# SC-900 Q&As

Microsoft Security Compliance and Identity Fundamentals

## Pass Microsoft SC-900 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/sc-900.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

**QUESTION 1**

In a hybrid identity model, what can you use to sync identities between Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD)?

A. Active Directory Federation Services (AD FS)

B. Azure Sentinel

C. Azure AD Connect

D. Azure Ad Privileged Identity Management (PIM)

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

**QUESTION 2**

You are creating a custom trainable classifier to identify organizational product codes referenced in Microsoft 365 content.

You identify 300 files to use as seed content.

Where should you store the seed content?

A. a Microsoft SharePoint Online folder

B. a Microsoft OneDrive for Business folder

C. an Azure file share

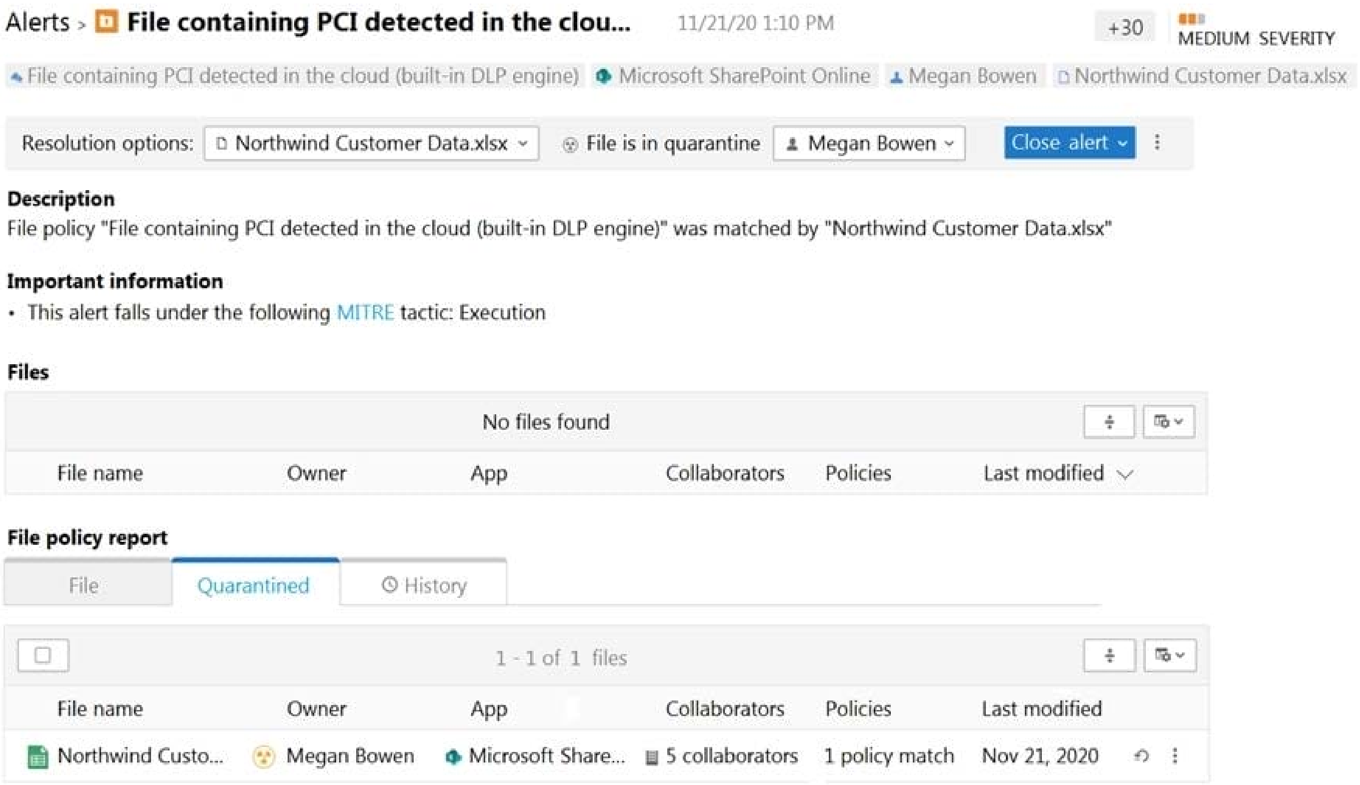
D. Microsoft Exchange Online shared mailbox

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

**QUESTION 3**

A user reports that she can no longer access a Microsoft Excel file named Northwind Customer Data.xlsx. From the Cloud App Security portal, you discover the alert shown in the exhibit.



Alerts > File containing PCI detected in the clou... 11/21/20 1:10 PM +30 MEDIUM SEVERITY

File containing PCI detected in the cloud (built-in DLP engine) | Microsoft SharePoint Online | Megan Bowen | Northwind Customer Data.xlsx

Resolution options: Northwind Customer Data.xlsx | File is in quarantine | Megan Bowen | Close alert

**Description**

File policy "File containing PCI detected in the cloud (built-in DLP engine)" was matched by "Northwind Customer Data.xlsx"

**Important information**

- This alert falls under the following MITRE tactic: Execution

**Files**

No files found

| File name | Owner | App | Collaborators | Policies | Last modified |
|---|---|---|---|---|---|

**File policy report**

File | Quarantined | History

1 - 1 of 1 files

| File name | Owner | App | Collaborators | Policies | Last modified |
|---|---|---|---|---|---|
| Northwind Custo... | Megan Bowen | Microsoft Share... | 5 collaborators | 1 policy match | Nov 21, 2020 |

You restore the file from quarantine.

You need to prevent files that match the policy from being quarantined. Files that match the policy must generate an alert.

What should you do?

A. Modify the policy template.

B. Assign the Global reader role to the file owners.

C. Exclude file matching by using a regular expression.

D. Update the governance action.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies#create-a-new-file-policy

**QUESTION 4**

You have an Azure subscription.

You need to implement approval-based, time-bound role activation.

What should you use?

