



Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.



SC-900 Practice Questions  
SC-900 Practice Test  
SC-900 Practice Exam  
SC-900 Exam Questions  
SC-900 Study Guide



[killexams.com](https://killexams.com)

**Microsoft**

# SC-900

*Microsoft Security, Compliance, and Identity Fundamentals*

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/SC-900>



### Question: 309

An organization uses Microsoft Entra ID to manage user identities. A security administrator configures a custom role with the following JSON definition to restrict access to specific Azure resources:

```
{
  "Name": "CustomReader",
  "Actions": [
    "Microsoft.Resources/subscriptions/resourceGroups/read"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/12345678-1234-1234-1234-1234567890ab"
  ]
}
```

Which identity concept is this configuration addressing?

- A. Authentication
- B. Authorization
- C. Directory Services
- D. Identity Providers

Answer: B

Explanation: The custom role defines permissions for accessing specific Azure resources, which is an aspect of authorization, determining what actions a user can perform after authentication.

### Question: 310

An organization uses Microsoft Purview to improve its compliance score. The compliance manager recommends implementing Microsoft 365 Insider Risk Management. How does this action impact the compliance score?

- A. It has no impact unless sensitivity labels are applied to user activities
- B. It increases the score by addressing improvement actions related to user behavior monitoring
- C. It decreases the score due to increased configuration complexity
- D. It only affects the score if DLP policies are disabled

Answer: B

Explanation: Implementing Microsoft 365 Insider Risk Management in Microsoft Purview addresses improvement actions related to monitoring user behavior for potential data risks, improving the compliance score. Sensitivity labels, DLP policies, and configuration complexity do not negate the positive impact of enabling Insider Risk Management.

### Question: 311

An organization uses Microsoft Sentinel as a SIEM solution. They configure an analytic rule to detect suspicious PowerShell activity using the KQL query below. The rule generates false positives for legitimate administrative tasks. What modification should the team make to reduce false positives?

Exhibit:

```
SecurityEvent
| where EventID == 4688
| where CommandLine contains "powershell"
| summarize ProcessCount = count() by Account, Computer, bin(TimeGenerated, 1h)
| where ProcessCount > 10
```

- A. Increase the ProcessCount threshold to 20
- B. Add a filter to exclude known administrative accounts
- C. Reduce the time window to 30 minutes
- D. Replace EventID 4688 with EventID 4104

Answer: B

Explanation: Filtering out known administrative accounts reduces false positives by excluding legitimate PowerShell usage. EventID 4688 tracks process creation, which is appropriate for detecting PowerShell execution. Increasing the threshold or reducing the time window may miss suspicious activity, and EventID 4104 (script block logging) requires additional configuration and may not cover all PowerShell activity.

### Question: 312

An organization implements a security strategy requiring continuous validation of user identities across all access attempts. The system uses machine learning to analyze user behavior patterns and triggers step-up authentication when anomalies are detected. Which model is this organization adopting?

- A. Defense-in-Depth
- B. Governance, Risk, and Compliance (GRC)

- C. Zero Trust
- D. Shared Responsibility Model

Answer: C

Explanation: The Zero Trust model emphasizes continuous validation of identities and assumes no implicit trust, requiring verification for every access attempt. Machine learning-based behavior analysis and step-up authentication align with Zero Trust principles, ensuring robust security by dynamically assessing risk.

### Question: 313

An organization implements Microsoft Entra ID and wants to enforce strong authentication for users accessing sensitive applications. The IT team configures a Conditional Access policy that requires multi-factor authentication (MFA) for all users. However, they notice that some users are still able to access applications without MFA. Confirm the users are part of a dynamic group

- B. Ensure the Conditional Access policy excludes trusted locations
- C. Verify the application's enterprise settings for MFA
- D. Which setting should be verified to ensure MFA is enforced?
- D. Check the Azure AD tenant's MFA registration policy

Answer: D

Explanation: The MFA registration policy in Microsoft Entra ID determines whether users are prompted to register for MFA. If users haven't registered, they may bypass Conditional Access policies requiring MFA. Excluding trusted locations could weaken enforcement but doesn't address registration. Application settings may require MFA but rely on user registration, and dynamic groups are unrelated to MFA enforcement.

### Question: 314

A company uses Azure to host a web application. The application stores sensitive customer data in an Azure SQL Database, encrypted using Transparent Data Encryption (TDE) with a customer-managed key stored in Azure Key Vault. Which component of the shared responsibility model is the customer responsible for securing?

