



## **Microsoft**

### **Exam Questions SC-900**

Microsoft Security, Compliance and Identity Fundamentals

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**

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 Sentinel data connectors support only Microsoft services.	<input type="radio"/>	<input type="radio"/>
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	<input type="radio"/>	<input type="radio"/>
Hunting provides you with the ability to identify security threats before an alert is triggered.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	<input checked="" type="radio"/>	<input type="radio"/>
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	<input checked="" type="radio"/>	<input type="radio"/>
Hunting provides you with the ability to identify security threats before an alert is triggered.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 2**

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
Digitally signing a document requires a private key.	<input type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the public key of the signer.	<input type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the private key of the singer.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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: Yes

**NEW QUESTION 3**

What is the purpose of Azure Active Directory (Azure AD) Password Protection?

- A. to control how often users must change their passwords
- B. to identify devices to which users can sign in without using multi-factor authentication (MFA)
- C. to encrypt a password by using globally recognized encryption standards
- D. to prevent users from using specific words in their passwords

**Answer:** D

**Explanation:**

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your

organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

**NEW QUESTION 4**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

provides benchmark recommendations and guidance for protecting Azure services.

- Azure Application Insights
- Azure Network Watcher
- Log Analytics workspaces
- Security baselines for Azure

**NEW 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.

**Answer Area**

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	<input type="radio"/>	<input type="radio"/>
Global administrator is a role in Azure Active Directory (Azure AD).	<input type="radio"/>	<input type="radio"/>
An Azure Active Directory (Azure AD) user can be assigned only one role.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

Azure AD supports custom roles.

Box 2: Yes

Global Administrator has access to all administrative features in Azure Active Directory. Box 3: No

**NEW 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.

**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"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**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"/>

**NEW QUESTION 7**

**HOTSPOT**

Select the answer that correctly completes the sentence.

In Azure Sentinel, you can automate common tasks by using

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

In Azure Sentinel, you can automate common tasks by using

**NEW QUESTION 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.

**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"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

Box 2: No

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

**NEW QUESTION 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
You can restrict communication between users in Exchange Online by using Information Barriers.	<input type="radio"/>	<input type="radio"/>
You can restrict accessing a SharePoint Online site by using Information Barriers.	<input type="radio"/>	<input type="radio"/>
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	<input checked="" type="radio"/>	<input type="radio"/>
You can restrict accessing a SharePoint Online site by using Information Barriers.	<input type="radio"/>	<input type="radio"/>
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	<input type="radio"/>	<input type="radio"/>

**NEW QUESTION 10**

Which Microsoft portal provides information about how Microsoft manages privacy, compliance, and security?

- A. Microsoft Service Trust Portal
- B. Compliance Manager
- C. Microsoft 365 compliance center
- D. Microsoft Support

Answer: A

Explanation:

Reference:

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

**NEW QUESTION 10**

What are two reasons to deploy multiple virtual networks instead of using just one virtual network? Each correct answer presents a complete solution.

NOTE; Each correct selection is worth one point.

- A. to separate the resources for budgeting
- B. to meet Governance policies
- C. to isolate the resources
- D. to connect multiple types of resources

Answer: BC

**NEW QUESTION 11**

What are two capabilities of Microsoft Defender for Endpoint? Each correct selection presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. automated investigation and remediation
- B. transport encryption
- C. shadow IT detection
- D. attack surface reduction

Answer: AD

Explanation:

Reference:

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

**NEW 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.

**Answer Area**

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (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"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No  
 Box 2: Yes  
 Leaked Credentials indicates that the user's valid credentials have been leaked.  
 Box 3: Yes  
 Multi-Factor Authentication can be required based on conditions, one of which is user risk.

**NEW QUESTION 18**

**HOTSPOT**

Select the answer that correctly completes the sentence.