A. access reviews in Azure AD

B. Azure AD Privileged Identity Management (PIM)

C. Azure AD Identity Protection

D. Conditional access in Azure AD

Correct Answer: B

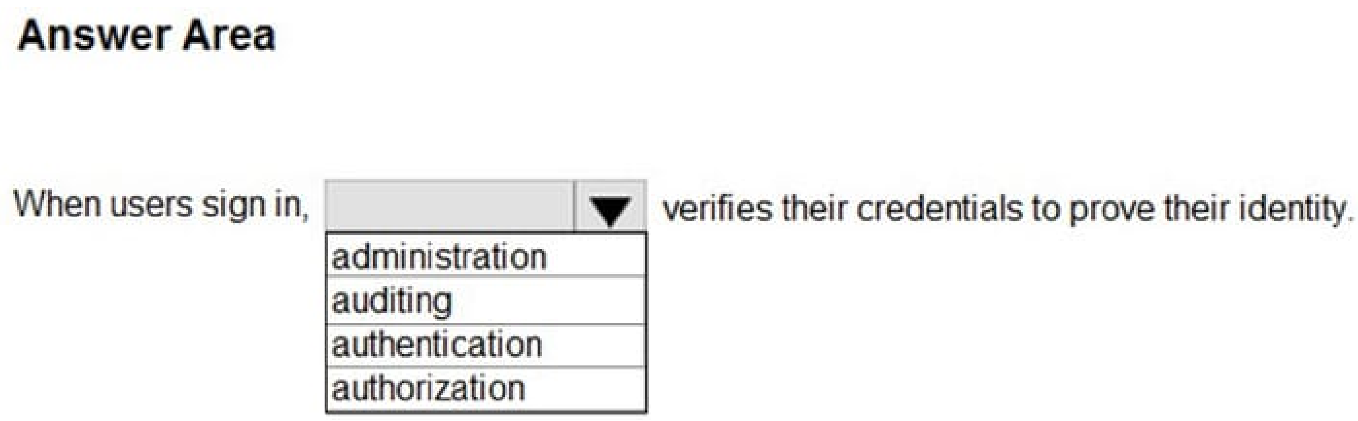
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

**QUESTION 5**

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

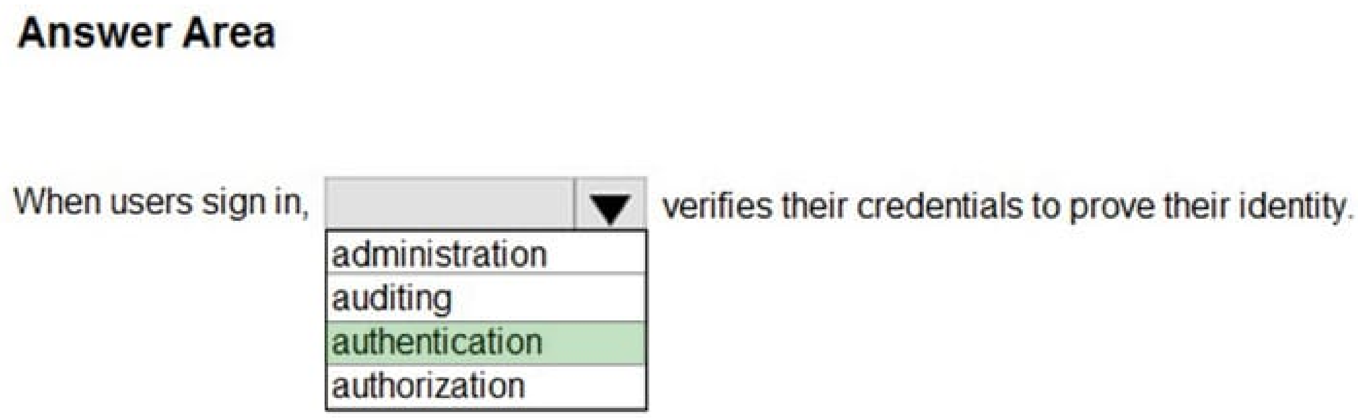


Answer Area

When users sign in, [▼] verifies their credentials to prove their identity.

- administration
- auditing
- authentication
- authorization

Correct Answer:



Answer Area

When users sign in, [▼] verifies their credentials to prove their identity.

- administration
- auditing
- authentication ✓
- authorization

Authentication

What is the difference between authentication and authorization in Azure?

In simple terms, authentication is the process of verifying who a user is, while authorization is the process of verifying what they have access to.

