



SC-900

Microsoft Security, Compliance and Identity Fundamentals



EXAMKILLER

Help Pass Your Exam At First Try

Microsoft

Exam SC-900

Microsoft Security Compliance and Identity Fundamentals

Version: 8.0

[Total Questions: 138]

Question No : 1 HOTSPOT

Select the answer that correctly completes the sentence.

	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.
Customer Lockbox	
Information barriers	
Privileged Access Management (PAM)	
Sensitivity labels	

Answer:

	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.
Customer Lockbox	
Information barriers	
Privileged Access Management (PAM)	
Sensitivity labels	

	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.
Customer Lockbox	
Information barriers	
Privileged Access Management (PAM)	
Sensitivity labels	

Explanation:

Text

Description automatically generated

Question No : 2 HOTSPOT

Select the answer that correctly completes the sentence.

	provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.
Azure Defender	
The Microsoft 365 compliance center	
The Microsoft 365 security center	
Microsoft Endpoint Manager	

Answer:

	provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.
Azure Defender	
The Microsoft 365 compliance center	
The Microsoft 365 security center	
Microsoft Endpoint Manager	

	▼
Azure Defender	
The Microsoft 365 compliance center	
The Microsoft 365 security center	
Microsoft Endpoint Manager	

provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.

Explanation:

Text

Description automatically generated

Question No : 3 HOTSPOT

Select the answer that correctly completes the sentence.

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
Microsoft Sentinel
Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

Answer:

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
Microsoft Sentinel
Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

Explanation:

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
Microsoft Sentinel
Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

Question No : 4

Which Azure Active Directory (Azure AD) feature can you use to provide just-in-time (JIT) access to manage Azure resources?

- A. conditional access policies
- B. Azure AD Identity Protection
- C. Azure AD Privileged Identity Management (PIM)
- D. authentication method policies

Answer: C

Explanation:

Azure AD Privileged Identity Management (PIM) provides just-in-time privileged access to Azure AD and Azure resources

Reference:

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

Question No : 5 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.

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	<input type="radio"/>	<input type="radio"/>
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area	Statements	Yes	No
	Applying system updates increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
	The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
	Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

Graphical user

interface, text, application, email

Description automatically generated

Box 1: Yes

System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes

Box 3: Yes

If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure.

Question No : 6

Which two Azure resources can a network security group (NSG) be associated with? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. a network interface
- B. an Azure App Service web app
- C. a virtual network
- D. a virtual network subnet
- E. a resource group

Answer: C,E

Explanation:

You can use an Azure network security group **to filter network traffic to and from Azure resources in an Azure virtual network**. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

Question No : 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.

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area**

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:**Answer Area**

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input checked="" type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input checked="" type="radio"/>

Graphical user

interface, text, application

Description automatically generated

Question No : 8 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.

Statements	Yes	No
Azure AD Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can detect whether user credentials were leaked to the public.	<input type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Azure AD Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input checked="" type="radio"/>
Azure AD Identity Protection can detect whether user credentials were leaked to the public.	<input checked="" type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Statements	Yes	No
Azure AD Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input checked="" type="radio"/>
Azure AD Identity Protection can detect whether user credentials were leaked to the public.	<input checked="" type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input checked="" type="radio"/>	<input type="radio"/>

Question No : 9 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.

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	<input type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	<input type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	<input type="radio"/>	<input type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	<input checked="" type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	<input checked="" type="radio"/>	<input type="radio"/>

Graphical user

interface, text, application, email

Description automatically generated

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.

Question No : 10 DRAG DROP

Match the types Of compliance score actions to the appropriate tasks.

To answer, drag the appropriate action type from the column on the left to its task on the right. Each type may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Compliance score action	Answer Area
Corrective	Action Use encryption to protect data at rest.
Detective	Action Actively monitor systems to identify irregularities that might represent risks.
Preventative	

Answer:

Compliance score action	Answer Area
Corrective	Preventative Use encryption to protect data at rest.
Detective	Detective Actively monitor systems to identify irregularities that might represent risks.
Preventative	

Explanation:

Preventative	Use encryption to protect data at rest.
Detective	Actively monitor systems to identify irregularities that might represent risks.

Question No : 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.

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>
Conditional access policies can be used to block access to an application based on the location of the user.	<input type="radio"/>	<input type="radio"/>
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can be used to block access to an application based on the location of the user.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can be used to block access to an application based on the location of the user.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	<input type="radio"/>	<input checked="" type="radio"/>

Graphical user

interface, text, application, email

Description automatically generated

Question No : 12

Which two types of resources can be protected by using Azure Firewall? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Azure virtual machines
- B. Azure Active Directory (Azure AD) users
- C. Microsoft Exchange Online inboxes
- D. Azure virtual networks
- E. Microsoft SharePoint Online sites

Answer: A,D

Explanation: Firewall is really not directly protecting the Virtual Networks though DDOS would have been ideal for VNETS

Question No : 13 HOTSPOT

Select the answer that correctly completes the sentence.

