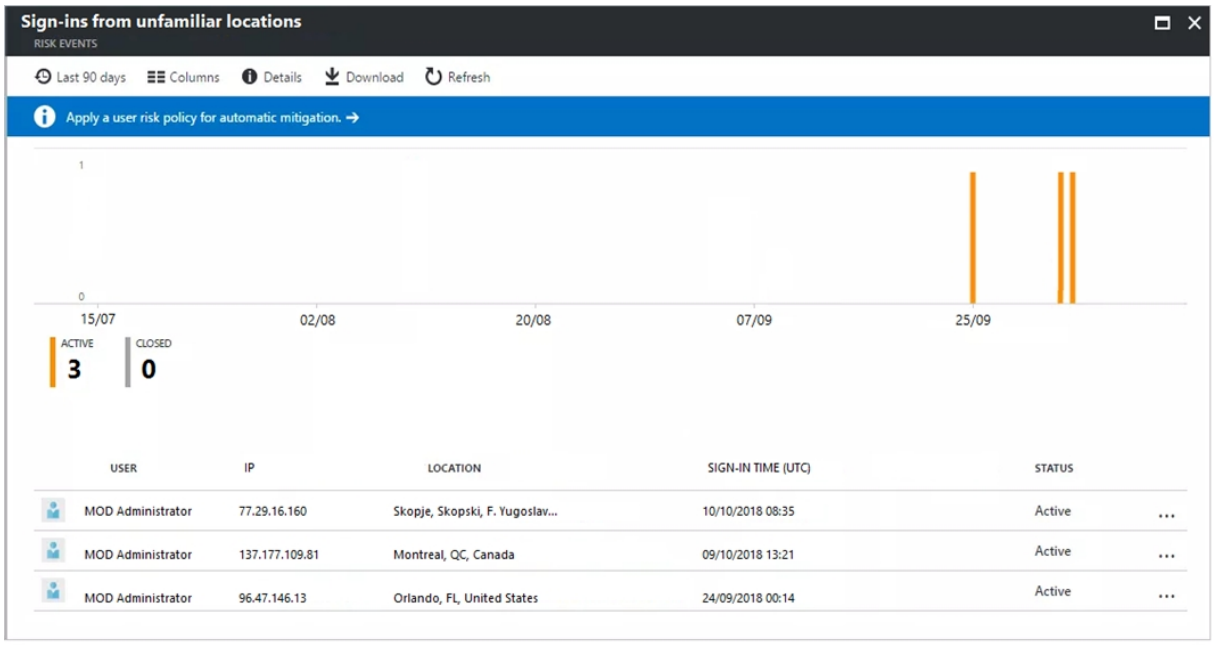
- ☐ From the Security & Compliance admin center, create a label and a label policy.
- ☐ From the Exchange admin center, create a mail flow rule.
- ☐ From the Security & Compliance admin center, start a message trace.
- ☐ From Exchange admin center, start a mail flow message trace.

Licensed to Berend Post berend.post@it-university.nl

Question 52

HOTSPOT

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [**answer choice**].

- named location in Azure AD
- sign-in risk policy
- user risk policy

To avoid generating alerts when signing in to the Montreal location, create [**answer choice**].

- a named location in Azure AD
- a sign-in risk policy
- a user risk policy

Licensed to Berend Post berend.post@it-university.nl

Question 53

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 54

Your company uses Microsoft Azure Advanced Threat Protection (ATP) and Windows Defender ATP.

You need to integrate Windows Defender ATP and Azure ATP.

What should you do?

- ☐ From Azure ATP, configure the notifications and reports.
- ☐ From Azure ATP, configure the data sources.
- ☐ From Windows Defender Security Center, configure the Machine management settings.
- ☐ From Windows Defender Security Center, configure the General settings.

Licensed to Berend Post berend.post@it-university.nl

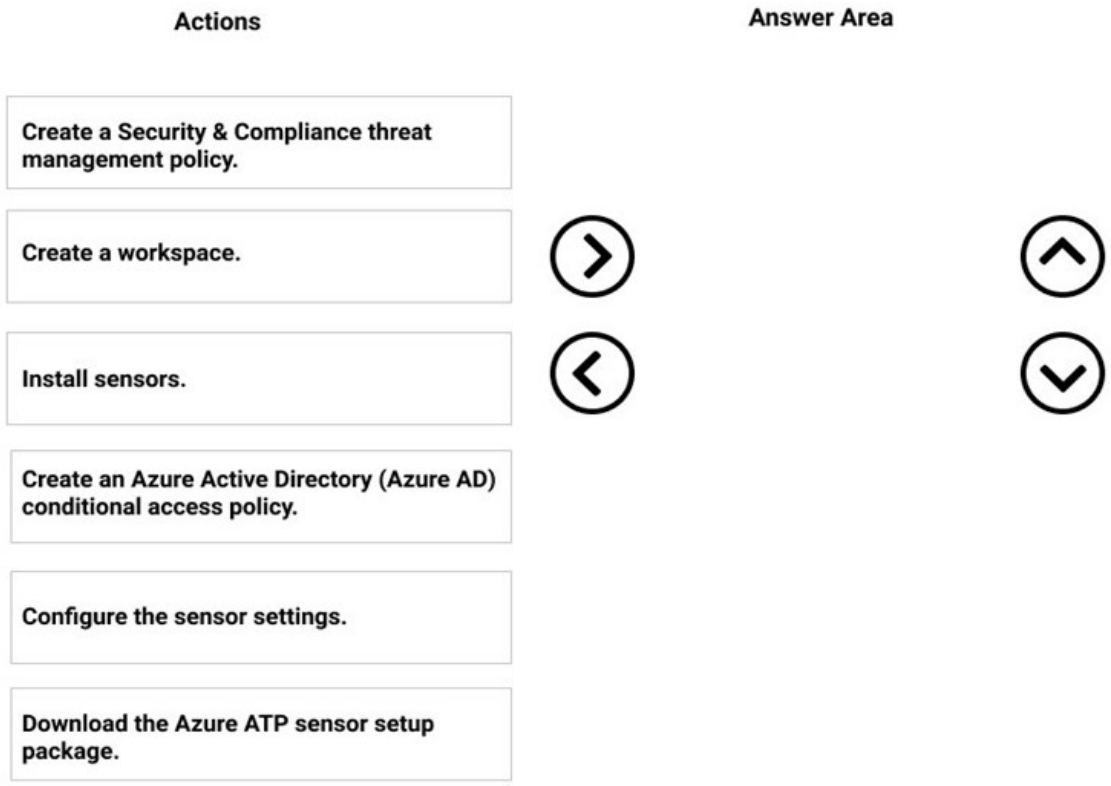
Question 55

DRAG DROP

You create a Microsoft 365 subscription.

You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Question 56

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

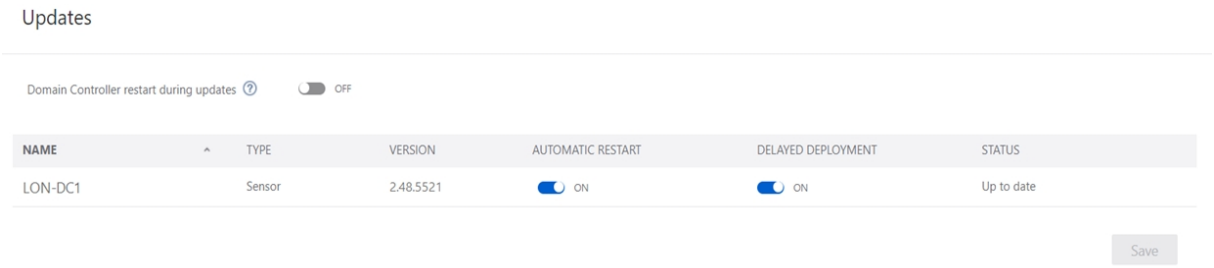
- ☐ From the Exchange admin center, create an in-place eDiscovery & hold.
- ☐ From the Security & Compliance admin center, create a safe attachments policy.
- ☐ From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- ☐ From the Security & Compliance admin center, create an alert policy.

Licensed to Berend Post berend.post@it-university.nl

Question 57

You implement Microsoft Azure Advanced Threat Protection (Azure ATP).

You have an Azure ATP sensor configured as shown in the following exhibit.



How long after the Azure ATP cloud service is updated will the sensor update?

- ☐ 1 hour
- ☐ 12 hours
- ☐ 48 hours
- ☐ 7 days
- ☐ 24 hours

Question 58

You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription.

You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.

What should you do first?

- ☐ Enable Microsoft Office 365 Cloud App Security.
- ☐ Deploy Windows Defender Advanced Threat Protection (Windows Defender ATP)
- ☐ Enable Microsoft Office 365 Analytics.

Licensed to Berend Post berend.post@it-university.nl

Question 59

HOTSPOT

You use Windows Defender Advanced Threat Protection (Windows Defender ATP).

You have the Windows Defender ATP machine groups shown in the following table.

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

You plan to onboard computers to Windows Defender ATP as shown in the following table.

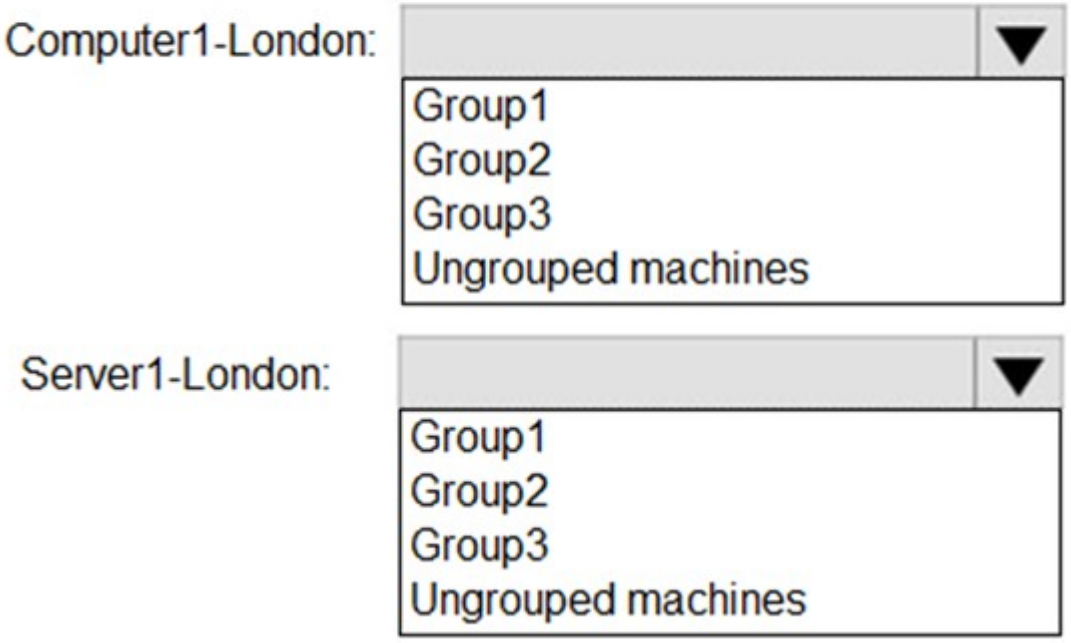
Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

To which machine group will each computer be added? To answer, select the appropriate options in the answer are.

NOTE: Each correct selection is worth one point.

Licensed to Berend Post berend.post@it-university.nl

Answer Area



Question 60

The users at your company use Dropbox Business to store documents. The users access Dropbox Business by using the MyApps portal.

You need to ensure that user access to Dropbox Business is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to a device that is not trusted.

What should you do?

- ☐ From the Device Management admin center, configure conditional access settings.
- ☐ From the Azure Active Directory admin center, configure the device settings.
- ☐ From the Azure Active Directory admin center, configure the organizational relationships settings.
- ☐ From the Device Management admin center, configure Exchange on-premises access settings.

Licensed to Berend Post berend.post@it-university.nl

Question 61

HOTSPOT

Your company uses Microsoft Cloud App Security.

You plan to integrate Cloud App Security and security information and event management (SIEM).

You need to deploy a SIEM agent on a server that runs Windows Server 2016.

What should you do? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First action to perform:

- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Question 62

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

The company purchases a cloud app named App1 that supports Microsoft Cloud App Security monitoring.

You configure App1 to be available from the My Apps portal.

You need to ensure that you can monitor App1 from Cloud App Security.

What should you do?

- ☐ From the Azure Active Directory admin center, create a conditional access policy.
- ☐ From the Azure Active Directory admin center, create an app registration.
- ☐ From the Device Management admin center, create an app protection policy.
- ☐ From the Device Management admin center, create an app configuration policy.

Licensed to Berend Post berend.post@it-university.nl

Question 63

You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain.

You need to enable Windows Defender Credential Guard on all the computers.

What should you do?

- ☐ From the Security & Compliance admin center, configure the DKIM signatures for the domain.
- ☐ From a domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.
- ☐ From the Security & Compliance admin center, create a device security policy.
- ☐ From a domain controller, create a Group Policy object (GPO) that enabled the Turn On Virtualization Based Security setting.

Question 64

Your network contains an on-premises Active Directory domain.

Your company has a security policy that prevents additional software from being installed on domain controllers.

You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP).

What should you do? More than one answer choice may achieve the goal. Select the BEST answer.

- ☐ Deploy an Azure ATP sensor, and then configure port mirroring.
- ☐ Deploy an Azure ATP sensor, and then configure detections.
- ☐ Deploy an Azure ATP standalone sensor, and then configure detections.
- ☐ Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Licensed to Berend Post berend.post@it-university.nl

Question 65

HOTSPOT

You have a new Microsoft 365 subscription.