Reference: https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization

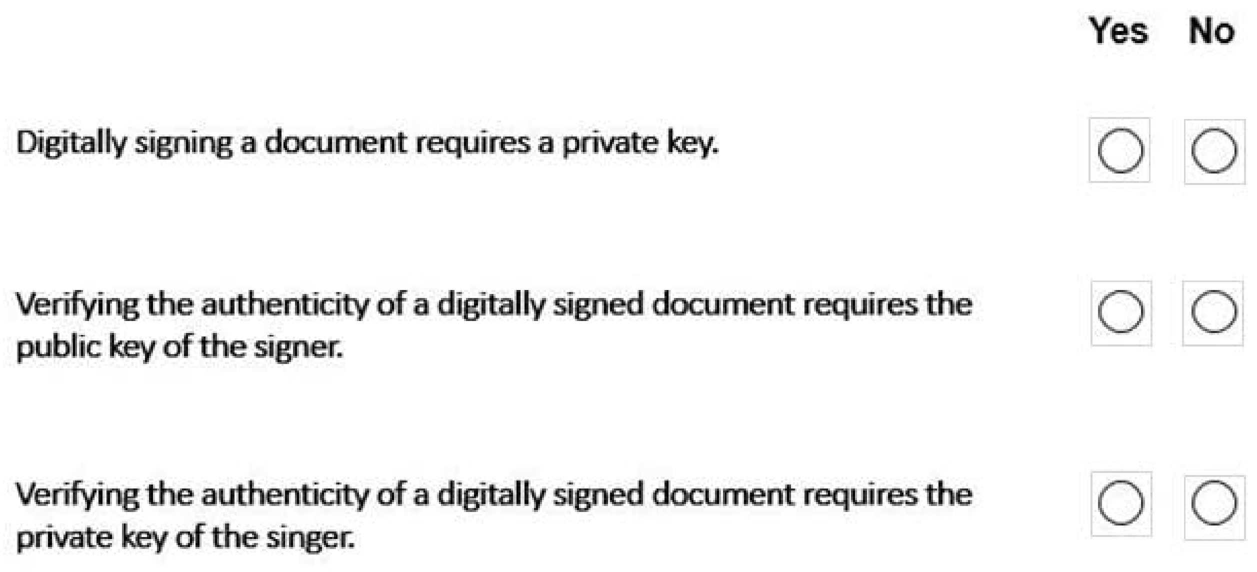
**QUESTION 6**

HOTSPOT

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

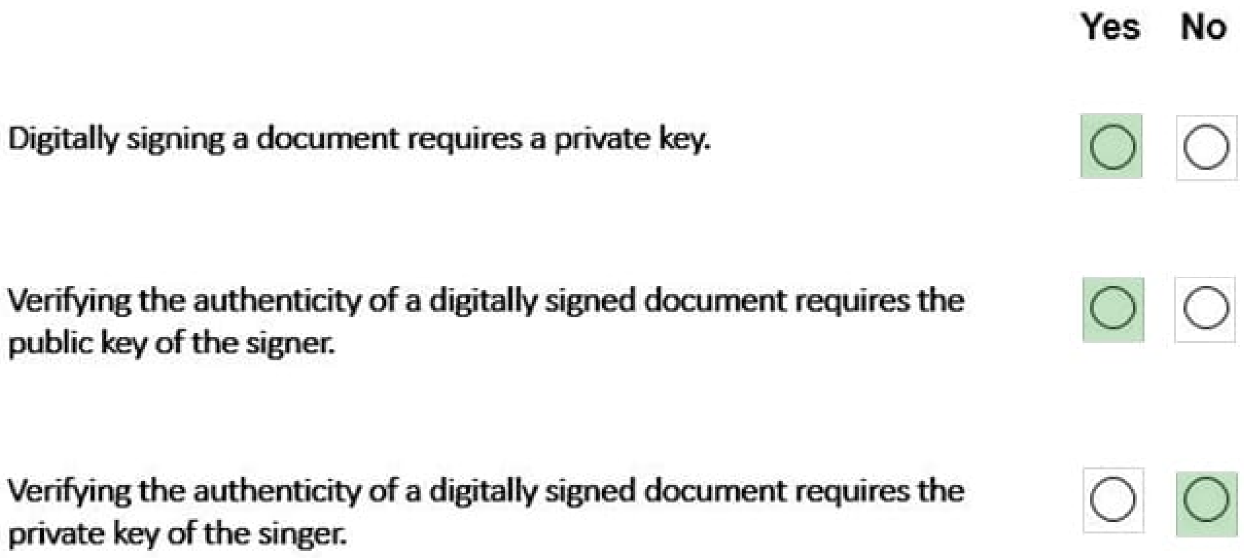
NOTE: Each correct selection is worth one point.

Hot Area:



| | Yes | No |
|---|---|---|
| Digitally signing a document requires a private key. | ○ | ○ |
| Verifying the authenticity of a digitally signed document requires the public key of the signer. | ○ | ○ |
| Verifying the authenticity of a digitally signed document requires the private key of the singer. | ○ | ○ |

Correct Answer:



| | Yes | No |
|---|---|---|
| Digitally signing a document requires a private key. | ● | ○ |
| Verifying the authenticity of a digitally signed document requires the public key of the signer. | ● | ○ |
| Verifying the authenticity of a digitally signed document requires the private key of the singer. | ○ | ● |

Box 1: Yes A certificate is required that provides a private and a public key. Box 2: Yes The public key is used to validate the private key that is associated with a digital signature. Box 3: NO

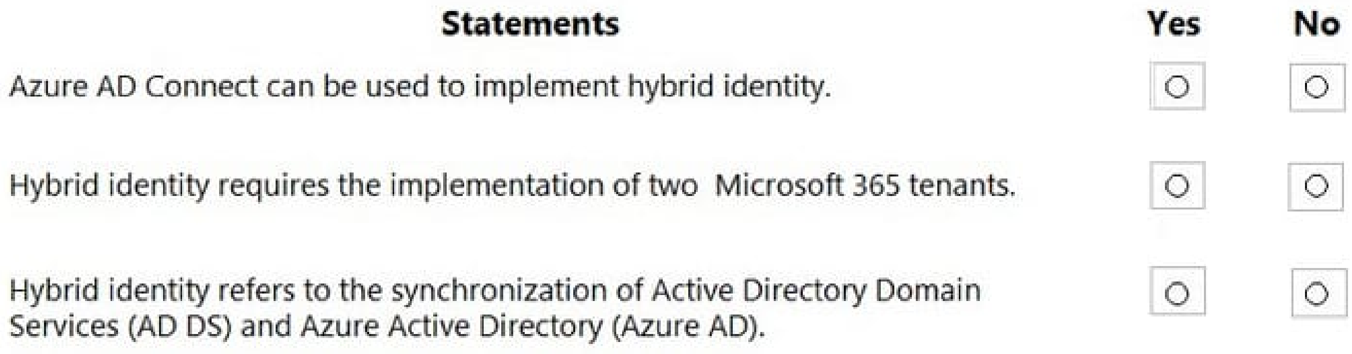
**QUESTION 7**

HOTSPOT

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

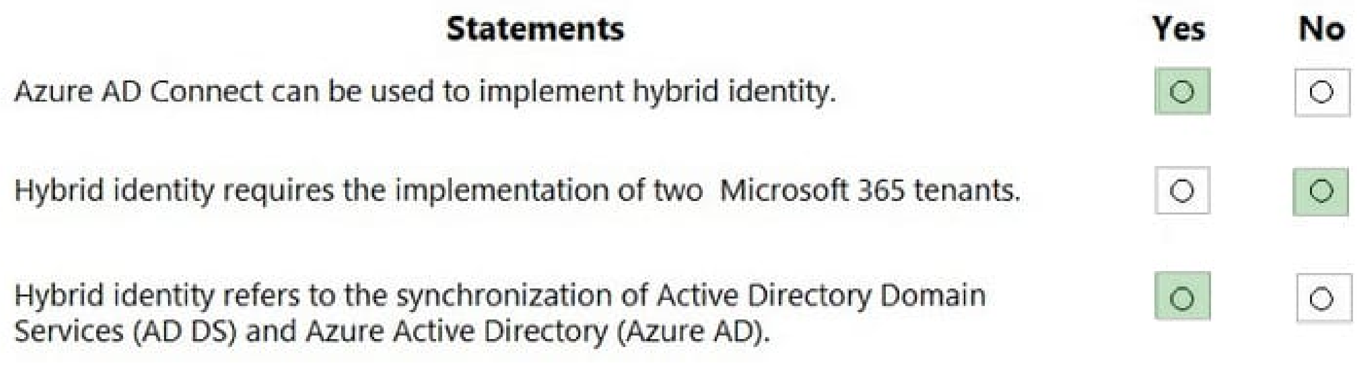
NOTE: Each correct selection is worth one point.