- A. Physical infrastructure of Azure data centers
- B. Management of the Azure Key Vault service
- C. Configuration of the Azure SQL Database firewall
- D. Patching of the Azure SQL Database engine

Answer: C

Explanation: In the shared responsibility model, Microsoft is responsible for securing the physical infrastructure and patching the database engine, while the customer manages configurations like the Azure SQL Database firewall and the customer-managed key in Azure Key Vault.

**Question: 315**

An organization wants to use Compliance Manager to automate the assignment of compliance tasks to specific roles based on GDPR requirements. Which feature allows them to customize task workflows and assign responsibilities?

- A. Improvement Actions
- B. Assessment Templates
- C. Action Items
- D. Solutions

Answer: A

Explanation: Improvement Actions in Compliance Manager allow organizations to customize and assign compliance tasks, including GDPR-related responsibilities, with automated workflows. Action Items track tasks, Assessment Templates evaluate compliance, and Solutions provide general tools without task customization.

**Question: 316**

An organization uses Microsoft Purview to apply sensitivity labels. They want to ensure that documents labeled "Public" are accessible to external users without encryption. Which sensitivity label setting should be configured?

- A. Enable content marking with a watermark indicating "Public"
- B. Configure the label with no encryption and allow external user access
- C. Set up a DLP rule to allow external sharing of labeled documents
- D. Apply co-author permissions to allow external editing

Answer: B

Explanation: Sensitivity labels in Microsoft Purview can control encryption and access. Configuring a "Public" label with no encryption and allowing external user access ensures external users can view documents without restrictions. Content marking adds visual indicators, DLP rules control sharing but

not access, and co-author permissions are for editing, not access.

**Question: 317**

An administrator is configuring Microsoft Priva to detect overexposed personal data in Teams chats, such as passport numbers shared with external users. They need to set a policy with a confidence level of 90% and trigger alerts. Which Priva feature and configuration should they use?

- A. Data Loss Prevention, Teams Policy
- B. Privacy Risk Management, Overexposure Policy
- C. Records Management, Retention Label
- D. Subject Rights Request, Data Exposure

Answer: B

Explanation: Privacy Risk Management in Microsoft Priva allows configuring Overexposure Policies to detect sensitive data, like passport numbers in Teams, with a specified confidence level (90%) and trigger alerts. Data Loss Prevention focuses on preventing leaks, Records Management handles retention, and Subject Rights Requests address data queries.

**Question: 318**

An enterprise uses Microsoft Entra ID to secure access to a custom application. The application requires fine-grained access control based on user roles and group memberships. The IT team wants to implement a solution that dynamically assigns roles to users based on their attributes, such as department or location. Which Microsoft Entra ID feature should be used?

- A. Azure AD Privileged Identity Management (PIM)
- B. Role-based access control (RBAC)
- C. Dynamic group membership
- D. Static group assignments

Answer: C

Explanation: Dynamic group membership in Microsoft Entra ID allows groups to be populated automatically based on user attributes, such as department or location. This enables fine-grained access control when combined with role assignments for applications. PIM manages privileged roles, RBAC assigns roles but doesn't dynamically adjust group membership, and static group assignments require manual updates, which doesn't meet the dynamic requirement.

**Question: 319**

An organization uses Microsoft Entra ID to manage identities for a cloud-native application. The IT team needs to implement a solution that allows temporary access to resources for contractors without creating permanent accounts. Which Microsoft Entra ID feature supports this requirement?

- A. Entitlement Management
- B. Azure AD B2C
- C. Azure AD B2B collaboration
- D. Privileged Identity Management

Answer: A

Explanation: Entitlement Management in Microsoft Entra ID allows organizations to manage access packages, enabling temporary access for users like contractors without permanent accounts. Azure AD B2B is for external collaboration, B2C is for consumer apps, and PIM manages privileged roles, none of which directly support temporary access management.

KILL EXAMS

KILL EXAMS

## Question: 320

### HOTSPOT

Select the answer that correctly completes the sentence.

#### Answer Area

Azure Active Directory (Azure AD) is  
used for authentication and authorization.

an extended detection and response (XDR) system
an identity provider
a management group
a security information and event management (SIEM) system

#### Answer: Answer Area

Azure Active Directory (Azure AD) is  
used for authentication and authorization.

an extended detection and response (XDR) system
an identity provider
a management group
a security information and event management (SIEM) system

Explanation:

Graphical user interface, text, application

Description automatically generated

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide>

## Question: 321

### 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 Policy supports automatic remediation.	<input type="radio"/>	<input type="radio"/>
Azure Policy can be used to ensure that new resources adhere to corporate standards.	<input type="radio"/>	<input type="radio"/>
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	<input type="radio"/>	<input type="radio"/>

## Answer: Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Policy can be used to ensure that new resources adhere to corporate standards.	<input checked="" type="radio"/>	<input type="radio"/>
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Graphical user interface, text, application, email

Description automatically generated

## Question: 322

DRAG DROP

Match the Azure networking service to the appropriate description.