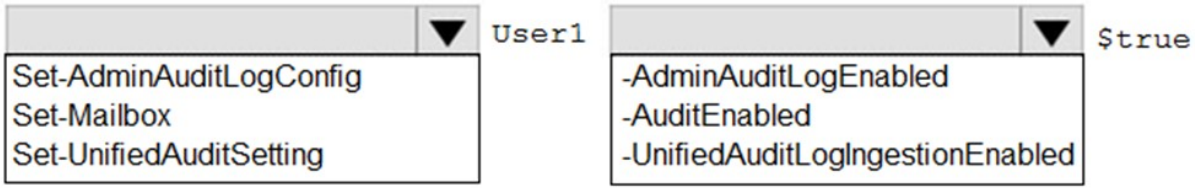
A user named User1 has a mailbox in Microsoft Exchange Online.

You need to log any changes to the mailbox folder permissions of User1.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Licensed to Berend Post berend.post@it-university.nl

Question 66

HOTSPOT

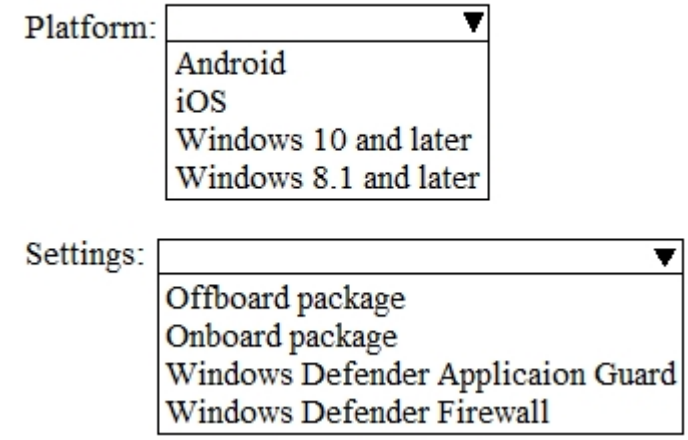
You have a Microsoft 365 subscription.

You need to implement Windows Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



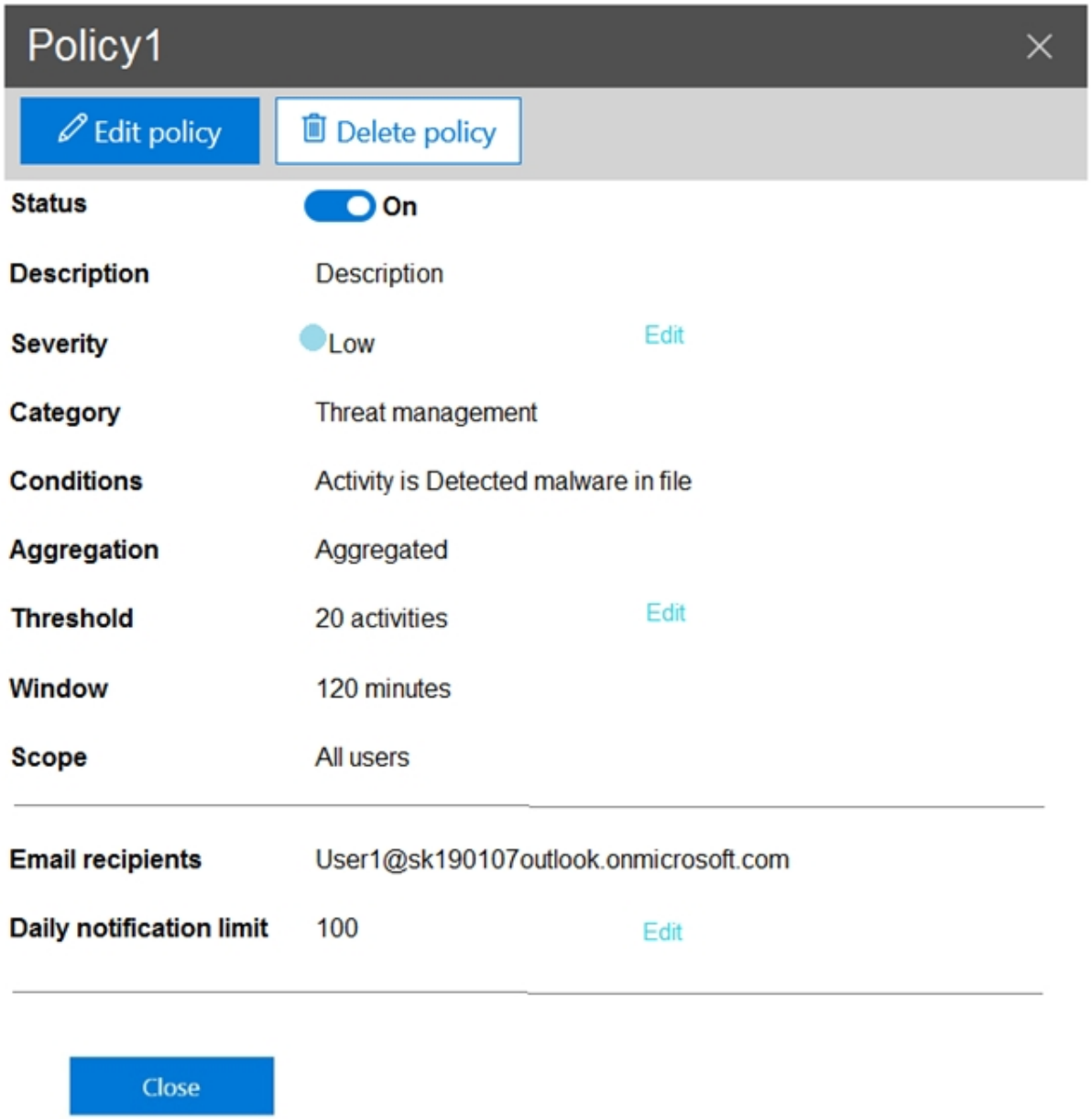
Licensed to Berend Post berend.post@it-university.nl

Question 67

HOTSPOT

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.

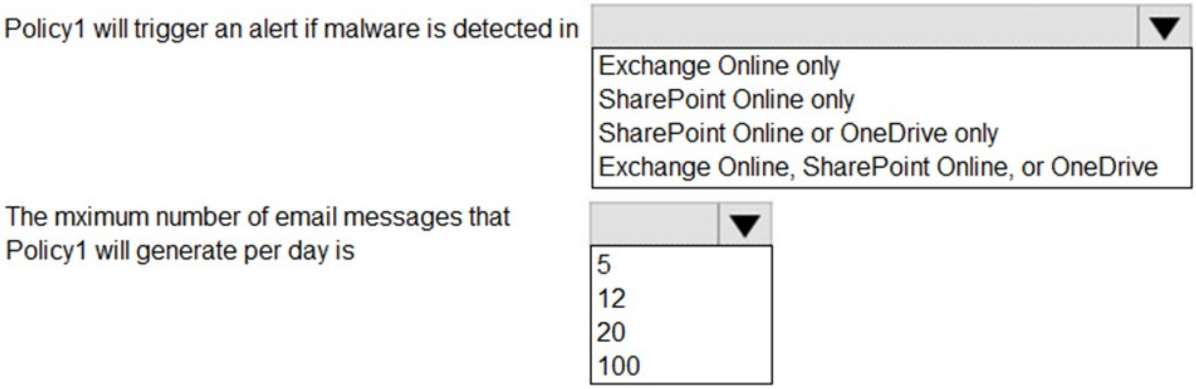


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Licensed to Berend Post berend.post@it-university.nl

Answer Area



Question 68

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.

You need to analyze the traffic logs.

What should you do from Microsoft Cloud App Security?

- ☐ Click Investigate, and then click Activity log.
- ☐ Click Control, and then click Policies. Create a file policy.
- ☐ Click Discover, and then click Create snapshot report.
- ☐ Click Investigate, and then click Files.

Licensed to Berend Post berend.post@it-university.nl

Question 69

HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	*Not applicable*

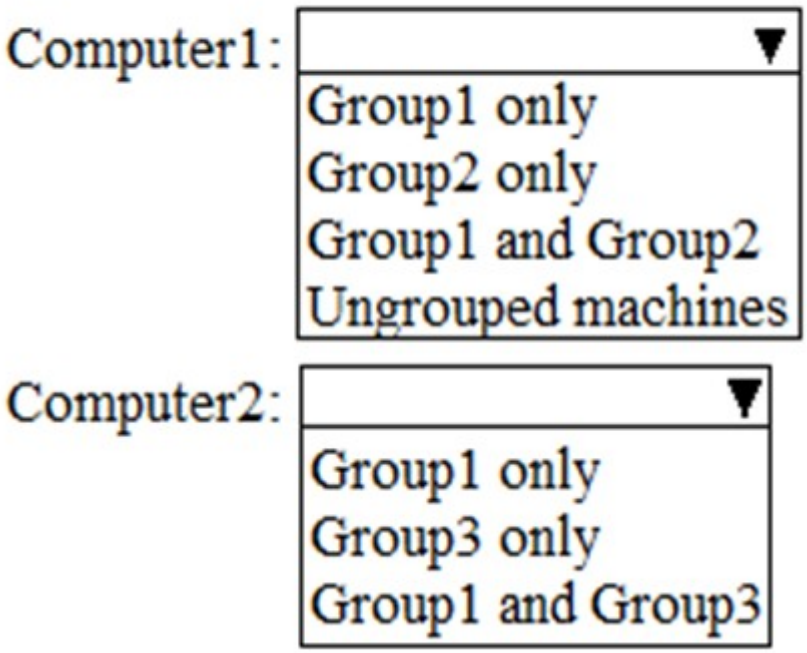
You onboard computers to Windows Defender ATP as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Licensed to Berend Post berend.post@it-university.nl

Question 70

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- ☐ From the Exchange admin center, create an in-place eDiscovery & hold.
- ☐ From the Security & Compliance admin center, create a data governance event.
- ☐ From the Exchange admin center, create an anti-malware policy.
- ☐ From the Exchange admin center, create a mail-flow rule.

Licensed to Berend Post berend.post@it-university.nl

Question 71

HOTSPOT

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 72

You have a Microsoft 365 subscription.

Your company purchases a new financial application named App1.

From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.

You need to prevent the missing information from affecting the score.

What should you configure from the Cloud Discover settings?

- ☐ Organization details
- ☐ Default behavior
- ☐ Score metrics
- ☐ App tags

Question 73

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.

Does this meet the goal?

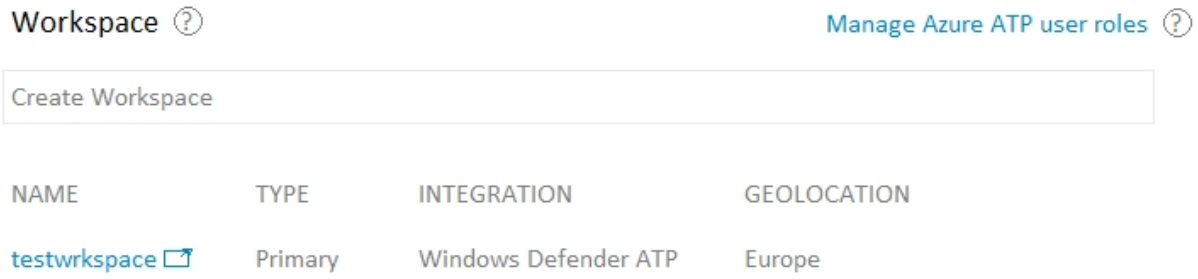
- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

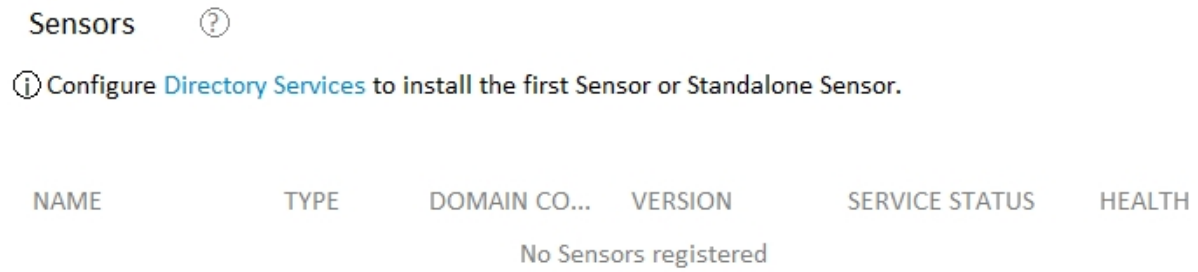
Question 74

DRAG DROP

You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)



The sensors settings for the workspace are configured as shown in the Sensors exhibit. (Click the Sensors tab.)



You need to ensure that Azure ATP stores data in Asia.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Modify the integration setting for the workspace.	
Delete the workspace.	
Regenerate the access keys.	
Create a new workspace.	
Modify the Azure ATP user roles.	

Licensed to Berend Post berend.post@it-university.nl

Question 75

Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender Advanced Threat Protection (ATP).

You need to create a filtered view that displays which Windows Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Windows Defender ATP?