Hot Area:



| Statements | Yes | No |
|---|---|---|
| Azure AD Connect can be used to implement hybrid identity. | ○ | ○ |
| Hybrid identity requires the implementation of two Microsoft 365 tenants. | ○ | ○ |
| Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD). | ○ | ○ |

Correct Answer:



| Statements | Yes | No |
|---|---|---|
| Azure AD Connect can be used to implement hybrid identity. | [✓ ○] | ○ |
| Hybrid identity requires the implementation of two Microsoft 365 tenants. | ○ | [✓ ○] |
| Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD). | [✓ ○] | ○ |

**QUESTION 8**

What can you use to view the Microsoft Secure Score for Devices?

A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for Endpoint

C. Microsoft Defender for Identity

D. Microsoft Defender for Office 365

Correct Answer: B

Artikel 3 Minuten Lesedauer Microsoft Secure Score for DevicesApplies to:

1.

Microsoft Defender for Endpoint Plan 2

2.

Microsoft Defender Vulnerability Management

3.

Microsoft 365 Defender

Some information relates to pre-released product which may be substantially modified before it\\'s commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

To sign up for the Defender Vulnerability Management public preview or if you have any questions, contact us (mdvmtrial@microsoft.com).

Already have Microsoft Defender for Endpoint P2? Sign up for a free trial of the Defender Vulnerability Management Add-on.

Configuration score is now part of vulnerability management as Microsoft Secure Score for Devices.

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat attacks. It reflects the collective security configuration state of your devices across the following categories:

1.

Application

2.

Operating system

3.

Network

4.

Accounts

5.

Security controls

Select a category to go to the Security recommendations page and view the relevant recommendations.

Turn on the Microsoft Secure Score connectorForward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as your

Microsoft Secure Score data.

Changes might take up to a few hours to reflect in the dashboard.

1.

In the navigation pane, go to Settings > Endpoints > General > Advanced features

2.

Scroll down to Microsoft Secure Score and toggle the setting to On.

3.

Select Save preferences.

How it worksMicrosoft Secure Score for Devices currently supports configurations set via Group Policy. Due to the current partial Intune support, configurations which might have been set through Intune might show up as misconfigured.

Contact your IT Administrator to verify the actual configuration status in case your organization is using Intune for secure configuration management.

The data in the Microsoft Secure Score for Devices card is the product of meticulous and ongoing vulnerability discovery process. It is aggregated with configuration discovery assessments that continuously:

1.

Compare collected configurations to the collected benchmarks to discover misconfigured assets

2.

Map configurations to vulnerabilities that can be remediated or partially remediated (risk reduction)

3.

Collect and maintain best practice configuration benchmarks (vendors, security feeds, internal research teams)

4.

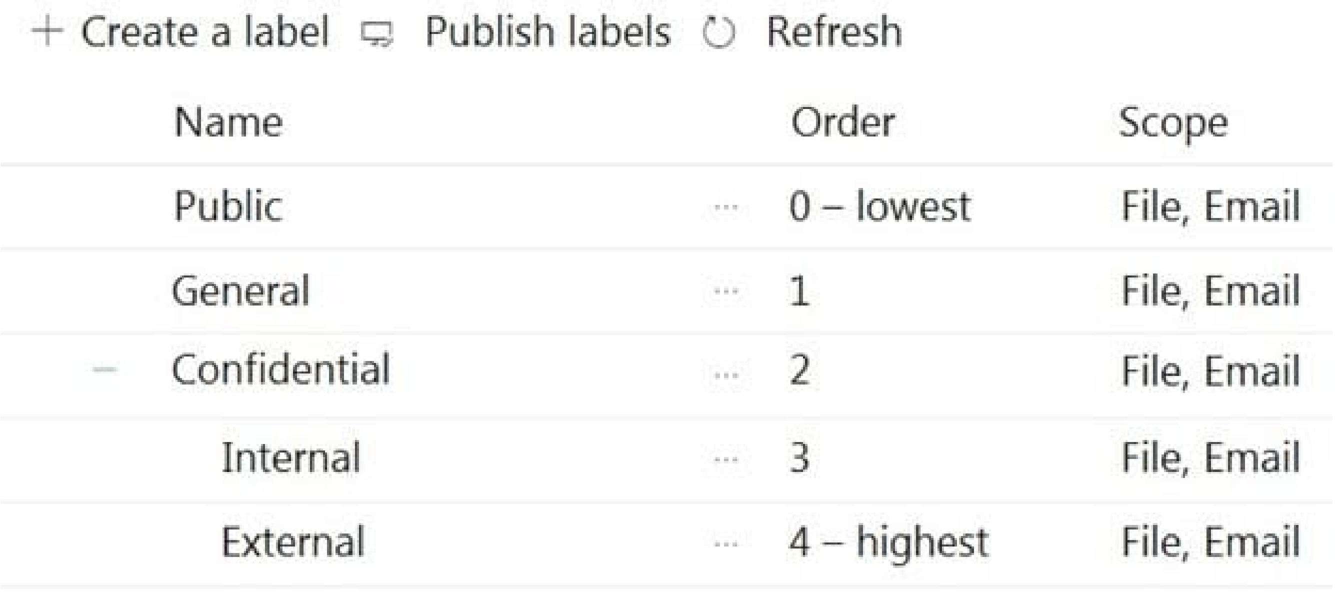
Collect and monitor changes of security control configuration state from all assets