▼	provides benchmark recommendations and guidance for protecting Azure services.
Azure Application Insights	
Azure Network Watcher	
Log Analytics workspaces	
Security baselines for Azure	

Answer:

▼	provides benchmark recommendations and guidance for protecting Azure services.
Azure Application Insights	
Azure Network Watcher	
Log Analytics workspaces	
Security baselines for Azure	

▼	provides benchmark recommendations and guidance for protecting Azure services.
Azure Application Insights	
Azure Network Watcher	
Log Analytics workspaces	
Security baselines for Azure	

Explanation:

Text

Description automatically generated with medium confidence

Question No : 14 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.

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	<input type="radio"/>	<input type="radio"/>
Transparency is a key privacy principle of Microsoft.	<input type="radio"/>	<input type="radio"/>
Shared responsibility is a key privacy principle of Microsoft.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	<input checked="" type="radio"/>	<input type="radio"/>
Transparency is a key privacy principle of Microsoft.	<input checked="" type="radio"/>	<input type="radio"/>
Shared responsibility is a key privacy principle of Microsoft.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	<input checked="" type="radio"/>	<input type="radio"/>
Transparency is a key privacy principle of Microsoft.	<input checked="" type="radio"/>	<input type="radio"/>
Shared responsibility is a key privacy principle of Microsoft.	<input type="radio"/>	<input checked="" type="radio"/>

Graphical user

interface, text, application, email

Description automatically generated

Question No : 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.

Statements	Yes	No
You can add a resource lock to an Azure subscription.	<input type="radio"/>	<input type="radio"/>
You can add only one resource lock to an Azure resource.	<input type="radio"/>	<input type="radio"/>
You can delete a resource group containing resources that have resource locks.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can add a resource lock to an Azure subscription.	<input checked="" type="radio"/>	<input type="radio"/>
You can add only one resource lock to an Azure resource.	<input type="radio"/>	<input checked="" type="radio"/>
You can delete a resource group containing resources that have resource locks.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation: Yes

NO

NO

YES - As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

NO - The most restrictive lock in the inheritance takes precedence.

NO - If you delete a resource group with a locked resource, the portal UI will give you an error and no resources are deleted.

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>

Question No : 16 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.

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	<input type="radio"/>	<input type="radio"/>
Conditional access policies apply before first-factor authentication is complete.	<input type="radio"/>	<input type="radio"/>
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies apply before first-factor authentication is complete.	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies apply before first-factor authentication is complete.	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	<input checked="" type="radio"/>	<input type="radio"/>

Graphical user

interface, text, application, email

Description automatically generated

Box 1: Yes

Box 2: No

Conditional Access policies are enforced after first-factor authentication is completed. Box 3: Yes

Question No : 17

What can you use to provision Azure resources across multiple subscriptions in a consistent manner?

- A. Microsoft Defender for Cloud
- B. Azure Blueprints
- C. Microsoft Sentinel
- D. Azure Policy

Answer: B

Question No : 18

What should you use in the Microsoft 365 security center to view security trends and track the protection status of identities?

- A. Attack simulator
- B. Reports
- C. Hunting
- D. Incidents

Answer: B

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-and-insights-in-security-and-compliance?view=o365-worldwide>

Question No : 19 HOTSPOT

Select the answer that correctly completes the sentence.

When you enable security defaults in Azure Active Directory (Azure AD),

▼
Azure AD Identity Protection
Azure AD Privileged Identity Management (PIM)
multi-factor authentication (MFA)

will be enabled for all Azure AD users.

Answer:

When you enable security defaults in Azure Active Directory (Azure AD),

▼
Azure AD Identity Protection
Azure AD Privileged Identity Management (PIM)
multi-factor authentication (MFA)

will be enabled for all Azure AD users.

When you enable security defaults in Azure Active Directory (Azure AD),

▼
Azure AD Identity Protection
Azure AD Privileged Identity Management (PIM)
multi-factor authentication (MFA)

will be enabled for all Azure AD users.

Explanation:

Graphical user interface, text, application

Description automatically generated

Question No : 20

Which score measures an organization's progress in completing actions that help reduce risks associated to data protection and regulatory standards?

- A. Microsoft Secure Score
- B. Productivity Score
- C. Secure score in Azure Security Center
- D. Compliance score

Answer: D

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide>

Question No : 21

Which Microsoft 365 feature can you use to restrict users from sending email messages that contain lists of customers and their associated credit card numbers?

- A. retention policies
- B. data loss prevention (DLP) policies
- C. conditional access policies
- D. information barriers

Answer: B

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

Question No : 22 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

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input checked="" type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input checked="" type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input checked="" type="radio"/>	<input type="radio"/>

Question No : 23

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

Answer: C

Explanation:

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 No : 24 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

Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	<input type="radio"/>	<input type="radio"/>
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	<input type="radio"/>	<input type="radio"/>
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	<input checked="" type="radio"/>	<input type="radio"/>
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	<input type="radio"/>	<input checked="" type="radio"/>
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	<input checked="" type="radio"/>	<input type="radio"/>

Explanation: