Vendor: Microsoft

Exam Code: MS-101

Exam Name: Microsoft 365 Mobility and Security

Version: DEMO

QUESTION 1
Case Study 1 - Contoso, Ltd
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 device
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 ES subscription.

Existing Environment
Requirement
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 are 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.

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.

You need to meet the compliance requirements for the Windows 10 devices.
What should you create from the Intune admin center?

A. a device compliance policy

B. a device configuration profile
C. an application policy
D. an app configuration policy

Answer: C
Explanation:
WIP can be configured with app protection policy.
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

QUESTION 2
Case Study 2 - A. Datum
Overview
Existing Environment
This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Current Infrastructure
A . Datum 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.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors. A.Datum uses and processes Personally Identifiable Information (PII).

Problem Statements
Requirements
A.Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.
Business Goals
A.Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.
A.Datum wants to minimize the cost of hardware and software whenever possible.

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

What should you include in the recommendation?

A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
B. Microsoft Azure Active Directory (Azure AD) Identity Protection
C. Microsoft Azure Active Directory (Azure AD) conditional access policies
D. Microsoft Azure Active Directory (Azure AD) authentication methods

Answer: B
Explanation:
Identity Protection is a pre-requisite of this kind of Conditional Access policy:
"Identity Protection - The scenario in this quickstart requires Identity Protection to be enabled. If you don't know how to enable Identity Protection, see Enabling Azure Active Directory Identity Protection."
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-sign-in-risk#:~:text=On%20the%20Conditional%20Access%20%2D%20Policies,%2Din%20risk%2C%20select%20Medium.

QUESTION 3
Case Study 3 - Litware, Inc

Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment
Existing Environment
The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.

Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com.
Audit log search is turned on for the litware.com tenant.

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements.

What should you do?

A. From the Microsoft 365 security center, configure an alert policy.
B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
C. From the Microsoft 365 admin center, configure a Briefing email.
D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

Answer: A
Explanation:
You create the planned DLP policies.
You need to configure notifications to meet the technical requirements.
Technical requirement:
A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.

By default, when you go to https://compliance.microsoft.com/homepage
you get to see 'Active alerts'
Therefore if you configure alert policy to create alert when DLP policy is triggered, that alert will appear in the Microsoft 365 compliance center = technical requirement met.

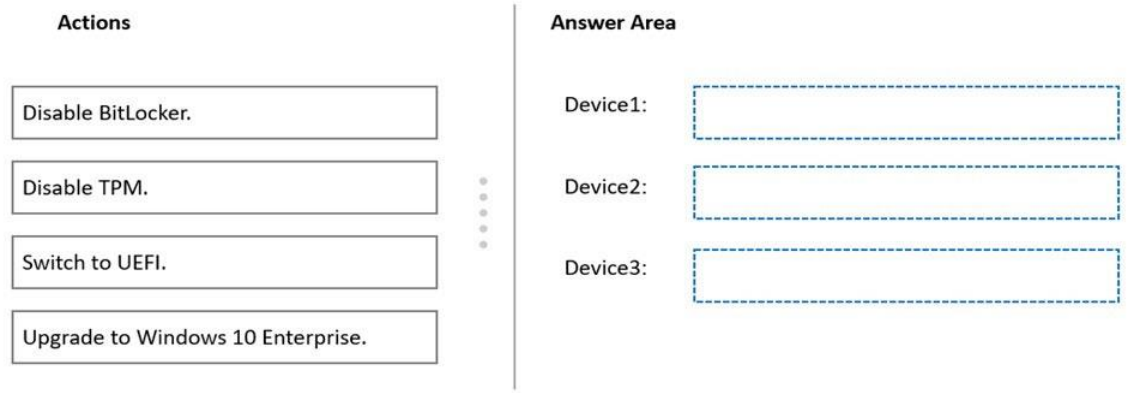
QUESTION 4
Drag and Drop Question

You have a Microsoft 365 subscription.
You have the devices shown in the following table.

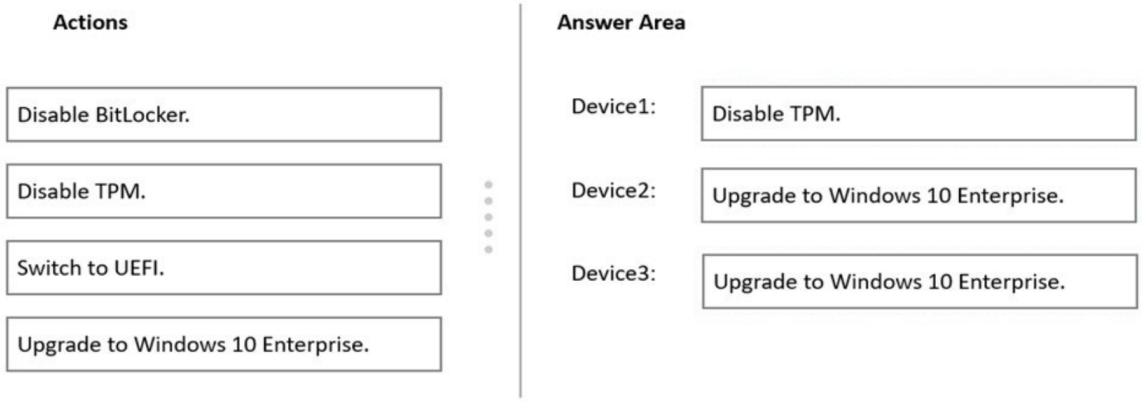
Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	**Not applicable**
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD).