**QUESTION 9**

HOTSPOT

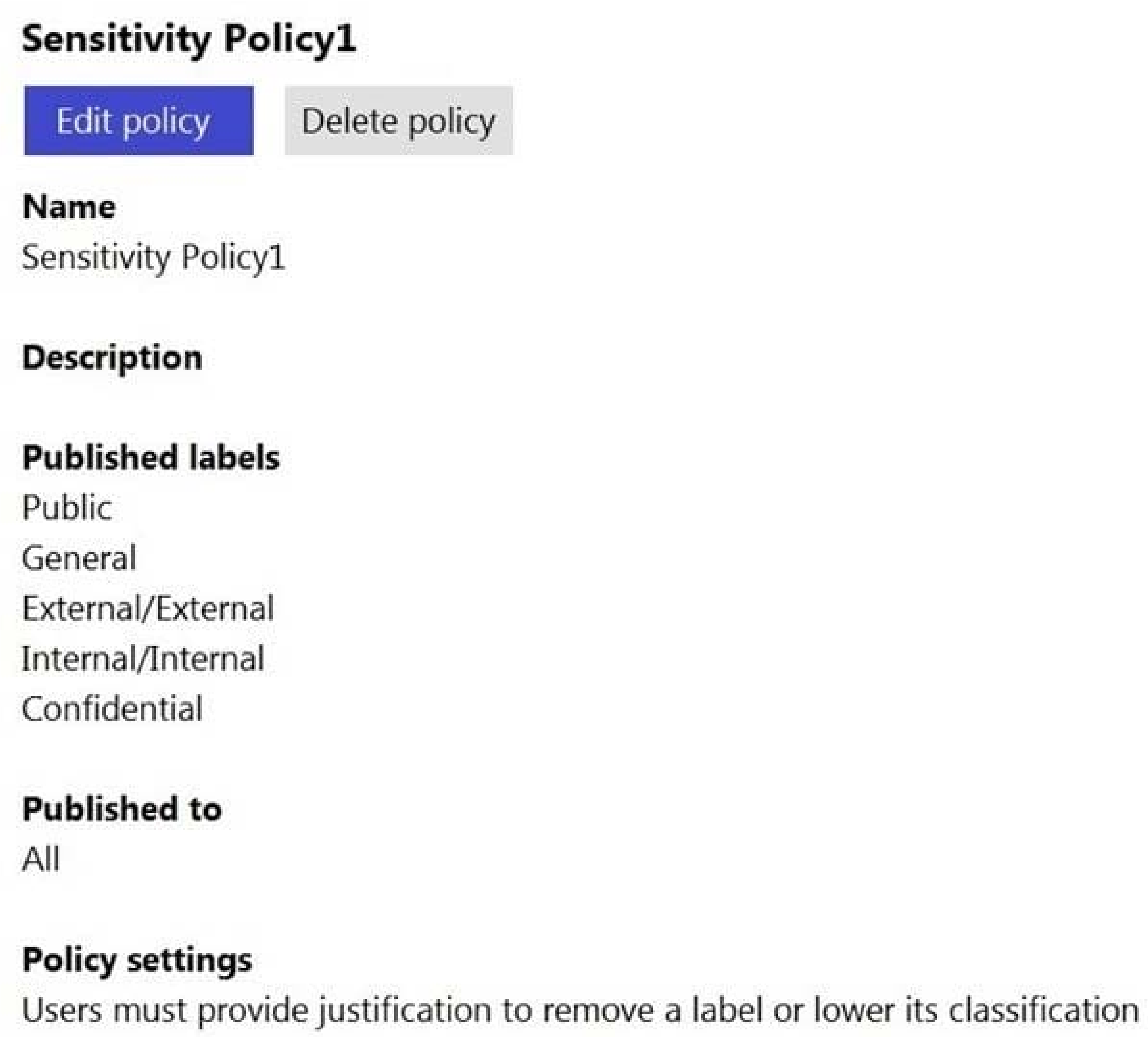
You have a Microsoft 365 E5 tenant.

You create sensitivity labels as shown in the Sensitivity Labels exhibit.



| Name | | Order | Scope |
|---|---|---|---|
| Public | ··· | 0 – lowest | File, Email |
| General | ··· | 1 | File, Email |
| − Confidential | ··· | 2 | File, Email |
| Internal | ··· | 3 | File, Email |
| External | ··· | 4 – highest | File, Email |

The Confidential/External sensitivity label is configured to encrypt files and emails when applied to content. The sensitivity labels are published as shown in the Published exhibit.



**Sensitivity Policy1**

**Name**
Sensitivity Policy1

**Description**

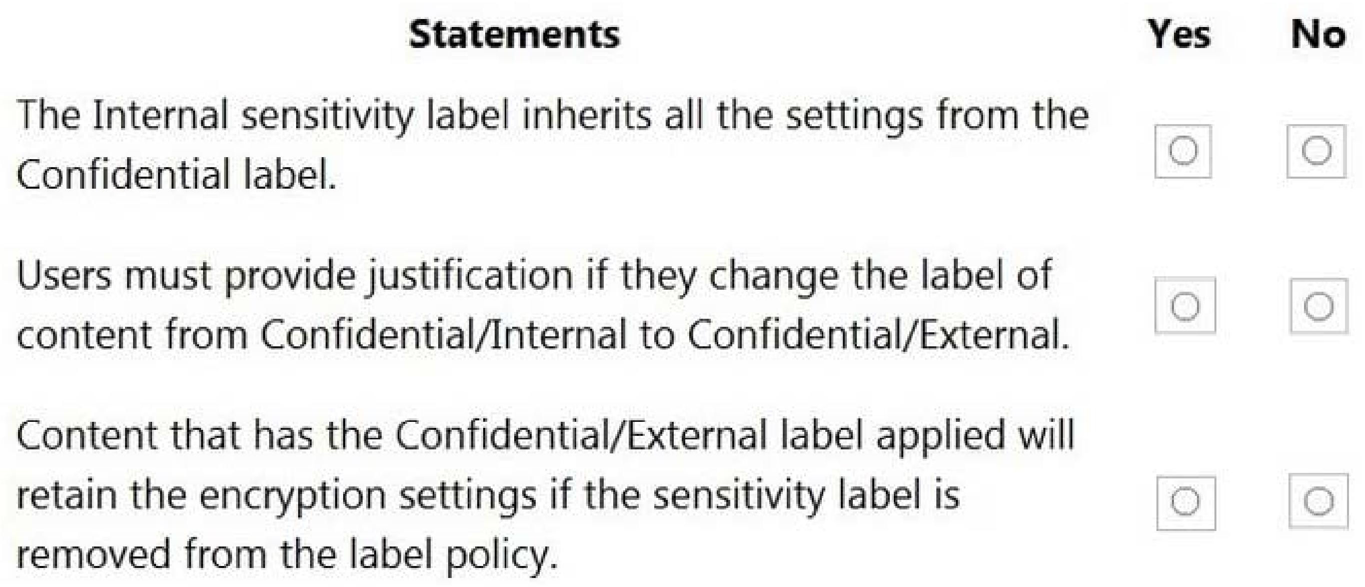
**Published labels**
Public
General
External/External
Internal/Internal
Confidential