- ☐ the threat intelligence API
- ☐ Automated investigations
- ☐ Threat analytics
- ☐ Advanced hunting

Licensed to Berend Post berend.post@it-university.nl

Question 76

HOTSPOT

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	*None*
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	*None*

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	○	○
User2 can sign in to Windows Defender Security Center.	○	○
User3 can view Device1 in Windows Defender Security Center.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 77

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a device configuration profile.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 78

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint admin center, you modify the sharing settings.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 79

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

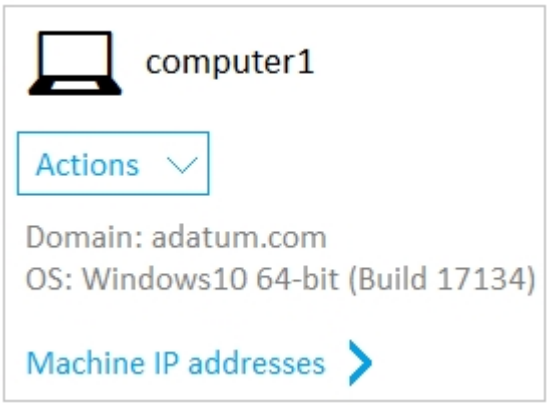
Question 80

HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP includes the machine groups shown in the following table.

Rank	Machine group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped machines (default)	*Not applicable*

You onboard a computer named computer1 to Windows Defender ATP as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of [**answer choice**].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of [**answer choice**].

- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped machines

Licensed to Berend Post berend.post@it-university.nl

Question 81

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP-related data to be stored in the United States.

You plan to onboard all the devices to Windows Defender ATP.

You need to store the Windows Defender ATP data in Europe.

What should you first?

- ☐ Create a workspace.
- ☐ Onboard a new device.
- ☐ Delete the workspace.
- ☐ Offboard the test devices.

Question 82

You have a Microsoft Azure Active Directory (Azure AD) tenant.

The organization needs to sign up for Microsoft Store for Business. The solution must use the principle of least privilege.

Which role should you assign to the user?

- ☐ Global administrator
- ☐ Cloud application administrator
- ☐ Application administrator
- ☐ Service administrator

Licensed to Berend Post berend.post@it-university.nl

Case Study (1 questions)

Case Study
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Licensed to Berend Post berend.post@it-university.nl

Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements
Planned Changes

Contoso plans to implement the following changes:

Implement Microsoft 365.
Manage devices by using Microsoft Intune.
Implement Azure Advanced Threat Protection (ATP).
Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
User1 must be able to enroll all the New York office mobile devices in Intune.
Azure ATP sensors must be installed and must NOT use port mirroring.
Whenever possible, the principle of least privilege must be used.
A Microsoft Store for Business must be created.
Compliance Requirements

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question 83

On which server should you install the Azure ATP sensor?

- ☐ Server1
- ☐ Server2
- ☐ Server3
- ☐ Server4
- ☐ Server5

Licensed to Berend Post berend.post@it-university.nl

Case Study (1 questions)

Case Study
Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment
Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

Licensed to Berend Post berend.post@it-university.nl

ADatum identifies the following technical requirements:

Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question 84

You need to meet the technical requirement for large-volume document retrieval.

What should you create?

- ☐ an activity policy from Microsoft Cloud App Security
- ☐ a data loss prevention (DLP) policy from the Security & Compliance admin center
- ☐ a file policy from Microsoft Cloud App Security
- ☐ an alert policy from the Security & Compliance admin center

Licensed to Berend Post berend.post@it-university.nl

Manage Microsoft 365 governance and compliance

(59 questions)

Question 85

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Exchange admin center, you create a data loss prevention (DLP) policy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 86

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

Exempt apps: App2
Protected apps: App1
Windows Information Protection mode: Block
Network boundary: IPv4 range of: 192.168.1.1-192.168.1.255

You need to identify the apps from which you can open File1.abc.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can open File1.abc in App1.	○	○
You can open File1.abc in App2.	○	○
You can open File1.abc in App3.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 87

Your company has a Microsoft 365 subscription.

You implement Microsoft Azure Information Protection.

You need to automatically protect email messages that contain the word Confidential in the subject line.

What should you create?

- ☐ a mail flow rule from the Exchange admin center
- ☐ a message trace from the Security & Compliance admin center
- ☐ a supervision policy from the Security & Compliance admin center
- ☐ a sharing policy from the Exchange admin center

Licensed to Berend Post berend.post@it-university.nl

Question 88

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2

The domain contains the devices shown in the following table.

Name	Compliance status
Device1	Compliant
Device2	Noncompliant

The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.

Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	*None*	All device states	Device marked as compliant	Block access
Policy2	Group1	Group2	*None*	*None*	Block Access
Policy3	Group1	*None*	All device states	*None*	Grant access

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	○	○
User2 can access App1 from Device1.	○	○
User2 can access App1 from Device2.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 89

HOTSPOT

You have a Microsoft 365 subscription.

You have a group named Support. Users in the Support group frequently send email messages to external users.

The manager of the Support group wants to randomly review messages that contain attachments.

You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To meet the goal for the manager, create: [▼]
- A label policy
- A retention policy
- A supervisor policy
- An alert policy
- MyAnalytics

To review the messages, the manager must use: [▼]
- A message trace
- An eDiscovery case
- MyAnalytics
- Outlook Web App

Licensed to Berend Post berend.post@it-university.nl

Question 90

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

Your company implements Windows Information Protection (WIP).

You need to modify which users and applications are affected by WIP.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To modify which users are affected by WIP, configure:

- The Azure AD app registration
- The Azure AD device settings
- The MAM User scope
- The mobile device management (MDM) authority

To modify which applications are affected by WIP, configure:

- App configuration policies
- App protection policies
- Compliance policies
- Device configuration profiles

Question 91

You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

In the tenant, you create a user named User1.

You need to ensure that User1 can publish retention labels from the Security & Compliance admin center. The solution must use the principle of least privilege.

To which role group should you add User1?

- ☐ Security Administrator
- ☐ Records Management
- ☐ Compliance Administrator
- ☐ eDiscovery Manager

Licensed to Berend Post berend.post@it-university.nl

Question 92

Your company has a Microsoft 365 tenant.

The company sells products online and processes credit card information.

You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.

What should you use?

- ☐ a Security & Compliance data loss prevention (DLP) policy
- ☐ a Microsoft Cloud App Security access policy
- ☐ a Security & Compliance retention policy
- ☐ a Microsoft Cloud App Security file policy

Question 93

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint site.

What should you do?

- ☐ From the Security & Compliance admin center, create an alert policy.
- ☐ From the SharePoint site, create an alert.
- ☐ From the SharePoint admin center, modify the sharing settings.
- ☐ From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Licensed to Berend Post berend.post@it-university.nl

Question 94

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User2 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 95

You have a Microsoft 365 subscription.

You need to investigate user activity in Microsoft 365, including from where users signed in, which applications were used, and increases in activity during the past month. The solution must minimize administrative effort.

Which admin center should you use?

- ☐ Azure ATP
- ☐ Security & Compliance
- ☐ Cloud App Security
- ☐ Flow

Licensed to Berend Post berend.post@it-university.nl

Question 96

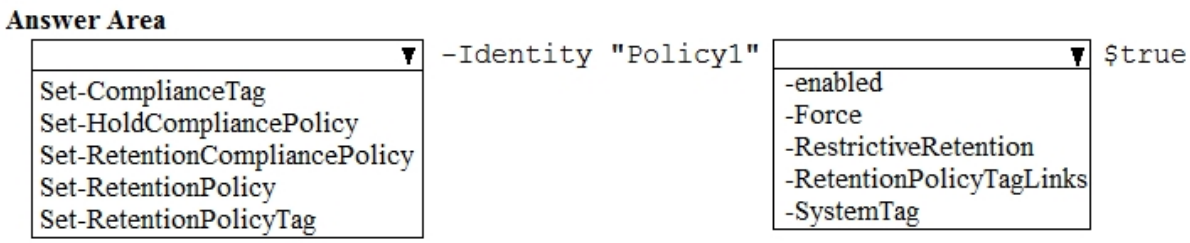
HOTSPOT

From the Security & Compliance admin center, you create a retention policy named Policy1.

You need to prevent all users from disabling the policy or reducing the retention period.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Licensed to Berend Post berend.post@it-university.nl

Question 97

HOTSPOT

You have a Microsoft 365 tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Azure AD role	Office 365 role group
User1	Application administrator	eDiscovery Administrator
User2	Application administrator	Organization Management
User3	Cloud application administrator	Global Administrator
User4	Compliance administrator	eDiscovery Manager

You have the eDiscovery cases shown in the following table.

Name	Created by
Case1	User1
Case2	User2
Case3	User3
Case4	User4

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can delete Case4.	○	○
User3 can add members to Case2.	○	○
User4 can close Case3.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 98

HOTSPOT

You have a Microsoft Office 365 subscription.

You need to delegate eDiscovery tasks as shown in the following table.

User	Task
User1	• Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content. • View the eDiscovery cases created by User1. • Configure case settings. • Place content on hold.
User2	• View the eDiscovery cases created by User1. • Export data from Advanced eDiscovery.

The solution must follow the principle of the least privilege.

To which role group should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:
- eDiscovery Administrator
- eDiscovery Manager
- Records Management
- Reviewer
- Security Administrator

User2:
- eDiscovery Administrator
- eDiscovery Manager
- Records Management
- Reviewer
- Security Administrator

Licensed to Berend Post berend.post@it-university.nl

Question 99

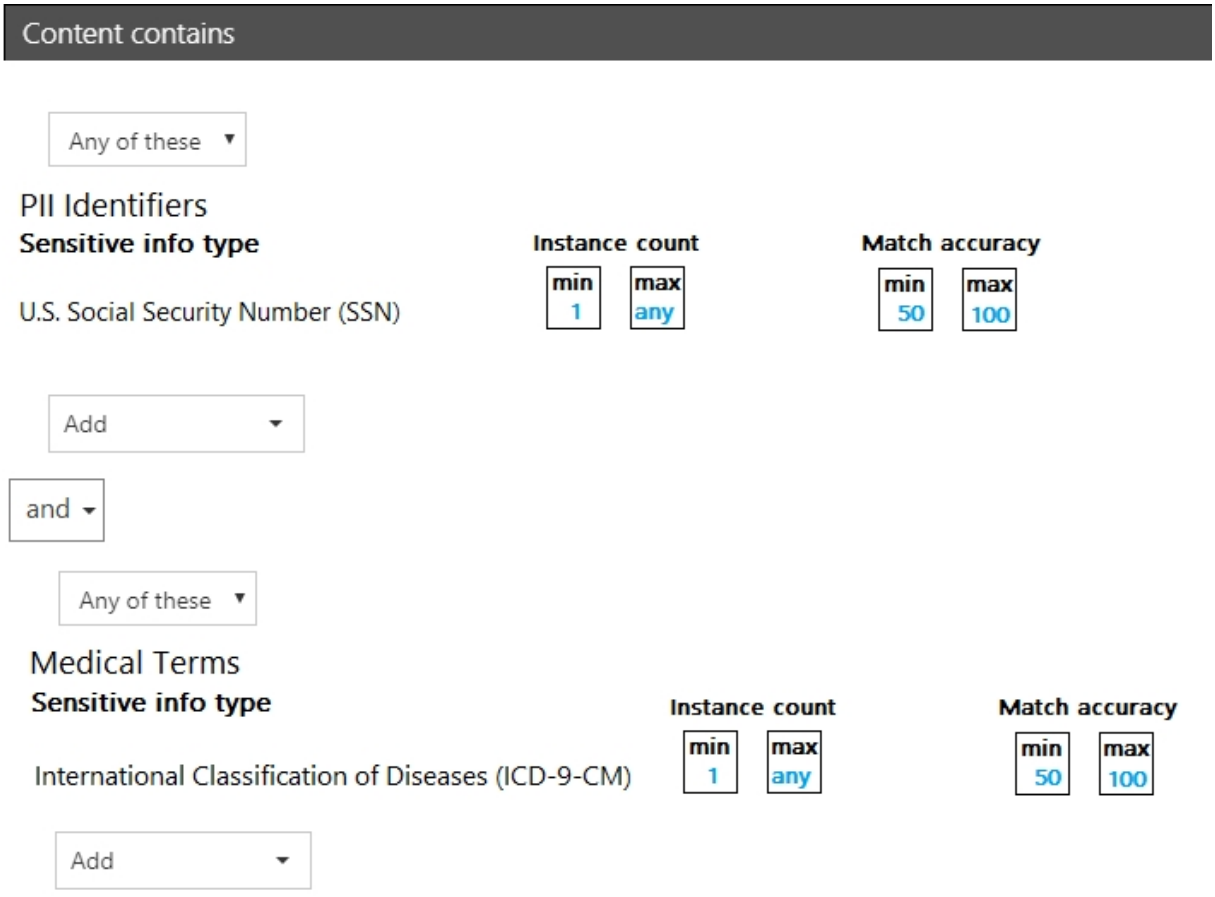
HOTSPOT

You have a data loss prevention (DLP) policy.

You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM). The solution must minimize the number of false positives.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.



Licensed to Berend Post berend.post@it-university.nl

Question 100

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-AzureRmRoleAssignment cmdlet with the appropriate parameters.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 101

You have a Microsoft 365 subscription.

You have a user named User1.

You need to ensure that User1 can place a hold on all mailbox content.

Which role should you assign to User1?

- ☐ eDiscovery Manager from the Security & Compliance admin center
- ☐ compliance management from the Exchange admin center
- ☐ User management administrator from the Microsoft 365 admin center
- ☐ Information Protection administrator from the Azure Active Directory admin center

Licensed to Berend Post berend.post@it-university.nl

Question 102

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign for Microsoft Store for Business.