What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of 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.



Answer:



Explanation:
Box 1: Disable TPM.
Hybrid Azure AD join is supported for FIPS-compliant TPM 2.0 and not supported for TPM 1.2.
If your devices have FIPS-compliant TPM 1.2, you must disable them before proceeding with hybrid Azure AD join.

Box 2: Upgrade to Windows 10 Enterprise
Windows 10 Home edition cannot be joined to a domain. First we must upgrade Windows 10 to Professional or Enterprise.

Box 3: Upgrade to Windows 10 Enterprise
Azure AD join isn't supported on previous versions of Windows or other operating systems. If you have Windows 7/8.1 devices, you must upgrade at least to Windows 10 to deploy Azure AD join.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan
https://docs.microsoft.com/en-us/azure/active-directory/devices/azureadjoin-plan
https://www.microsoft.com/en-us/windows/compare-windows-10-home-vs-pro

QUESTION 6
You have a Microsoft 365 E5 subscription.

You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.

What should you do?

A. From the Cloud App Security admin center, select **Users and accounts**.
B. From the Microsoft 365 security center, view the Threat tracker.
C. From the Microsoft 365 admin center, view the Security & compliance report.
D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Answer: A
Explanation:
The Microsoft Defender for Cloud Apps anomaly detection policies provide out-of-the-box user and entity behavioral analytics (UEBA) and machine learning (ML) so that you're ready from the outset to run advanced threat detection across your cloud environment.
Protection includes: Activity from anonymous IP addresses
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

QUESTION 6
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profiles?

A. Ubuntu Linux
B. macOS
C. iOS
D. Android

Answer: B
Explanation:
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Windows 10

2. macOS

Other incorrect answer options you may see on the exam include the following:
1. Android Enterprise
2. Windows 8.1

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

QUESTION 7
You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:

```
- Windows 10
- Android
- OS
```

On which devices can you configure the Endpoint DLP policies?

A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and macO Sonly
D. Windows 10, Android, and iOS

Answer: C
Explanation:
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

QUESTION 8
You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

A. Install the latest feature update and the latest quality update only.
B. Install the latest feature update and all the quality updates released since version 2004.
C. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.
D. Install all the feature updates released since version 2004 and the latest quality update only.

Answer: B
Explanation:
Feature updates are typically released twice per year and include new functionality and capabilities as well as potential fixes and security updates. Quality updates are more frequent and mainly include small fixes and security updates. Windows is designed to deliver both kinds of updates to devices through Windows Update.

Reference:
https://support.microsoft.com/en-us/topic/8a903416-6f45-0718-f5c7-375e92dddeb2

QUESTION 9
Your on-premises network contains the device types shown in the following table.

Name	Operating system	Drive encryption	BIOS	Image type
Type1	32-bit version of Windows 10 Pro	*None*	Legacy	Standard
Type2	64-bit version of Windows 8.1 Pro	*None*	Legacy	Start from VHD
Type3	64-bit version of Windows 8.1 Pro	BitLocker Drive Encryption (BitLocker)	Legacy	Custom
Type4	64-bit version of Windows 8.1 Pro	BitLocker Drive Encryption (BitLocker)	UEFI	Standard
Type5	64-bit version of Windows 8.1 Pro	*None*	Legacy	Standard

You plan to deploy an in-place upgrade to a 64-bit version of Windows 10 Enterprise by using the Microsoft Deployment Toolkit (MDT).
Which device types will support an in-place upgrade?

A. Type4 and Type5 only
B. Type3, Type4, and Type5 only
C. Type1, Type4, and Type5 only
D. Type1, Type2, and Type5 only

Answer: A
Explanation:
MDT has many useful features, such as:
* UEFI support. Supports deployment to machines using Unified Extensible Firmware Interface (UEFI) version 2.3.1.
* Offline BitLocker. Provides the capability to have BitLocker enabled during the Windows Preinstallation Environment (Windows PE) phase, thus saving hours of encryption time.
* Deploy to VHD. Provides ready-made task sequence templates for deploying Windows into a virtual hard disk (VHD) file.
Incorrect:
Not Type1: The upgrade process cannot change from a 32-bit operating system to a 64-bit due to the possible complications with drivers and applications it may bring.
Not Type2, not Type3: Boot images are the Windows Preinstallation Environment (Windows PE) images that are used to start the deployment.
You're not able to use a custom image of Windows 10 for the In-Place Upgrade scenario. You'd have to use the install.wim image provided with the latest
Windows 10 media that Microsoft has released.

Reference:
https://msendpointmgr.com/2015/10/26/deploy-windows-10-enterprise-using-in-place-upgrade/
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit

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.
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 Microsoft 365 Defender, you create a Threat policy.

Does this meet the goal?