**Published to**
All

**Policy settings**
Users must provide justification to remove a label or lower its classification

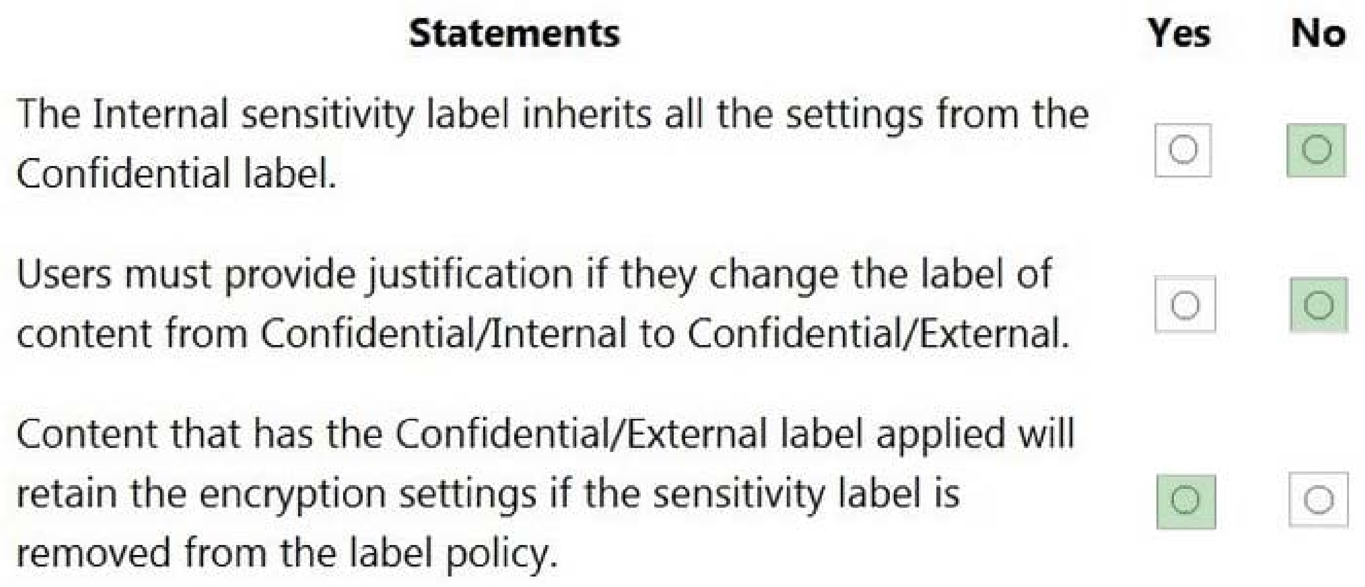
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



| Statements | Yes | No |
|---|---|---|
| The Internal sensitivity label inherits all the settings from the Confidential label. | ○ | ○ |
| Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External. | ○ | ○ |
| Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy. | ○ | ○ |

Correct Answer:



| Statements | Yes | No |
|---|---|---|
| The Internal sensitivity label inherits all the settings from the Confidential label. | ○ | ● |
| Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External. | ○ | ● |
| Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy. | ● | ○ |

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

**QUESTION 10**

You need to connect to an Azure virtual machine by using Azure Bastion. What should you use?

A. an SSH client

B. PowerShell remoting

C. the Azure portal

D. the Remote Desktop Connection client

Correct Answer: C

You can create an RDP connection to a Windows VM using Azure Bastion.

Reference: https://docs.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows

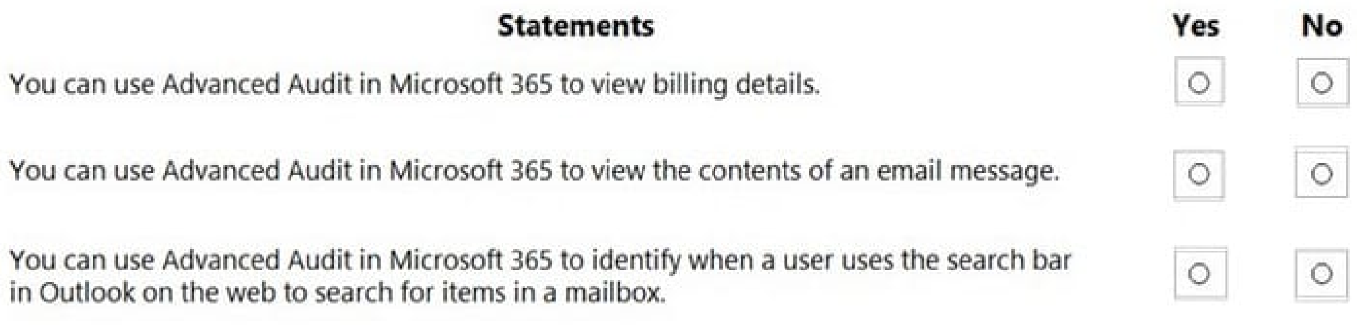
**QUESTION 11**

HOTSPOT

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

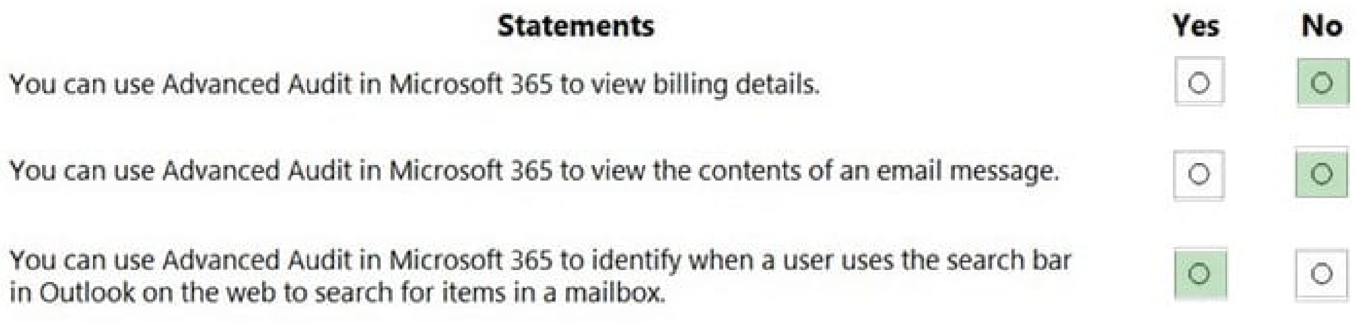
NOTE: Each correct selection is worth one point.

Hot Area:



| Statements | Yes | No |
|---|---|---|
| You can use Advanced Audit in Microsoft 365 to view billing details. | ○ | ○ |
| You can use Advanced Audit in Microsoft 365 to view the contents of an email message. | ○ | ○ |
| You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox. | ○ | ○ |

Correct Answer:



| Statements | Yes | No |
|---|---|---|
| You can use Advanced Audit in Microsoft 365 to view billing details. | ○ | ● |
| You can use Advanced Audit in Microsoft 365 to view the contents of an email message. | ○ | ● |
| You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox. | ● | ○ |

Box 1: No Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention.