**Answer Area**

a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- Encrypting

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- Encrypting

**NEW QUESTION 22**

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)

**Answer:** C

**Explanation:**

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

**NEW QUESTION 25**

**HOTSPOT**

Select the answer that correctly completes the sentence.

When users sign in to the Azure portal, they are first

assigned permissions.
authenticated.
authorized.
resolved.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

When users sign in to the Azure portal, they are first

assigned permissions.
authenticated.
authorized.
resolved.

**NEW QUESTION 30**

HOTSPOT

Select the answer that correctly completes the sentence.

**Answer Area**

Multi-factor authentication (MFA)
Pass-through authentication
Password writeback
Single sign-on (SSO)

requires additional verification, such as a verification code sent to a mobile phone.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

**NEW QUESTION 35**

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 AD Identity Protection generates risk detections once a user is authenticated.	<input type="radio"/>	<input type="radio"/>
Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	<input type="radio"/>	<input type="radio"/>
A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Statements	Yes	No
Azure AD Identity Protection generates risk detections once a user is authenticated.	<input checked="" type="radio"/>	<input type="radio"/>
Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	<input checked="" type="radio"/>	<input type="radio"/>
A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	<input checked="" type="radio"/>	<input type="radio"/>

### NEW QUESTION 39

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

**Answer: B**

#### Explanation:

Microsoft Secure Score for Devices

? Artikel

? 12.05.2022

? 3 Minuten Lesedauer Applies to:

? Microsoft Defender for Endpoint Plan 2

? Microsoft Defender Vulnerability Management

? 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](mailto: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:

? Application

? Operating system

? Network

? Accounts

? Security controls

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

Turn on the Microsoft Secure Score connector

Forward 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.

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

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

? Select Save preferences. How it works

Microsoft 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:

? Compare collected configurations to the collected benchmarks to discover misconfigured assets

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

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

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

### NEW QUESTION 44

HOTSPOT

Select the answer that correctly completes the sentence.

In an environment that has on-premises resources and cloud resources,

the cloud
a firewall
identity
Microsoft Defender for Cloud

should be the primary security perimeter.

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

In an environment that has on-premises resources and cloud resources,

the cloud
a firewall
identity
Microsoft Defender for Cloud

should be the primary security perimeter.

**NEW QUESTION 49**

HOTSPOT

Select the answer that correctly completes the sentence.

<input type="text" value=""/>	▼
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.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text  
 Description automatically generated

**NEW QUESTION 54**

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 Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	<input type="radio"/>	<input type="radio"/>
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	<input type="radio"/>	<input type="radio"/>
Microsoft Secure Score in the Microsoft 365 security center gives you points if you address the improvement action by using a third-party application or software.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, letter  
 Description automatically generated

**NEW QUESTION 57**

Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. fingerprint
- B. facial recognition
- C. PIN
- D. email verification
- E. security question

**Answer:** ABC

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication>

**NEW QUESTION 61**

Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your organization?

- A. sensitivity label policies
- B. Customer Lockbox
- C. information Barriers
- D. Privileged Access Management (PAM)

**Answer:** C

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers>

**NEW QUESTION 64**

**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 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"/>
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area

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"/>
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 67**

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>

**NEW QUESTION 71**

**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"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**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>

**NEW QUESTION 73**

What is a use case for implementing information barrier policies in Microsoft 365?

- A. to restrict unauthenticated access to Microsoft 365
- B. to restrict Microsoft Teams chats between certain groups within an organization
- C. to restrict Microsoft Exchange Online email between certain groups within an organization
- D. to restrict data sharing to external email recipients

**Answer: B**

**Explanation:**

Information barriers are supported in Microsoft Teams, SharePoint Online, and OneDrive for Business. A compliance administrator or information barriers administrator can define policies to allow or prevent communications between groups of users in Microsoft Teams. Information barrier policies can be used for situations like these:

**NEW QUESTION 76**

HOTSPOT

Select the answer that correctly completes the sentence.

**Answer Area**



**Answer Area**



**Answer Area**



**Answer Area**



Answer:

- A. Mastered
- B. Not Mastered

**Answer: A**

**NEW QUESTION 77**

Which statement represents a Microsoft privacy principle?

- A. Microsoft does not collect any customer data.
- B. Microsoft uses hosted customer email and chat data for targeted advertising.
- C. Microsoft manages privacy settings for its customers.
- D. Microsoft respects the local privacy laws that are applicable to its customers.

**Answer: C**

**NEW QUESTION 81**

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
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	<input type="radio"/>	<input type="radio"/>
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	<input type="radio"/>	<input type="radio"/>
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

The MailItemsAccessed event is a mailbox auditing action and is triggered when mail data is accessed by mail protocols and mail clients.

Box 2: No

Basic Audit retains audit records for 90 days.

Advanced Audit retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This is accomplished by a default audit log retention policy that retains any audit record that contains the value of Exchange, SharePoint, or AzureActiveDirectory for the Workload property (which indicates the service in which the activity occurred) for one year.

Box 3: yes

Advanced Audit in Microsoft 365 provides high-bandwidth access to the Office 365 Management Activity API.

**NEW QUESTION 84**

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

**Answer:** D

**NEW QUESTION 85**

HOTSPOT

Select the answer that correctly completes the sentence.

**Answer Area**

With Windows Hello for Business, a user's biometric data used for authentication

<input type="radio"/> is stored on an external device.
<input type="radio"/> is stored on a local device only.
<input type="radio"/> is stored in Azure Active Directory (Azure AD).
<input type="radio"/> is replicated to all the devices designated by the user.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, letter

Description automatically generated

Biometrics templates are stored locally on a device. Reference: <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

**NEW QUESTION 88**

HOTSPOT

Select the answer that correctly completes the sentence.

<input type="radio"/>
<input type="radio"/> Customer Lockbox
<input type="radio"/> Information barriers
<input type="radio"/> Privileged Access Management (PAM)
<input type="radio"/> 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.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



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.

**NEW QUESTION 91**

What is an assessment in Compliance Manager?

- A. A grouping of controls from a specific regulation, standard or policy.
- B. Recommended guidance to help organizations align with their corporate standards.
- C. A dictionary of words that are not allowed in company documents.
- D. A policy initiative that includes multiple policies.

**Answer:** A

**Explanation:**

Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps you manage your organization's compliance requirements with greater ease and convenience. Compliance Manager can help you throughout your compliance journey, from taking inventory of your data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Watch the video below to learn how Compliance Manager can help simplify how your organization manages compliance:

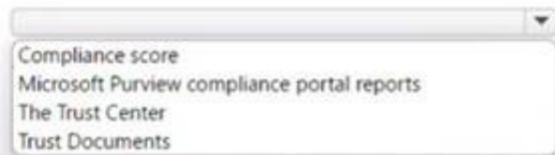
Compliance Manager helps simplify compliance and reduce risk by providing:

- ? Pre-built assessments for common industry and regional standards and regulations, or custom assessments to meet your unique compliance needs (available assessments depend on your licensing agreement; learn more).
- ? Workflow capabilities to help you efficiently complete your risk assessments through a single tool.
- ? Detailed step-by-step guidance on suggested improvement actions to help you comply with the standards and regulations that are most relevant for your organization. For actions that are managed by Microsoft, you'll see implementation details and audit results.
- ? A risk-based compliance score to help you understand your compliance posture by measuring your progress in completing improvement actions.