The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator
User5	*None*	*None*

Microsoft Store for Business has the following Shopping behavior settings:

Allow users to shop is set to On
Make everyone a Basic Purchaser is set to Off

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

- ☐ User1, User2, User3, User4, and User5
- ☐ User1 only
- ☐ User1 and User2 only
- ☐ User3 and User4 only
- ☐ User1, User2, User3, and User4 only

Question 103

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content.

What should you do?

- ☐ Run the Set-AadrmOnboardingControlPolicy cmdlet.
- ☐ Run the Add-AadrmRoleBasedAdministrator cmdlet.
- ☐ Create an Azure Information Protection policy.
- ☐ Configure the protection activation status for Azure Information Protection.

Licensed to Berend Post berend.post@it-university.nl

Question 104

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-ComplianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 105

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You have three applications named App1, App2, and App3 that have the same file extensions.

Your company uses Windows Information Protection (WIP). WIP has the following configurations:

Windows Information Protection mode: Silent
Protected apps: App1
Exempt apps: App2

From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

You can open File1 from: [▼]
- App1 only
- App1 and App2 only
- App1 and App3 only
- App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for: [▼]
- App1 only
- App3 only
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

Licensed to Berend Post berend.post@it-university.nl

Question 106

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User3 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 107

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

- ☐ From the Security & Compliance admin center, create an eDiscovery case.
- ☐ From the Exchange admin center, create a mail flow rule.
- ☐ From the Security & Compliance admin center, start a message trace.
- ☐ From Microsoft Cloud App Security, create an access policy.

Licensed to Berend Post berend.post@it-university.nl

Question 108

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named User1 is a member of a dynamic group named Group1.

User1 reports that he cannot access documents shared to Group1.

You discover that User1 is no longer a member of Group1.

You suspect that an administrator made a change that caused User1 to be removed from Group1.

You need to identify which administrator made the change.

Which audit log activity should you search in the Security & Compliance admin center?

- ☐ Azure AD group administration activities – Removed member from group
- ☐ User administration activities – Updated user
- ☐ Azure AD group administration activities – Updated group

Question 109

HOTSPOT

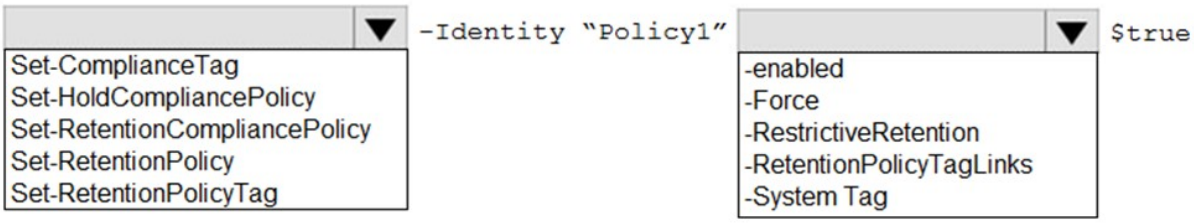
From the Security & Compliance admin center, you create a retention policy named Policy1.

You need to prevent all users from disabling the policy or reducing the retention period.

How should you configure the Azure PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Licensed to Berend Post berend.post@it-university.nl

Question 110

You plan to use the Security & Compliance admin center to import several PST files into Microsoft 365 mailboxes.

Which three actions should you perform before you import the data? Each correct answer presents part of the solution.

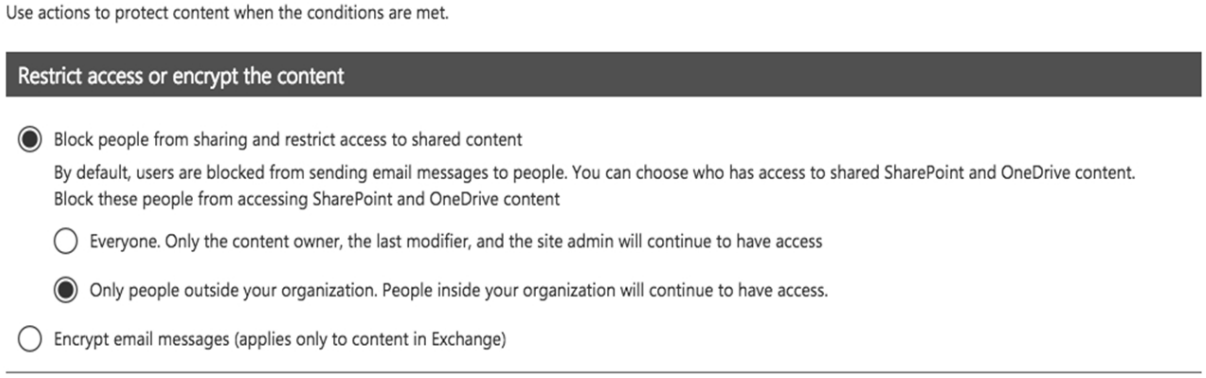
NOTE: Each correct selection is worth one point.

- ☐ From the Exchange admin center, create a public folder.
- ☐ Copy the PST files by using AzCopy.
- ☐ From the Exchange admin center, assign admin roles.
- ☐ From the Microsoft Azure portal, create a storage account that has a blob container.
- ☐ From the Microsoft 365 admin center, deploy an add-in.
- ☐ Create a mapping file that uses the CSV file format.

Question 111

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the Exhibit tab.)



You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.

What should you configure?

- ☐ an exception
- ☐ an action
- ☐ a condition
- ☐ a group

Licensed to Berend Post berend.post@it-university.nl

Question 112

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Azure portal, you create a Microsoft Azure Information Protection label and an Azure Information Protection policy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 113

Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
Opened a mailbox of which the user was not the owner
Reset a user password

What should you use?

- ☐ Microsoft Azure Activity Directory (Azure AD) audit logs
- ☐ Security & Compliance content search
- ☐ Microsoft Azure Activity Directory (Azure AD) sign-ins
- ☐ Security & Compliance audit log search

Licensed to Berend Post berend.post@it-university.nl

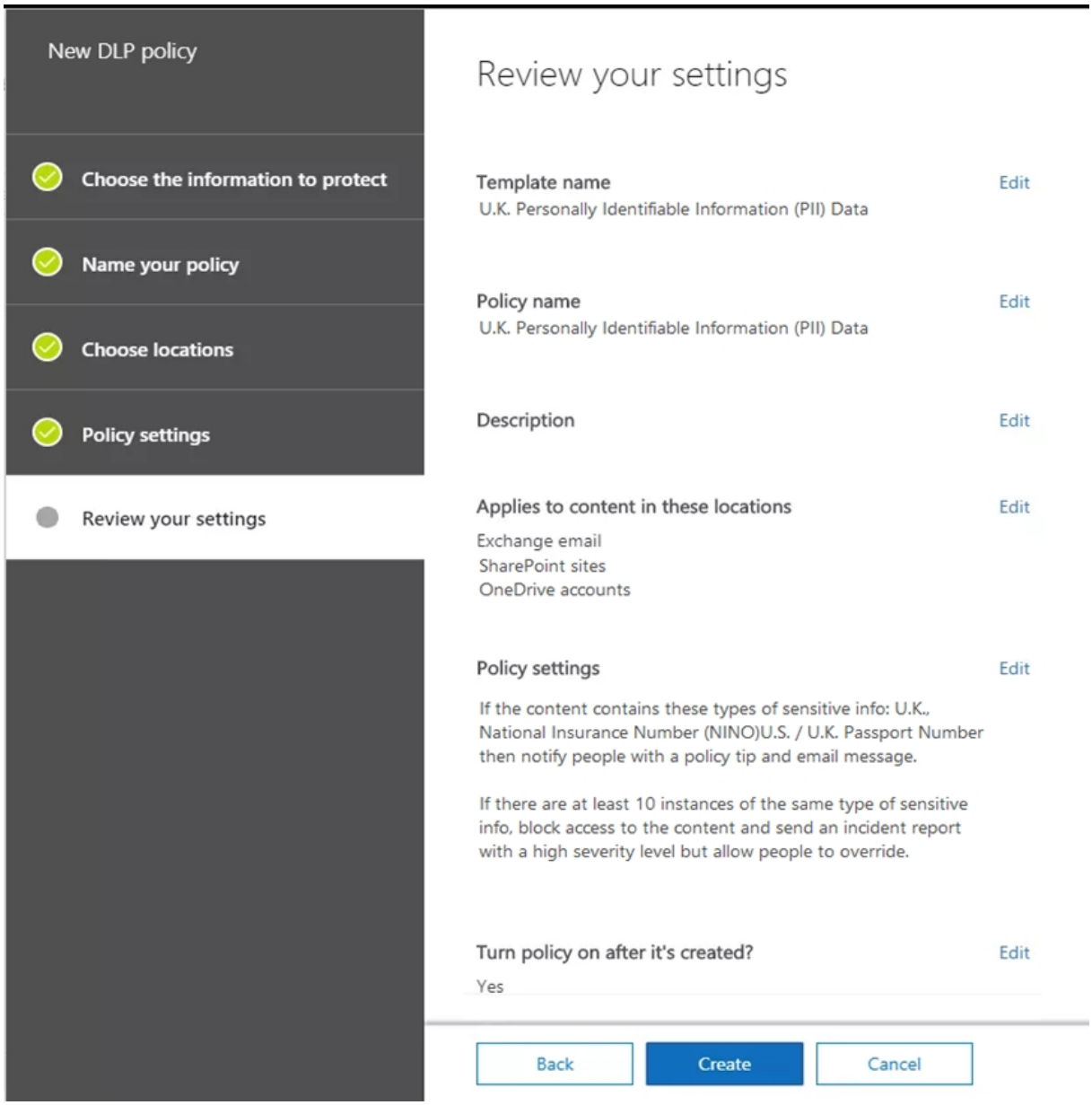
Question 114

HOTSPOT

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Licensed to Berend Post berend.post@it-university.nl

Answer Area

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be **[answer choice]**.

- allowed
- blocked without warning
- blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be **[answer choice]**.

- allowed
- blocked without warning
- blocked, but the user can override the policy

Question 115

You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS).

What should you do?

- ☐ From the Security & Compliance admin center, add SecAdmin1 to the eDiscovery Manager role group.
- ☐ From the Azure Active Directory admin center, add SecAdmin1 to the Security Reader role group.
- ☐ From the Security & Compliance admin center, add SecAdmin1 to the Compliance Administrator role group.
- ☐ From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

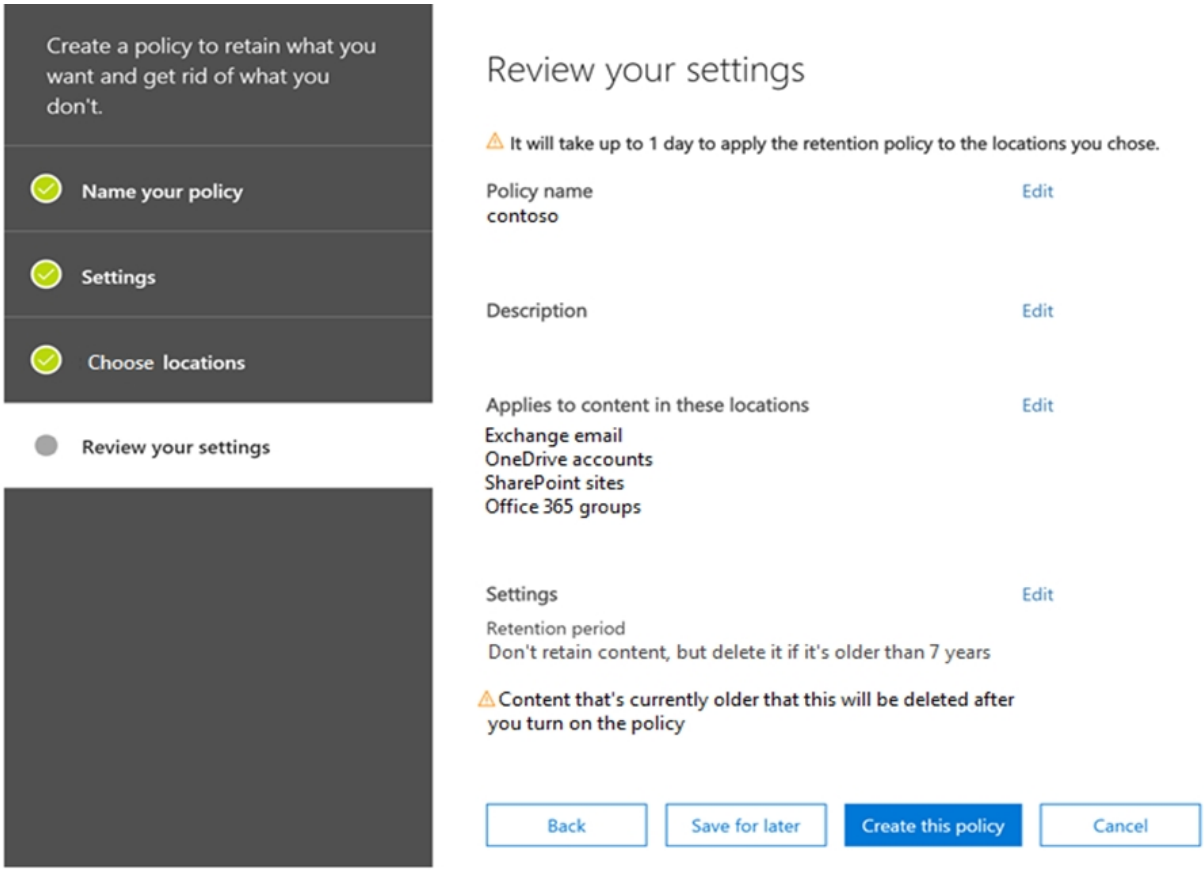
Licensed to Berend Post berend.post@it-university.nl

Question 116

HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft SharePoint files that are affected by the policy will be [**answer choice**].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [**answer choice**].