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

NOTE: Each correct match is worth one point.

Services	Answer Area
Azure Bastion	Service Provides Network Address Translation (NAT) services
Azure Firewall	Service Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Service Provides traffic filtering that can be applied to specific network interfaces on a virtual network

**Answer:**

Services	Answer Area
Azure Bastion	Azure Firewall Provides Network Address Translation (NAT) services
Azure Firewall	Azure Bastion Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Network security group (NSG) Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Explanation:

Graphical user interface, application

Description automatically generated

Box 1: Azure Firewall

Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.

Box 2: Azure Bastion

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

Box 3: Network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network.

**Question: 323**

HOTSPOT

Select the answer that correctly completes the sentence.

**Answer Area**

You can use  in the Microsoft 365 security center to identify devices that are affected by an alert.

classifications
incidents
policies
Secure score

**Answer:**

## Answer Area

You can use

classifications
incidents
policies
Secure score

in the Microsoft 365 security center to identify devices that are affected by an alert.

Explanation:

Text, letter

Description automatically generated

Question: 324

HOTSPOT

Select the answer that correctly completes the sentence.

## Answer Area

Azure Advisor
Azure Bastion
Azure Monitor
Azure Sentinel

is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Answer:

## Answer Area

Azure Advisor
Azure Bastion
Azure Monitor
Azure Sentinel

is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Explanation:

Text

Description automatically generated

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Question: 325

HOTSPOT

Select the answer that correctly completes the sentence.

## Answer Area

Azure DDoS Protection Standard can be used to protect

	▼
Azure Active Directory (Azure AD) applications.	
Azure Active Directory (Azure AD) users.	
resource groups.	
virtual networks.	

## Answer: Answer Area

Azure DDoS Protection Standard can be used to protect

	▼
Azure Active Directory (Azure AD) applications.	
Azure Active Directory (Azure AD) users.	
resource groups.	
virtual networks.	

Explanation:

Graphical user interface, text

Description automatically generated

Question: 326

HOTSPOT

Select the answer that correctly completes the sentence.

## Answer Area

	▼	is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.
Microsoft Cloud App Security		
Microsoft Defender for Endpoint		
Microsoft Defender for Identity		
Microsoft Defender for Office 365		

## Answer: Answer Area

	▼	is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.
Microsoft Cloud App Security		
Microsoft Defender for Endpoint		
Microsoft Defender for Identity		
Microsoft Defender for Office 365		

Explanation:

Graphical user interface, text

Description automatically generated with medium confidence

Question: 327

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Customer Lockbox
Data loss prevention (DLP)
eDiscovery
A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Answer:

Answer Area

Customer Lockbox
Data loss prevention (DLP)
eDiscovery
A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Explanation:

Graphical user interface, application

Description automatically generated

Question: 328

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

Explanation:

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: 329

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
Sensitivity labels can be used to encrypt documents.	<input type="radio"/>	<input type="radio"/>
Sensitivity labels can add headers and footers to documents.	<input type="radio"/>	<input type="radio"/>
Sensitivity labels can apply watermarks to emails.	<input type="radio"/>	<input type="radio"/>

**Answer:**

**Answer Area**

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity labels can add headers and footers to documents.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity labels can apply watermarks to emails.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Graphical user interface, text, application

Description automatically generated

Box 1: Yes

You can use sensitivity labels to provide protection settings that include encryption of emails and documents to prevent unauthorized people from accessing this data.

Box 2: Yes

You can use sensitivity labels to mark the content when you use Office apps, by adding watermarks, headers, or footers to documents that have the label applied.

Box 3: Yes

You can use sensitivity labels to mark the content when you use Office apps, by adding headers, or footers to email that have the label applied.

### Question: 330

What do you use to provide real-time integration between Azure Sentinel and another security source?

- A. Azure AD Connect
- B. a Log Analytics workspace
- C. Azure Information Protection
- D. a connector

**Answer:** D

Explanation:

To on-board Azure Sentinel, you first need to connect to your security sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, including Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity, and Microsoft Cloud App Security, etc.

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

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



## Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

## Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

## Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllabus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

## Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

## Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.