Box 2: No

Box 3: Yes Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide

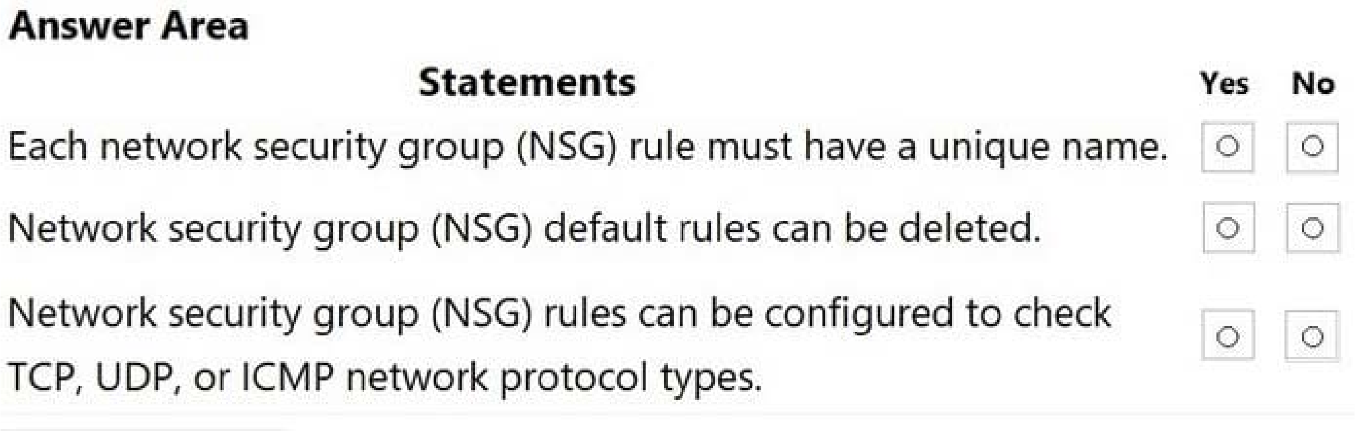
**QUESTION 12**

HOTSPOT

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

NOTE: Each correct selection is worth one point.

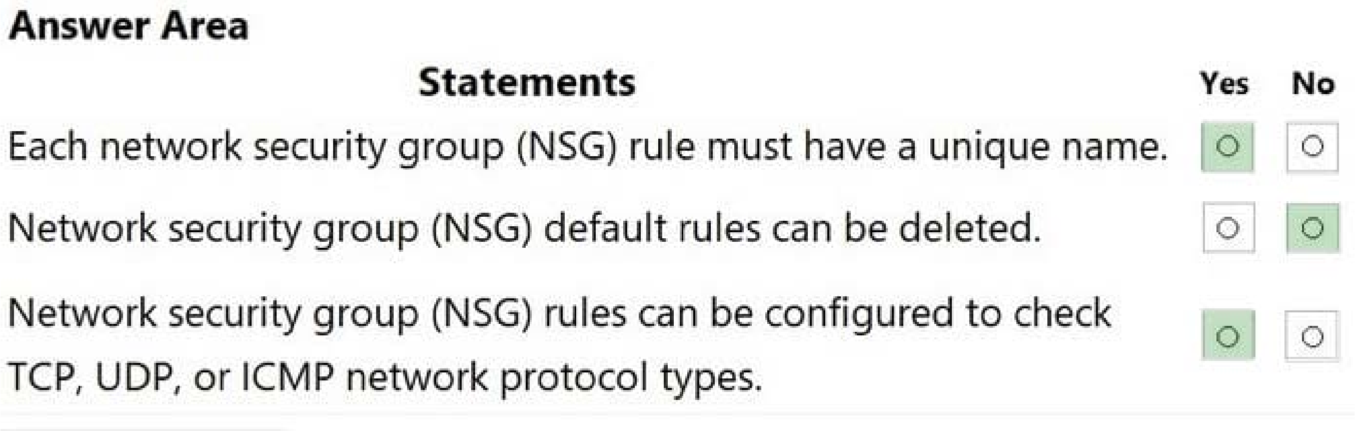
Hot Area:



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Each network security group (NSG) rule must have a unique name. | ○ | ○ |
| Network security group (NSG) default rules can be deleted. | ○ | ○ |
| Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types. | ○ | ○ |

Correct Answer:



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Each network security group (NSG) rule must have a unique name. | [✓ ○] | ○ |
| Network security group (NSG) default rules can be deleted. | ○ | [✓ ○] |
| Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types. | [✓ ○] | ○ |

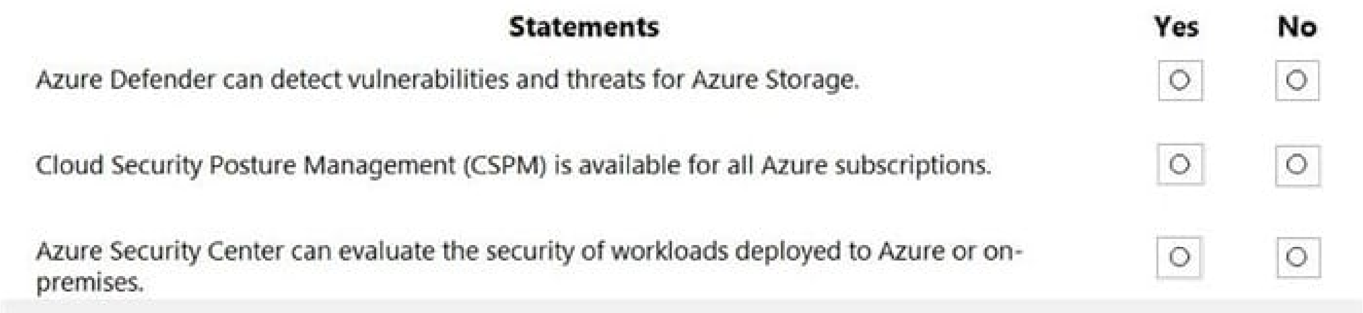
**QUESTION 13**

HOTSPOT

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

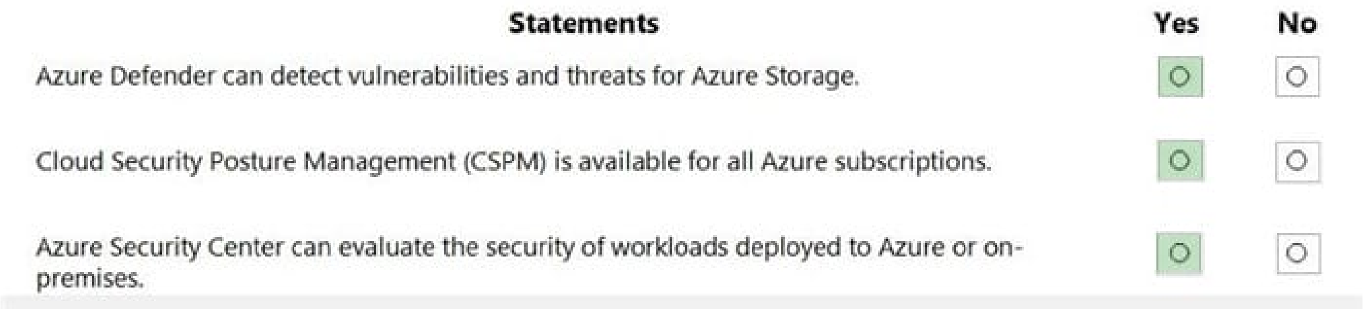
NOTE: Each correct selection is worth one point.

Hot Area:



| Statements | Yes | No |
|---|---|---|
| Azure Defender can detect vulnerabilities and threats for Azure Storage. | ○ | ○ |
| Cloud Security Posture Management (CSPM) is available for all Azure subscriptions. | ○ | ○ |
| Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises. | ○ | ○ |

Correct Answer:



| Statements | Yes | No |
|---|---|---|
| Azure Defender can detect vulnerabilities and threats for Azure Storage. | ● | ○ |
| Cloud Security Posture Management (CSPM) is available for all Azure subscriptions. | ● | ○ |
| Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises. | ● | ○ |

Box 1: Yes

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more

Box 2: Yes

Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they\\'re in

Azure or not - as well as on premises.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/azure-defender

https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction

https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction

**QUESTION 14**

Which Microsoft portal provides information about how Microsoft cloud services comply with regulatory standard, such as International Organization for Standardization (ISO)?

A. the Microsoft Endpoint Manager admin center

B. Azure Cost Management + Billing

C. Microsoft Service Trust Portal

D. the Azure Active Directory admin center

Correct Answer: C

The Microsoft Service Trust Portal contains details about Microsoft\\'s implementation of controls and processes that protect our cloud services and the customer data therein.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

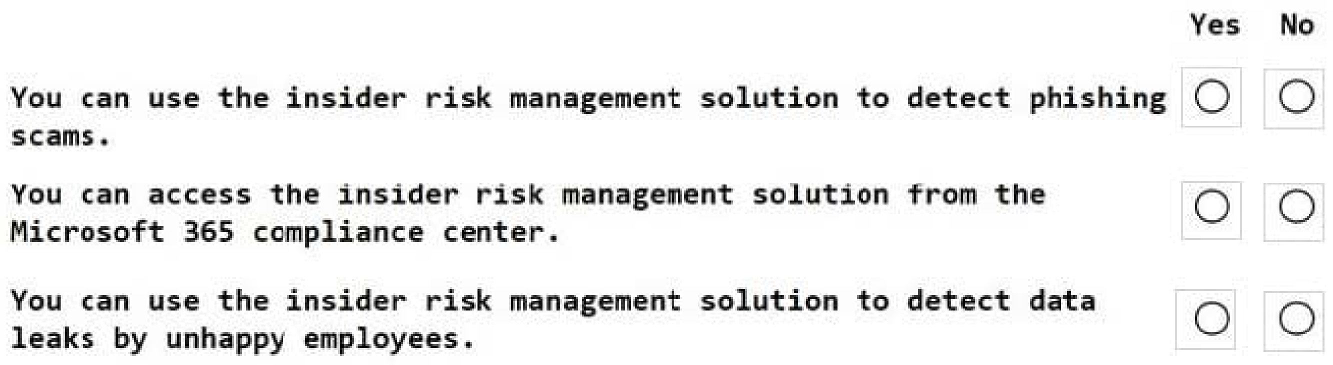
**QUESTION 15**

HOTSPOT

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

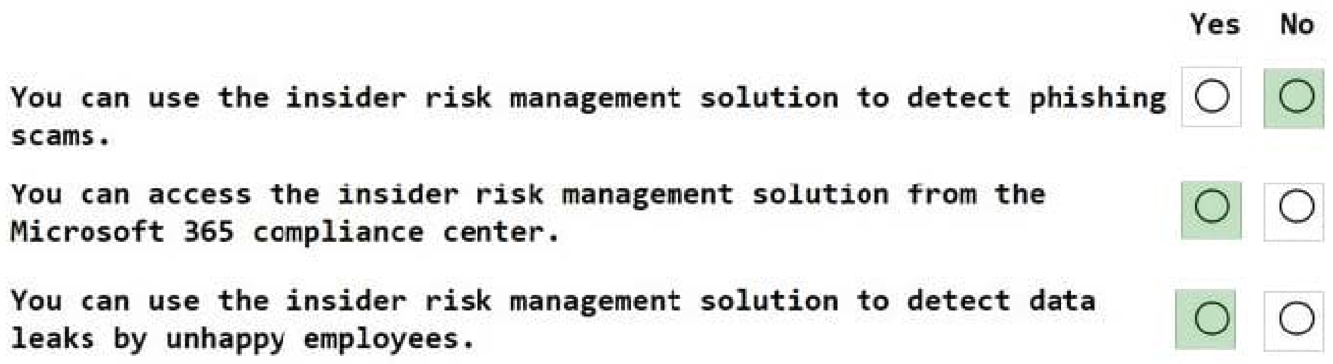
NOTE: Each correct selection is worth one point.

Hot Area:



| | Yes | No |
|---|---|---|
| You can use the insider risk management solution to detect phishing scams. | ○ | ○ |
| You can access the insider risk management solution from the Microsoft 365 compliance center. | ○ | ○ |
| You can use the insider risk management solution to detect data leaks by unhappy employees. | ○ | ○ |

Correct Answer:



| | Yes | No |
|---|---|---|
| You can use the insider risk management solution to detect phishing scams. | ○ | [✓ ○] |
| You can access the insider risk management solution from the Microsoft 365 compliance center. | [✓ ○] | ○ |
| You can use the insider risk management solution to detect data leaks by unhappy employees. | [✓ ○] | ○ |

Box 1: No

Phishing scams are external threats.

Box 2: Yes

Insider risk management is a compliance solution in Microsoft 365.

Box 3: Yes

Insider risk management helps minimize internal risks from users. These include:

1.

Leaks of sensitive data and data spillage

2.

Confidentiality violations

3.

Intellectual property (IP) theft

4.

Fraud

5.

Insider trading

6.

Regulatory compliance violations

Latest SC-900 Dumps SC-900 PDF Dumps SC-900 Braindumps