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Licensed to Berend Post berend.post@it-university.nl

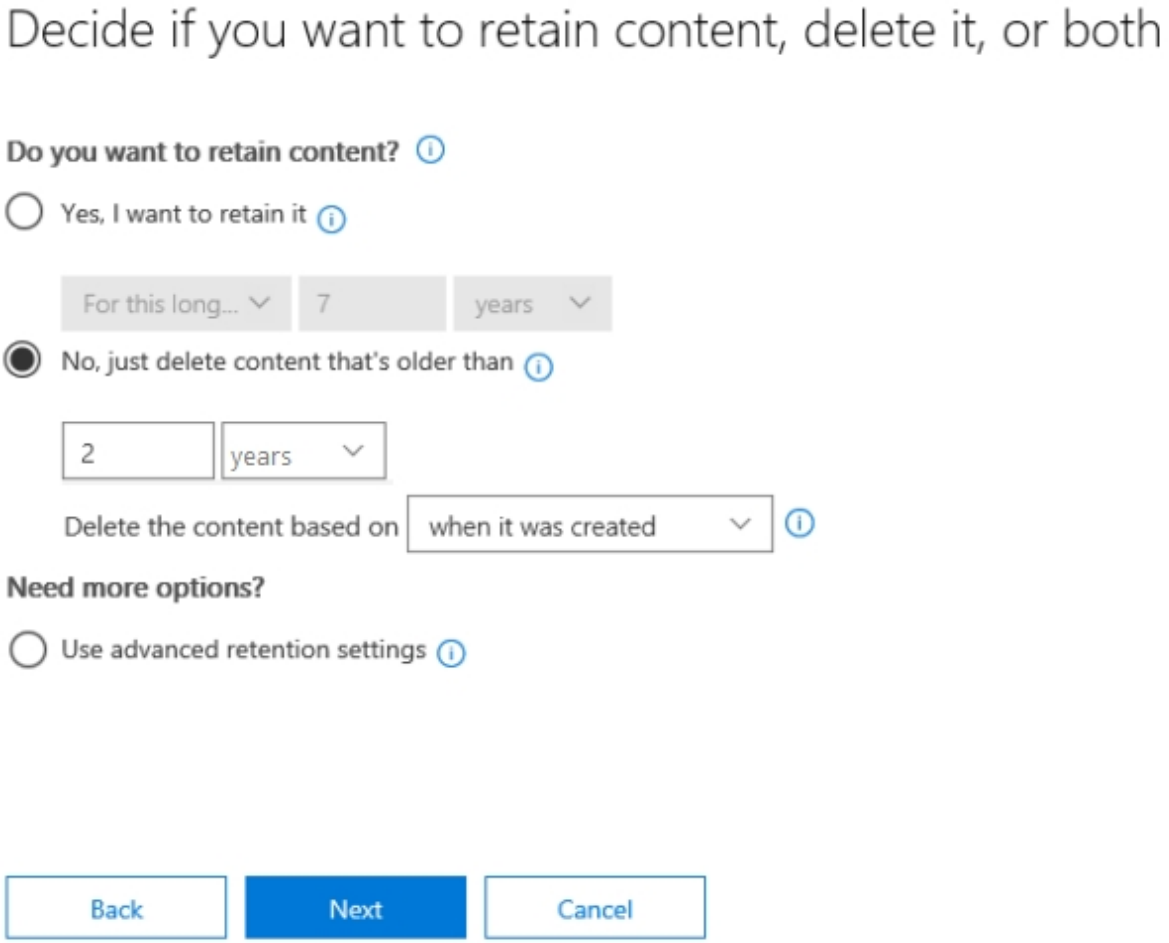
Question 117

HOTSPOT

You have retention policies in Microsoft 365 as shown in the following table.

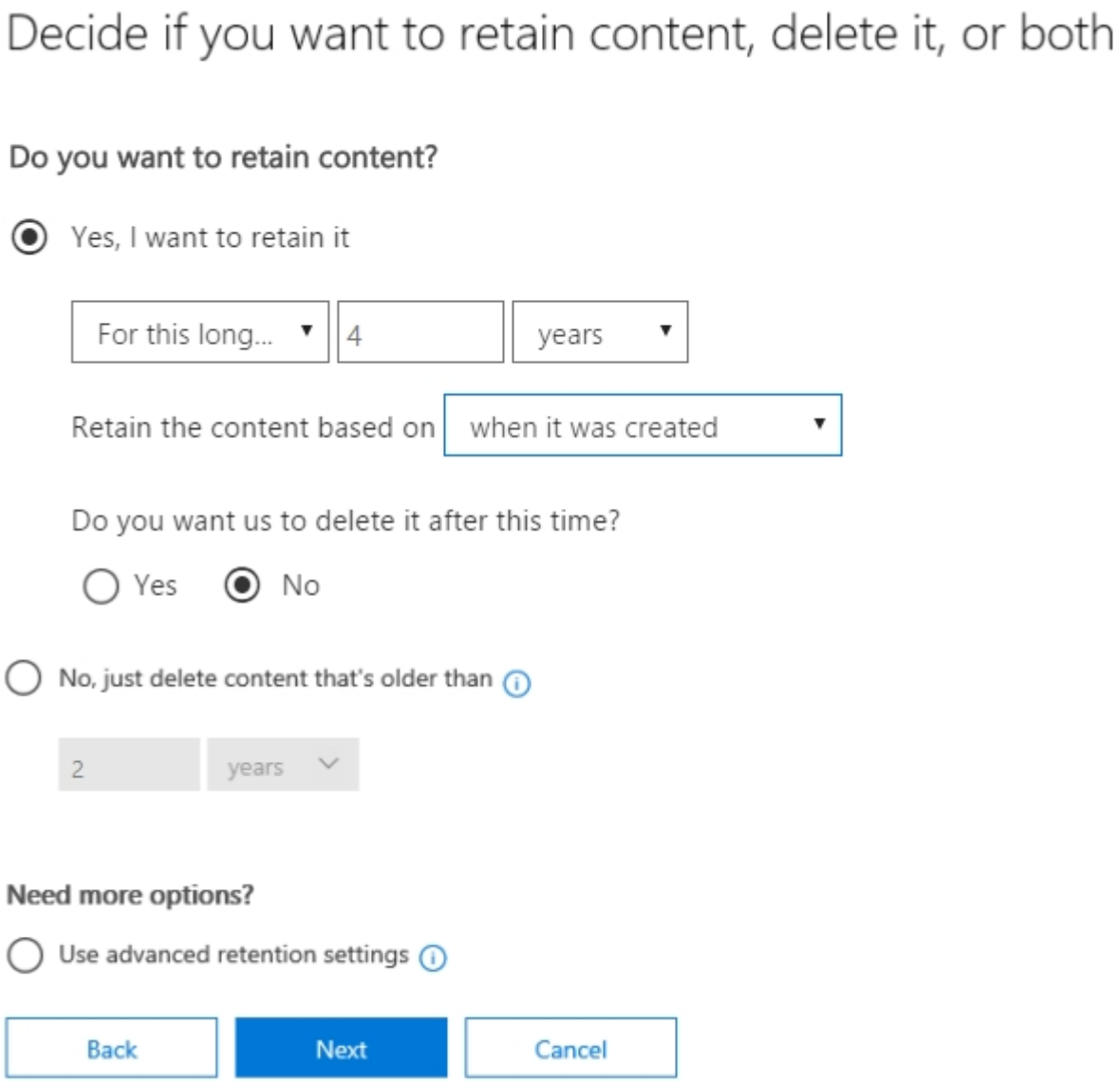
Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 is configured as shown in the Policy1 exhibit. (Click the Policy1 tab.)



Policy2 is configured as shown in the Policy2 exhibit. (Click the Policy2 tab.)

Licensed to Berend Post berend.post@it-university.nl



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 118

HOTSPOT

You purchase a new Microsoft 365 subscription.

You create 100 users who are assigned Microsoft 365 E3 licenses.

From the Security & Compliance admin center, you enable auditing.

Six months later, a manager sends you an email message asking the following questions:

Question1: Who created a team named Team1 14 days ago?
Question2: Who signed in to the mailbox of User1 30 days ago?
Question3: Who changed the site collection administrators of a site 60 days ago?

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
An audit log search from the Security & Compliance admin center will provide the answer to question 1.	○	○
An audit log search from the Security & Compliance admin center will provide the answer to question 2.	○	○
An audit log search from the Security & Compliance admin center will provide the answer to question 3.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 119

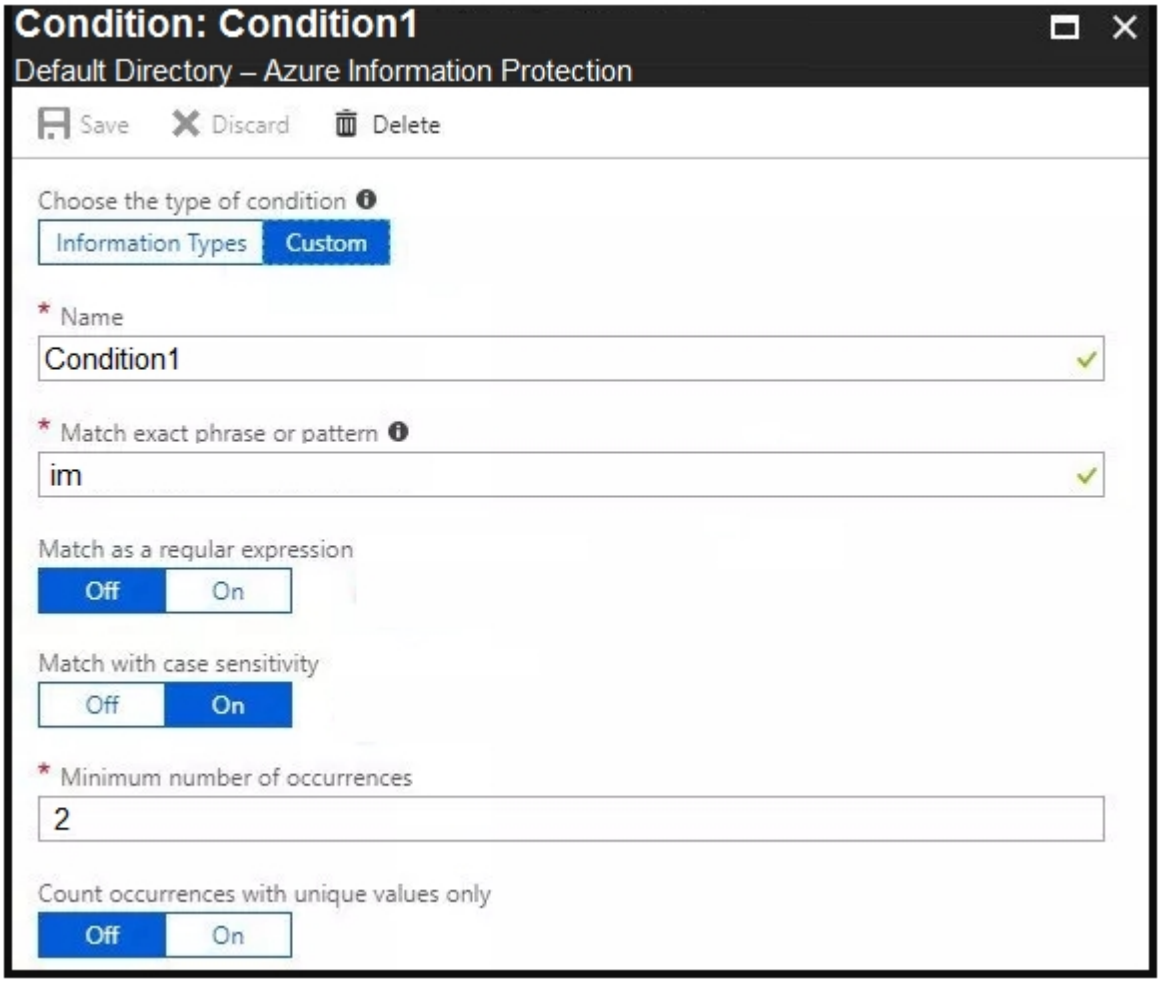
HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

A user named User1 has files on a Windows 10 device as shown in the following table.

Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination.
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Licensed to Berend Post berend.post@it-university.nl

Answer Area

Statements	Yes	No
Label1 applies to File1.docx.	○	○
Label1 applies to File2.docx.	○	○
Label1 applies to File3.docx.	○	○

Question 120

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Azure Active Directory admin center, you create a conditional access policy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 121

HOTSPOT

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

The company stores 2 TB of data in SharePoint Online document libraries.

The tenant has the labels shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

From the Azure portal, you activate unified labeling.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	◯	◯
Label2 can now be used as a retention label or an Azure Information Protection label.	◯	◯
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	◯	◯

Licensed to Berend Post berend.post@it-university.nl

Question 122

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User1 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 123

HOTSPOT

You create a Microsoft 365 subscription.

