

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.pass2lead.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



QUESTION 1

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Federation is used to establish between organizations.

multi-factor authentication (MFA)
a trust relationship
user account synchronization
a VPN connection

Correct Answer:

Answer Area

Federation is used to establish between organizations.

multi-factor authentication (MFA)
a trust relationship
user account synchronization
a VPN connection

Federation is a collection of domains that have established trust.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

QUESTION 2

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

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



will be enabled for all Azure AD users.

Correct Answer:

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



will be enabled for all Azure AD users.

QUESTION 3

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use

Reports
Hunting
Attack simulator
Incidents

in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

Correct Answer:

Answer Area

You can use

Reports
Hunting
Attack simulator
Incidents

in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide>

QUESTION 4

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:

You can use information barriers with Microsoft Exchange. Yes No

You can use information barriers with Microsoft SharePoint. Yes No

You can use information barriers with Microsoft Teams. Yes No

Correct Answer:

You can use information barriers with Microsoft Exchange. Yes No

You can use information barriers with Microsoft SharePoint. Yes No

You can use information barriers with Microsoft Teams. Yes No

Box 1: No

Information barriers and Exchange Online

IB policies aren't available to restrict communication and collaboration between groups and users in email messages.

Box 2: Yes

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.

Box 3: Yes

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

QUESTION 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.

Hot Area:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	<input type="radio"/>	<input type="radio"/>
Hybrid identity requires the implementation of two Microsoft 365 tenants.	<input type="radio"/>	<input type="radio"/>
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	<input checked="" type="radio"/>	<input type="radio"/>
Hybrid identity requires the implementation of two Microsoft 365 tenants.	<input type="radio"/>	<input checked="" type="radio"/>
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	<input checked="" type="radio"/>	<input type="radio"/>

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:

Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	<input type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can deny outbound traffic to the internet.	<input type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	<input checked="" type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can deny outbound traffic to the internet.	<input checked="" type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	<input checked="" type="radio"/>	<input type="radio"/>

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. For each rule, you can specify source and destination, port, and protocol.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

QUESTION 7

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

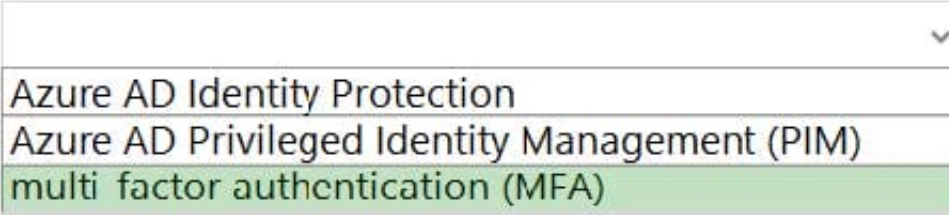
- Azure AD Identity Protection
- Azure AD Privileged Identity Management (PIM)
- multi factor authentication (MFA)

will be enabled for all Azure AD users.

Correct Answer:

Answer Area

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.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

QUESTION 8

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. E. a resource group

Correct Answer: AD

Association of network security groups

You can associate a network security group with virtual machines, NICs, and subnets, depending on the deployment model you use.

Reference:

<https://aviatrix.com/learn-center/cloud-security/create-network-security-groups-in-azure/>

QUESTION 9

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

In Azure Sentinel, you can automate common tasks by using

	▼
deep investigation tools.	
hunting search-and-query tools.	
playbooks.	
workbooks.	

Correct Answer:

Answer Area

In Azure Sentinel, you can automate common tasks by using

	▼
deep investigation tools.	
hunting search-and-query tools.	
playbooks.	
workbooks.	

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/overview>

QUESTION 10

In a Core eDiscovery workflow, what should you do before you can search for content?

- A. Create an eDiscovery hold.
- B. Run Express Analysis.
- C. Configure attorney-client privilege detection.
- D. Export and download results.

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide>

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
Authorization is used to identify the level of access to a resource.	<input type="radio"/>	<input type="radio"/>
Authentication is proving that users are who they say they are.	<input type="radio"/>	<input type="radio"/>
Authentication identifies whether you can read and write to a file.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Authorization is used to identify the level of access to a resource.	<input checked="" type="radio"/>	<input type="radio"/>
Authentication is proving that users are who they say they are.	<input checked="" type="radio"/>	<input type="radio"/>
Authentication identifies whether you can read and write to a file.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes

Authorization is the security process that determines a user or service's level of access.

Box 2: Yes

Authentication (AuthN) is a process that verifies that someone or something is who they say they are.

Box 3: No

Reference:

<https://www.onelogin.com/learn/authentication-vs-authorization>

QUESTION 12

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

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

D. Azure Blueprints

Correct Answer: D

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:

	Yes	No
You can use the insider risk management solution to detect phishing scams.	<input type="radio"/>	<input type="radio"/>
You can access the insider risk management solution from the Microsoft 365 compliance center.	<input type="radio"/>	<input type="radio"/>
You can use the insider risk management solution to detect data leaks by unhappy employees.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

	Yes	No
You can use the insider risk management solution to detect phishing scams.	<input type="radio"/>	<input checked="" type="radio"/>
You can access the insider risk management solution from the Microsoft 365 compliance center.	<input checked="" type="radio"/>	<input type="radio"/>
You can use the insider risk management solution to detect data leaks by unhappy employees.	<input checked="" type="radio"/>	<input type="radio"/>

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

QUESTION 14

HOTSPOT

You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

You need to create a new sensitive info type for the project codes. How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

(\s)(

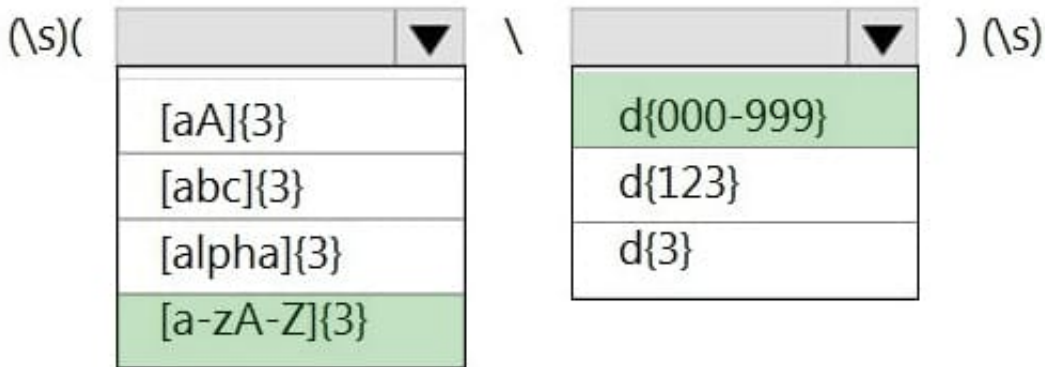
▼
[aA]{3}
[abc]{3}
[alpha]{3}
[a-zA-Z]{3}

 \

▼
d{000-999}
d{123}
d{3}

) (\s)

Correct Answer:



Reference: <https://joannecklein.com/2018/08/07/build-and-use-custom-sensitive-information-types-in-office-365/>

QUESTION 15

Which Azure Active Directory (Azure AD) feature can you use to evaluate group membership and automatically remove users that no longer require membership in a group?

- A. access reviews
- B. managed identities
- C. conditional access policies
- D. Azure AD Identity Protection

Correct Answer: A

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

[SC-900 VCE Dumps](#)

[SC-900 Practice Test](#)

[SC-900 Braindumps](#)