**NEW QUESTION 93**

**HOTSPOT**

Select the answer that correctly completes the sentence.



measures a company's progress in completing actions that help reduce risks

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



measures a company's progress in completing actions that help reduce risks

**NEW QUESTION 97**

**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
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	<input type="radio"/>	<input type="radio"/>
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	<input type="radio"/>	<input type="radio"/>
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	<input checked="" type="radio"/>	<input type="radio"/>
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 102**

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
Compliance Manager tracks only customer-managed controls.	<input type="radio"/>	<input type="radio"/>
Compliance Manager provides predefined templates for creating assessments.	<input type="radio"/>	<input type="radio"/>
Compliance Manager can help you assess whether data adheres to specific data protection standards.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

Compliance Manager tracks Microsoft managed controls, customer-managed controls, and shared controls. Box 2: Yes

Box 3: Yes

**NEW QUESTION 103**

HOTSPOT

Select the answer that correctly completes the sentence.

A domain controller

Active Directory Domain Services (AD DS)

Azure Active Directory (Azure AD) Privilege Identity Management (PIM)

Federation

provides single sign-on (SSO) capabilities across multiple identity providers.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A domain controller

Active Directory Domain Services (AD DS)

Azure Active Directory (Azure AD) Privilege Identity Management (PIM)

Federation

provides single sign-on (SSO) capabilities across multiple identity providers.

**NEW QUESTION 106**

What can you use to provide a user with a two-hour window to complete an administrative task in Azure?

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- B. Azure Multi-Factor Authentication (MFA)
- C. Azure Active Directory (Azure AD) Identity Protection
- D. conditional access policies

**Answer:** D

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>  
 Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management: Provide just-in-time privileged access to Azure AD and Azure resources Assign time-bound access to resources using start and end dates Require approval to activate privileged roles Enforce multi-factor authentication to activate any role Use justification to understand why users activate Get notifications when privileged roles are activated Conduct access reviews to ensure users still need roles Download audit history for internal or external audit Prevents removal of the last active Global Administrator role assignment

**NEW QUESTION 111**

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 Active Directory (Azure AD) is deployed to an on-premises environment.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) is an identity and access management service.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: No  
 Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.  
 Box 2: Yes  
 Microsoft 365 uses Azure Active Directory (Azure AD). Azure Active Directory (Azure AD) is included with your Microsoft 365 subscription.  
 Box 3: Yes  
 Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

**NEW QUESTION 113**

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
Device identity can be stored in Azure AD.	<input type="radio"/>	<input type="radio"/>
A single system-assigned managed identity can be used by multiple Azure resources.	<input type="radio"/>	<input type="radio"/>
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Statements	Yes	No
Device identity can be stored in Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
A single system-assigned managed identity can be used by multiple Azure resources.	<input checked="" type="radio"/>	<input type="radio"/>
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 114**

Which three tasks can be performed by using Azure Active Directory (Azure AD) Identity Protection? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Configure external access for partner organizations.
- B. Export risk detection to third-party utilities.
- C. Automate the detection and remediation of identity based-risks.

- D. Investigate risks that relate to user authentication.
- E. Create and automatically assign sensitivity labels to data.

**Answer:** BCD

**NEW QUESTION 117**

HOTSPOT

Select the answer that correctly completes the sentence.

An Azure resource can use a system-assigned  to access Azure services.

Azure Active Directory (Azure AD) joined device  
managed identity  
service principal  
user identity

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

An Azure resource can use a system-assigned  to access Azure services.

Azure Active Directory (Azure AD) joined device  
managed identity  
service principal  
user identity

**NEW QUESTION 119**

Which Microsoft 365 compliance feature can you use to encrypt content automatically based on specific conditions?

- A. Content Search
- B. sensitivity labels
- C. retention policies
- D. eDiscovery

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 123**

You have an Azure subscription that contains a Log Analytics workspace. You need to onboard Microsoft Sentinel. What should you do first?

- A. Create a hunting query.
- B. Correlate alerts into incidents.
- C. Connect to your security sources.
- D. Create a custom detection rule.

**Answer:** B

**NEW QUESTION 128**

.....

## Relate Links

**100% Pass Your SC-900 Exam with Examible Prep Materials**

<https://www.exambible.com/SC-900-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>