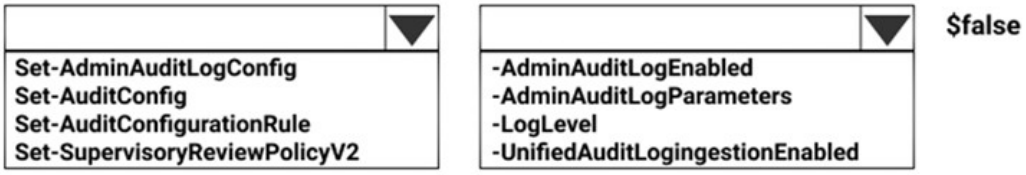
Your company's privacy policy states that user activities must NOT be audited.

You need to disable audit logging in Microsoft 365.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Licensed to Berend Post berend.post@it-university.nl

Question 124

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

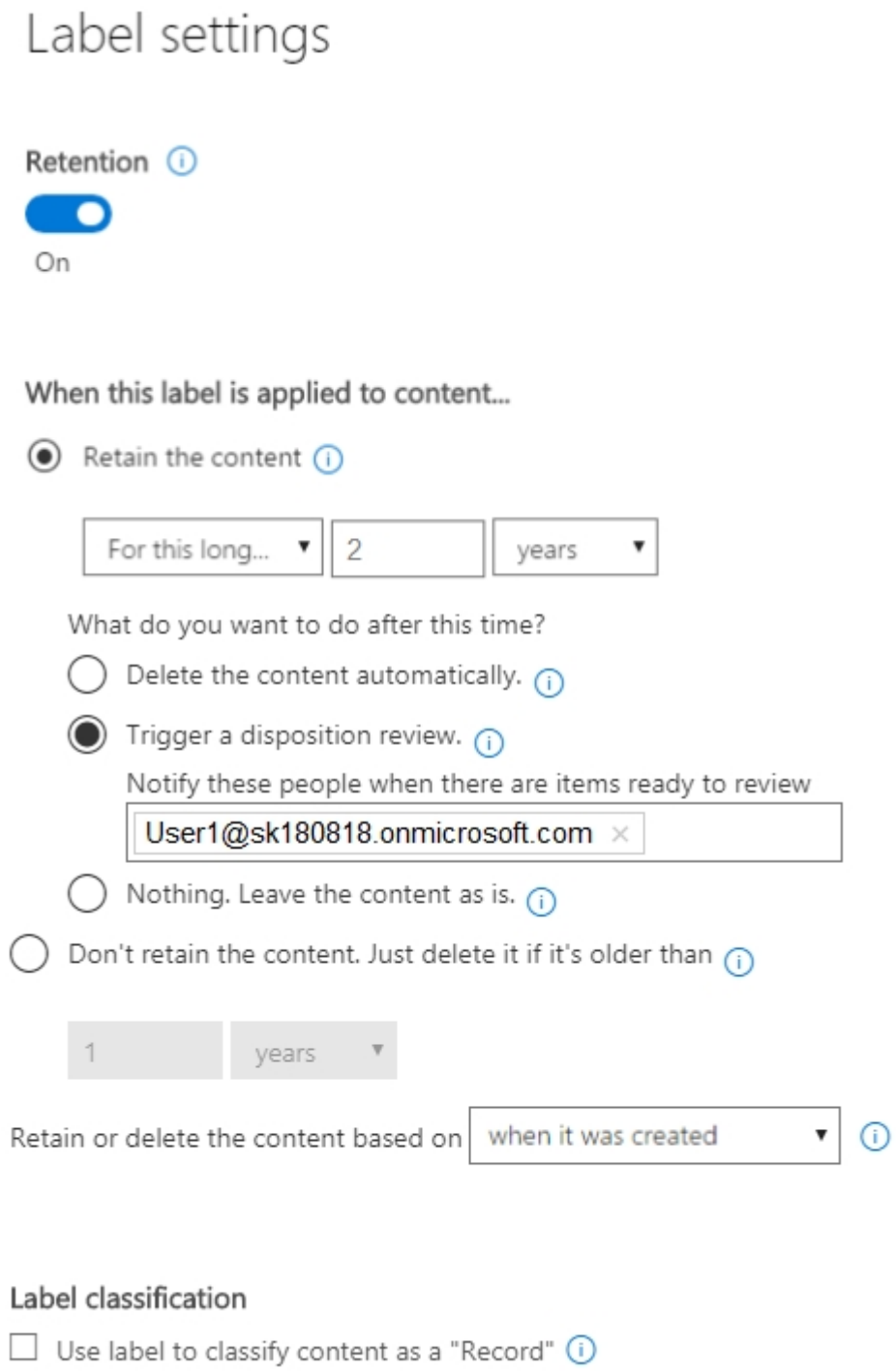
Three files were created on February 1, 2019, as shown in the following table.

Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

On March 1, 2019, you create two retention labels named Label1 and Label2.

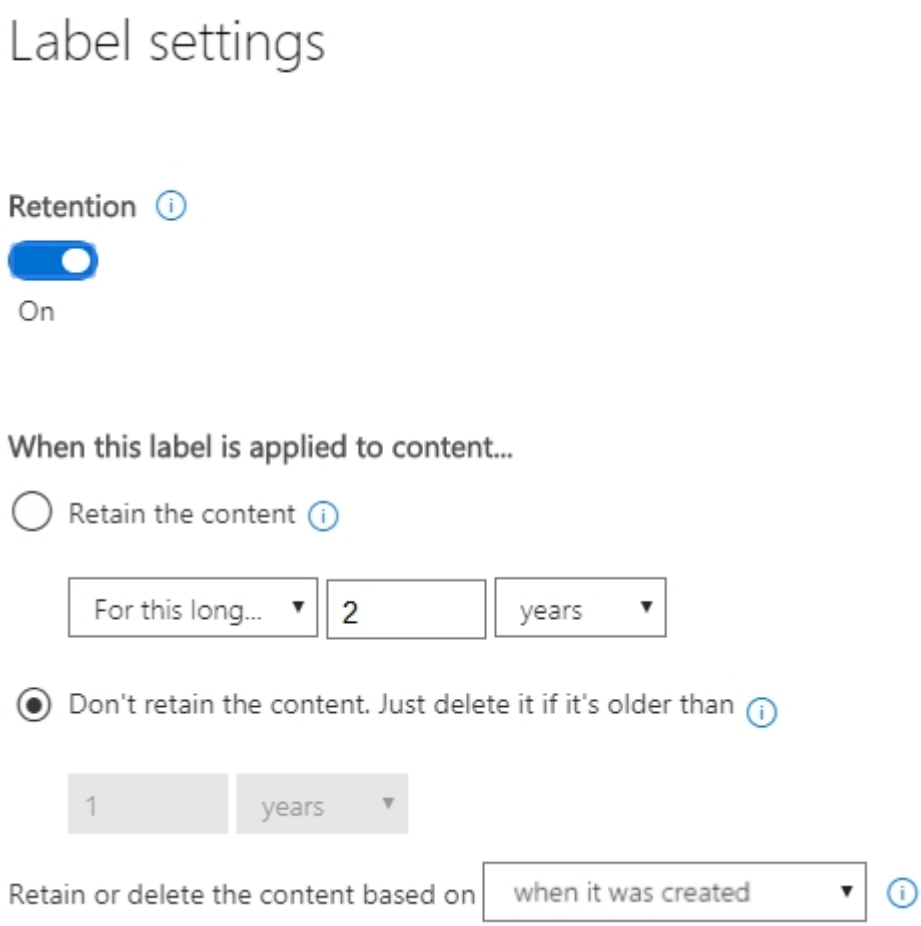
The settings for Lable1 are configured as shown in the Label1 exhibit. (Click the Label1 tab.)

Licensed to Berend Post berend.post@it-university.nl



The settings for Lable2 are configured as shown in the Label2 exhibit. (Click the Label2 tab.)

Licensed to Berend Post berend.post@it-university.nl



You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	○	○
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	○	○
File3 will be deleted automatically after February 1, 2021.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 125

You have a Microsoft 365 subscription.

Some users have iPads that are managed by your company.

You plan to prevent the iPad users from copying corporate data in Microsoft Word and pasting the data into other applications.

What should you create?

- ☐ A conditional access policy.
- ☐ A compliance policy.
- ☐ An app protection policy.
- ☐ An app configuration policy.

Question 126

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E3 license.

You enable auditing for your organization.

What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

- ☐ 2 years
- ☐ 1 year
- ☐ 30 days
- ☐ 90 days

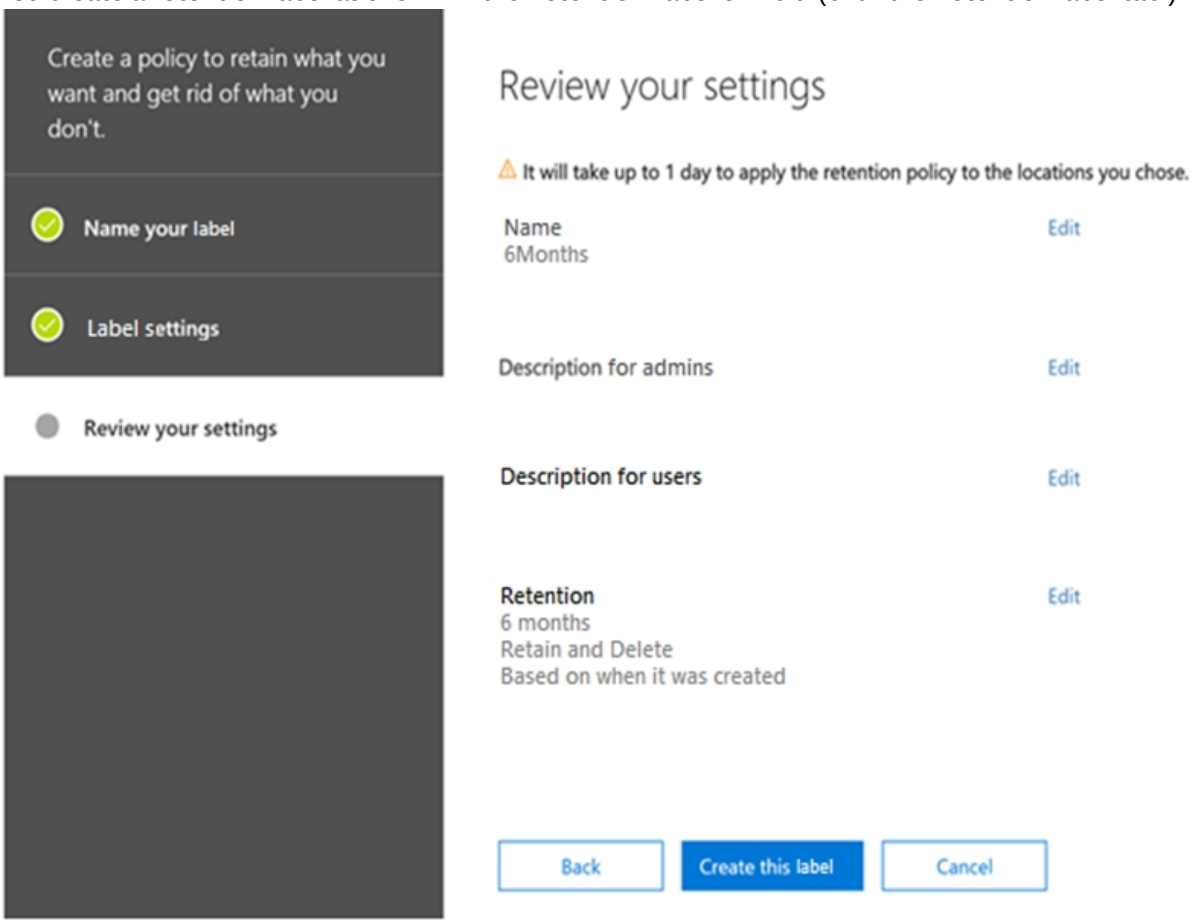
Licensed to Berend Post berend.post@it-university.nl

Question 127

HOTSPOT

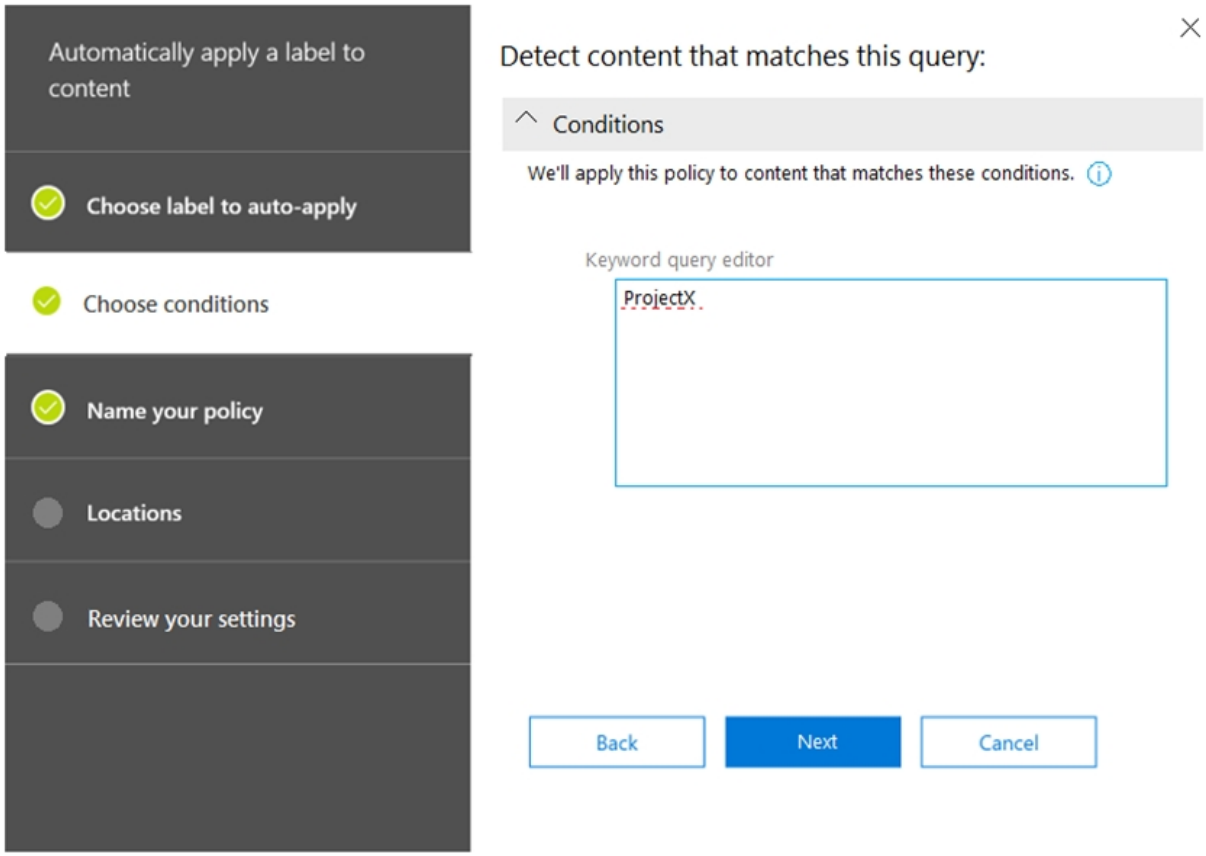
You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the RetentionLabel tab.)



You create a label policy as shown in the Label Policy Exhibit. (Click the Label Policy tab.)

Licensed to Berend Post berend.post@it-university.nl



The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	◯	◯
Any sent email message that contains the word ProjectX will be retained for six months.	◯	◯
Users are required to manually apply a label to email messages that contain the work ProjectX.	◯	◯

Licensed to Berend Post berend.post@it-university.nl

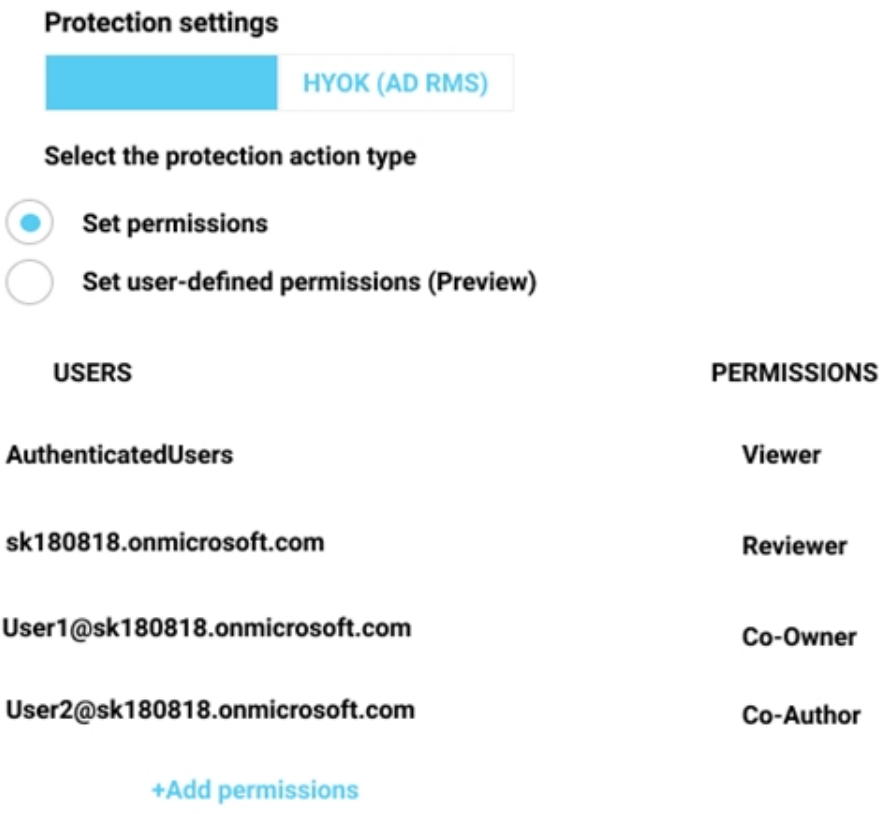
Question 128

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named sk180818.onmicrosoft.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@sk180818.onmicrosoft.com	Member
User2	User2@sk180818.onmicrosoft.com	Member
User3	User3@sk180818.onmicrosoft.com	Member
User4	User4@gmail.com	Guest

In Azure Information Protection, you create a label named Label1 as shown in the following exhibit.



Label1 is applied to a file named File1.

You send File1 as an email attachment to User1, User2, User3, and User4.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Licensed to Berend Post berend.post@it-university.nl

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User2 can modify File1.	◯	◯
User3 can print File1.	◯	◯
User4 can read File1.	◯	◯

Licensed to Berend Post berend.post@it-university.nl

Question 129

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User4 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 130

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users.

From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☐ An administrator creates a new Microsoft SharePoint site collection.
- ☐ An administrator creates a new mail flow rule.
- ☐ A user shares a Microsoft SharePoint folder with an external user.
- ☐ A user delegates permissions to their mailbox.
- ☐ A user purges messages from their mailbox.

Question 131

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the work ProjectX.

You need to export the results of the content search.

What do you need to download the report?

- ☐ a certification authority (CA) certificate
- ☐ an export key
- ☐ a password
- ☐ a user certificate

Licensed to Berend Post berend.post@it-university.nl

Question 132

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

- ☐ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 133

HOTSPOT

You have a Microsoft 365 subscription.

You are configuring permissions for Security & Compliance.

You need to ensure that the users can perform the tasks shown in the following table.

Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.

To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:
- Records Management
- Security Administrator
- Security Reader
- Supervisory Review

User2:
- Compliance Administrator
- Organization Management
- Security Administrator
- Security Reader
- Supervisory Review

Licensed to Berend Post berend.post@it-university.nl

Question 134

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of a mailbox.

You need to view the content of the mail messages found by the search as quickly as possible.

What should you select from the Content search settings?

- ☐ Export report
- ☐ Export results
- ☐ Re-run
- ☐ View results

Question 135

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

- ☐ the locations of the DLP policy
- ☐ the user overrides of the DLP policy rule
- ☐ the status of the DLP policy
- ☐ the conditions of the DLP policy rule

Licensed to Berend Post berend.post@it-university.nl

Question 136

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Cloud App Security admin center, you create an access policy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 137

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

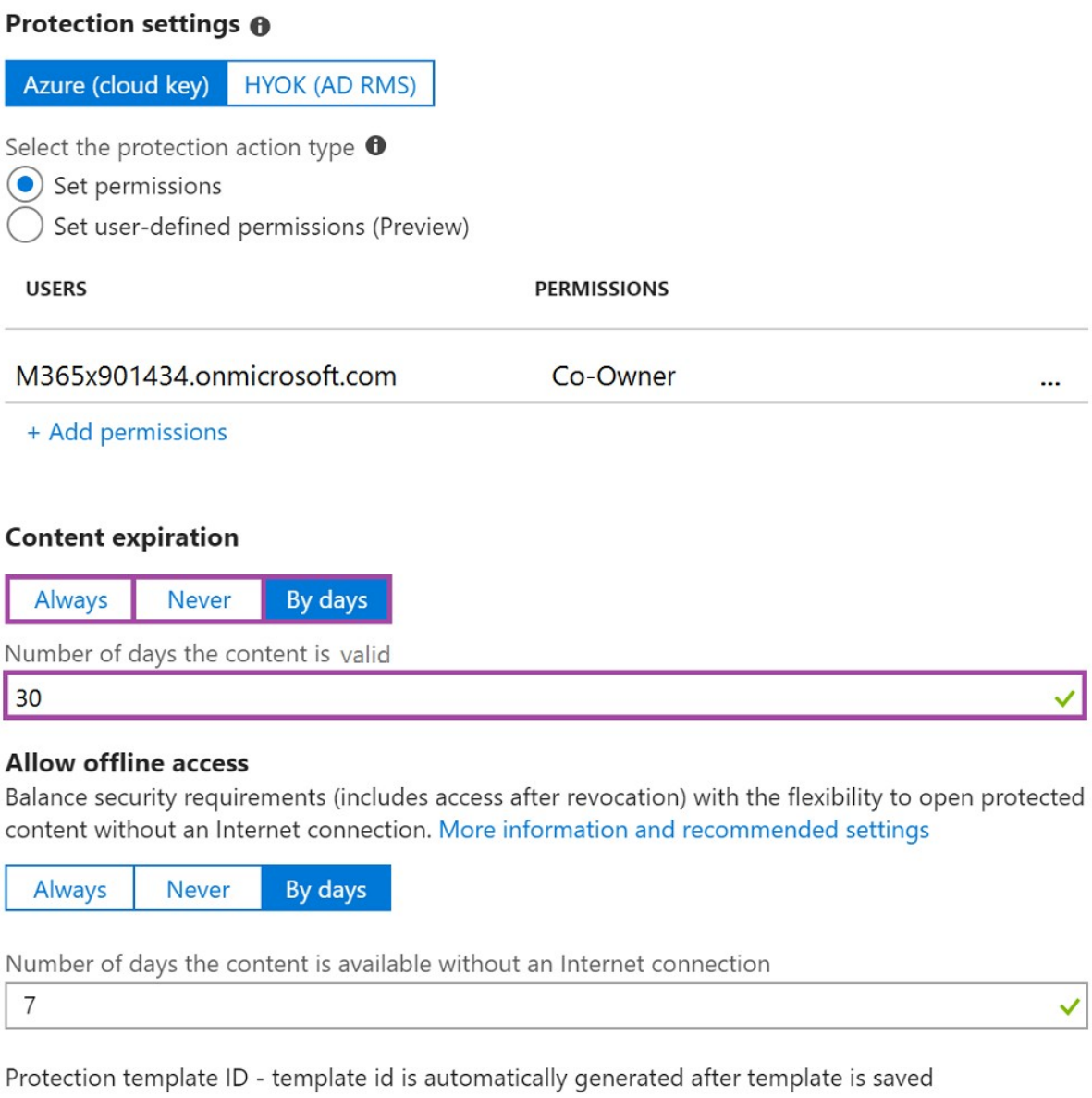
- ☐ incident reports
- ☐ actions
- ☐ exceptions
- ☐ user overrides

Licensed to Berend Post berend.post@it-university.nl

Question 138

HOTSPOT

You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Licensed to Berend Post berend.post@it-university.nl

Answer Area

If you copy the file from OneDrive to your internet connected computer, you [**answer choice**].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

If you email the document to a user outside your organization, the user [**answer choice**].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

Question 139

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded file based on the Confidential classification.

What should you do first?

- ☐ From the SharePoint admin center, configure hybrid search.
- ☐ From the SharePoint admin center, create a managed property.
- ☐ From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.
- ☐ From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

Question 140

You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint library.

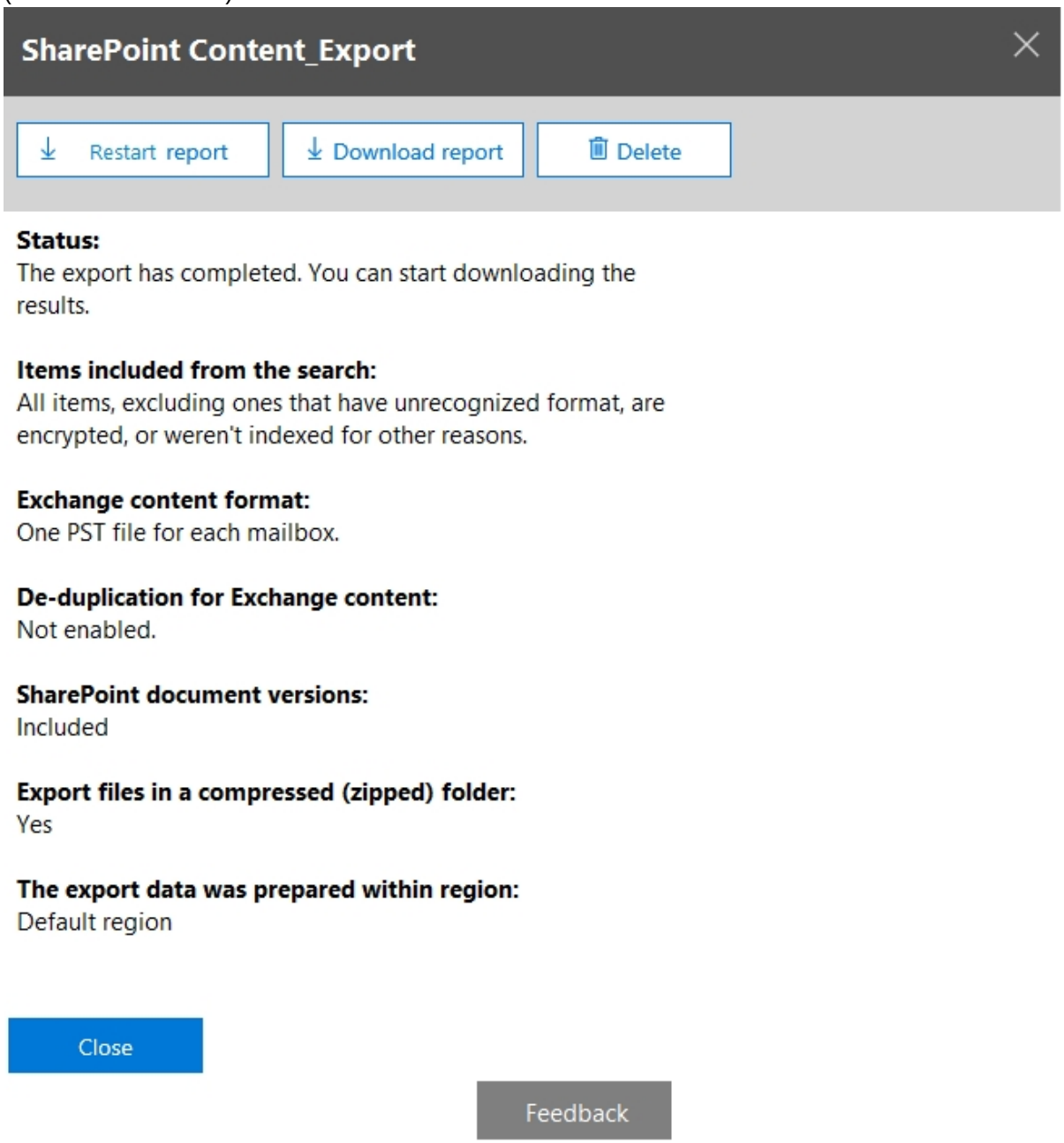
What should you do?