A. Yes
B. No

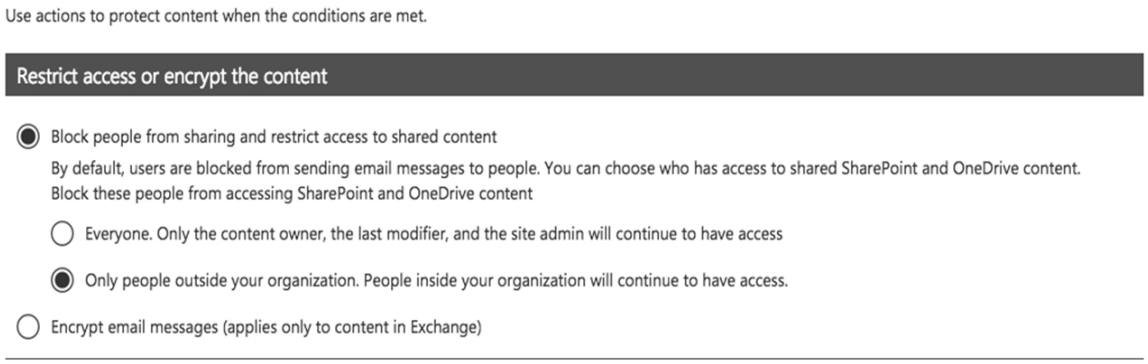
Answer: B
Explanation:
From the Security & Compliance admin center, Alerts, you create a new alert policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

QUESTION 11
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?

A. Windows Autopilot
B. Windows Update
C. Subscription Activation
D. an in-place upgrade

Answer: C
Explanation:
It would only require assigning the license and then having the user sign in. Autopilot is used for new/reset devices that are at the OOBE screen.
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

QUESTION 12
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?

A. an action
B. a group
C. an exception
D. a condition

Answer: C
Explanation:
You need to add an exception. In the Advanced Settings of the DLP policy, you can add a rule to configure the Conditions and Actions. There is also an 'Add Exception' button. This gives you several options that you can select as the exception. One of the options is 'except when recipient domain is'. You need to select that option and enter the domain name contoso.com.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work

QUESTION 13
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 verity your identity. Please contact your admin."

Which configuration prevents the users from signing in?

A. Microsoft Azure Active Directory (Azure AD) Identity Protection policies
B. Microsoft Azure Active Directory (Azure AD) conditional access policies
C. Security & Compliance supervision policies
D. Security & Compliance data loss prevention (DIP) policies

Answer: B
Explanation:
The user is being blocked due to a 'risky sign-in'. This can be caused by the user logging in from a device that hasn't been used to sign in before or from an unknown location.
Integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign in behavior. Policies can then force users to perform password changes or multi-factor

authentication to reduce their risk level or be blocked from access until an administrator takes manual action.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

QUESTION 14
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.

A. Select when Quality Updates are received
B. Select when Preview Builds and Feature Updates are received
C. Turn off auto-restart for updates during active hours
D. Manage preview builds
E. Automatic updates detection frequency

Answer: AB
Explanation:
GPO: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Quality Updates are received
GPO: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Preview Builds and Feature Updates are received
https://docs.microsoft.com/en-us/windows/deployment/update/wufb-manageupdate

QUESTION 15
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?

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

Answer: B
Explanation:
Your organization might use Windows Server FCI to identify documents with personally identifiable information (PII) such as social security numbers, and then classify the document by setting the Personally Identifiable Information property to High,
Moderate, Low, Public, or Not PII based on the type and number of occurrences of PII found in the document. In Office 365, you can create a DLP policy that identifies documents that have that property set to specific values, such as High and

Medium, and then takes an action such as blocking access to those files.
Before you can use a Windows Server FCI property or other property in a DLP policy, you need to create a managed property in the SharePoint admin center.
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties
https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties#before-you-create-the-dlp-policy

QUESTION 16
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?

A. Yes
B. No

Answer: A
Explanation:
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune.
In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune.

Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

QUESTION 17
You have a Microsoft 365 subscription.
From the subscription, you perform an audit log search, and you download all the results.
You plan to review the audit log data by using Microsoft Excel.
You need to ensure that each audited property appears in a separate Excel column.

What should you do first?

A. From Power Query Editor, transform the JSON data.
B. Format the Operations column by using conditional formatting.
C. Format the AuditData column by using conditional formatting.
D. From Power Query Editor, transform the XML data.

Answer: A
Explanation:
After you search the Office 365 audit log and download the search results to a CSV file, the file contains a column named AuditData, which contains additional information about each event. The data in this column is formatted as a JSON object, which contains multiple properties that are configured as property:value pairs separated by commas. You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column. This lets you sort and filter on one or more of these properties References:
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records

QUESTION 18
You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.
To which users can User1 send documents that contain PII?

A. User2 only
B. User2 and User3 only
C. User2, User3, and User4 only
D. User2, User3, User4, and User5

Answer: B
Explanation:
Guest accounts are considered "outside your organization". Users who have non-guest accounts in a host organization's Active Directory or Azure Active Directory tenant are considered as people inside the organization.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**