- ☐ From the SharePoint Online admin center, view the usage reports.
- ☐ From the Security & Compliance admin center, perform an audit log search.
- ☐ From the Microsoft 365 admin center, view the usage reports.
- ☐ From the Microsoft 365 admin center, view the properties of the user's user account.

Licensed to Berend Post berend.post@it-university.nl

Question 141

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



What will be excluded from the export?

- ☐ a 60-MB DOCX file
- ☐ a 12-MB BMP file
- ☐ a 5-KB RTF file
- ☐ a 100-MB VSDX file

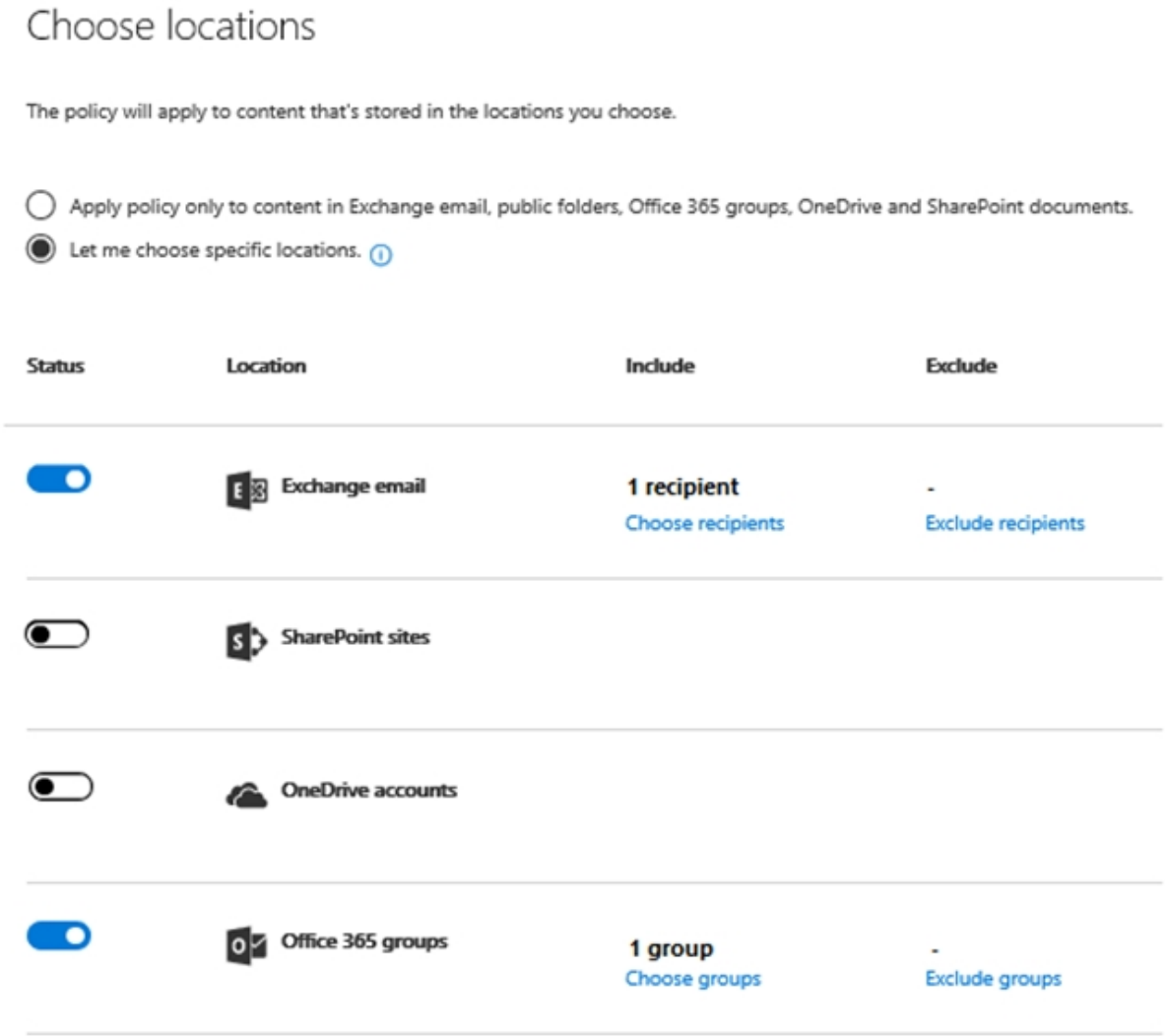
Licensed to Berend Post berend.post@it-university.nl

Question 142

HOTSPOT

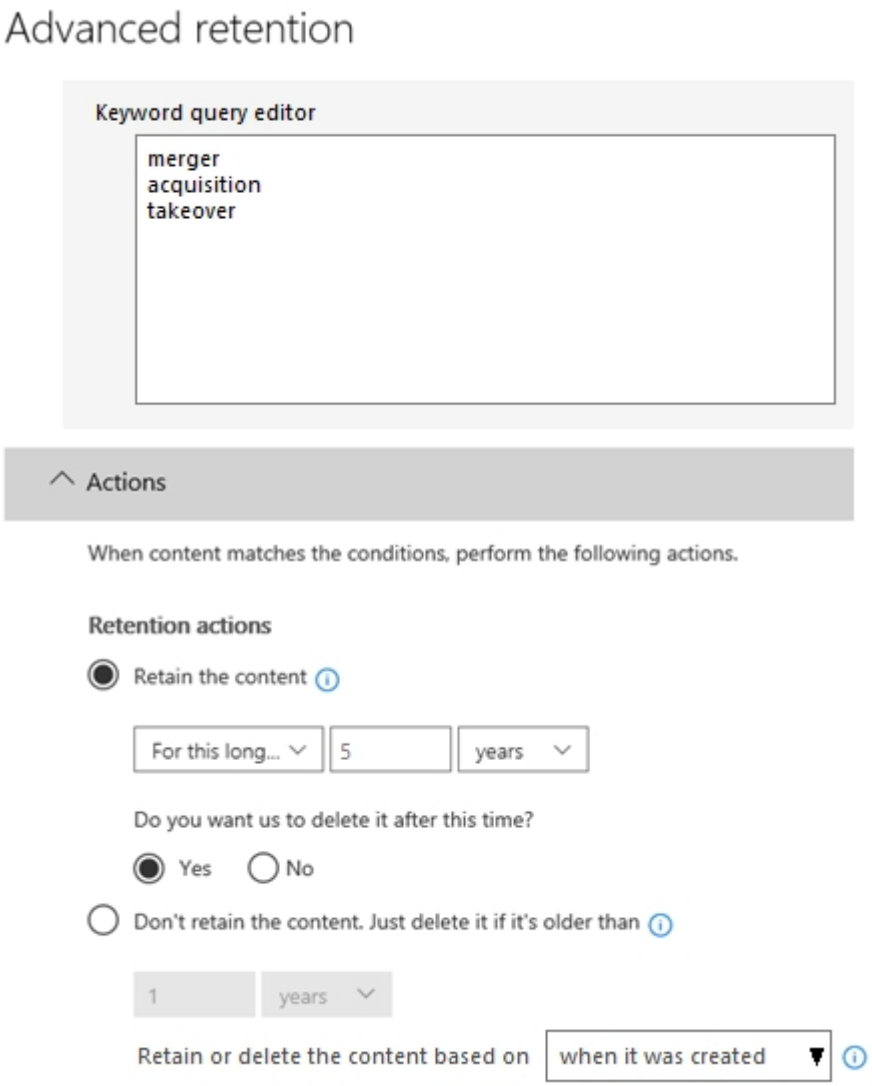
You have a Microsoft 365 subscription that contains all the user data.

You plan to create the retention policy shown in the Locations exhibit. (Click the Locations tab.)



You configure the Advanced retention settings as shown in the Retention exhibit. (Click the Retention tab.)

Licensed to Berend Post berend.post@it-university.nl



The locations specified in the policy include the groups shown in the following table.

Location	Include
Exchange email	A distribution group named LegalDL
Office 365 groups	A security group named LegalSG

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Licensed to Berend Post berend.post@it-university.nl

Answer Area

Statements	Yes	No
Any file stored in Microsoft SharePoint group library by a user in the LegalSG group will be stored for five years, and then deleted.	○	○
An email message that contains the word takeover and is sent by a user in the LegalDL group will be deleted automatically after five years.	○	○
If a new user is added to the LegalDL group next week, and the user sends an email message that contains the word takeover, the message will be deleted automatically after five years.	○	○

Licensed to Berend Post berend.post@it-university.nl

Question 143

HOTSPOT

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	**Policy name**	Managers	
	Description		
	Applied to	If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com	Edit
Impersonation	**Users to protect**	On - 3 User(s) specified	
	Protect all domains I own	On	
	Protect specific domains	On - 2 Domain(s) specified	
	Action > User impersonation	Move message to the recipients' Junk Email folders	
	Action > Domain impersonation	Delete the message before it's delivered	Edit
	Safety tips > User impersonation	Off	
	Safety tips > Domain impersonation	Off	
	Safety tips > Unusual characters	Off	
	Mailbox intelligence	Off	
Spoof	**Enable antispoofing protection**	On	
	Action	Quarantine the message	Edit
Advanced settings	**Advanced phishing thresholds**	3 - More Aggressive	Edit

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

If a message is identified as a domain impersonation, [**answer choice**].

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages are moved to the Junk Email folder

To reduce the likelihood of the impersonation policy generating false positives, configure [**answer choice**].

- Advanced phishing thresholds
- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

Licensed to Berend Post berend.post@it-university.nl

Case Study (1 questions)

Case Study
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Licensed to Berend Post berend.post@it-university.nl

Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements
Planned Changes

Contoso plans to implement the following changes:

Implement Microsoft 365.
Manage devices by using Microsoft Intune.
Implement Azure Advanced Threat Protection (ATP).
Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
User1 must be able to enroll all the New York office mobile devices in Intune.
Azure ATP sensors must be installed and must NOT use port mirroring.
Whenever possible, the principle of least privilege must be used.
A Microsoft Store for Business must be created.
Compliance Requirements

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question 144

You need to meet the compliance requirements for the Windows 10 devices.

What should you create from the Device Management admin center?

- ☐ a device compliance policy
- ☐ a device configuration profile
- ☐ an app protection policy

Licensed to Berend Post berend.post@it-university.nl

- ☐ an app configuration policy

Licensed to Berend Post berend.post@it-university.nl

Case Study (6 questions)

Case Study
Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment
Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

ADatum identifies the following technical requirements:

Licensed to Berend Post berend.post@it-university.nl

Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question 145

DRAG DROP

You need to meet the requirement for the legal department.

Which three actions should you perform in sequence from the Security & Compliance admin center? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Licensed to Berend Post berend.post@it-university.nl

Question 146

Which report should the New York office auditors view?

- ☐ DLP incidents
- ☐ Top Senders and Recipients
- ☐ DLP false positives and overrides
- ☐ DLP policy matches

Question 147

HOTSPOT

You need to meet the technical requirement for the SharePoint administrator.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

From the Security & Compliance admin center, perform a search by using: [Audit log / Data governance events / DLP policy matches / eDiscovery]

Filter by: [Activity / Detail / Item / User agent]

Question 148

You need to meet the technical requirement for the EU PII data.

What should you create?

- ☐ a data loss prevention (DLP) policy from the Security & Compliance admin center
- ☐ a data loss prevention (DLP) policy from the Exchange admin center
- ☐ a retention policy from the Exchange admin center
- ☐ a retention policy from the Security & Compliance admin center

Licensed to Berend Post berend.post@it-university.nl

Question 149

HOTSPOT

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of data sources: ▼
- 1
- 3
- 6

Minimum number of log collectors: ▼
- 1
- 3
- 6

Question 150

You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

- ☐ a data loss prevention (DLP) policy that contains a domain exception
- ☐ a Security & Compliance retention policy that detects content containing sensitive data
- ☐ a Security & Compliance alert policy that contains an activity
- ☐ a data loss prevention (DLP) policy that contains a user override

Licensed to Berend Post berend.post@it-university.nl