



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
You can use information barriers with Microsoft Exchange.	<input type="radio"/>	<input type="radio"/>
You can use information barriers with Microsoft SharePoint.	<input type="radio"/>	<input type="radio"/>
You can use information barriers with Microsoft Teams.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
You can use information barriers with Microsoft Exchange.	<input type="radio"/>	<input checked="" type="radio"/>
You can use information barriers with Microsoft SharePoint.	<input checked="" type="radio"/>	<input type="radio"/>
You can use information barriers with Microsoft Teams.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 2

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Azure Blueprints

Azure Policy

The Microsoft Cloud Adoption Framework for Azure

A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure Blueprints

Azure Policy

The Microsoft Cloud Adoption Framework for Azure

A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

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

What can you specify in Microsoft 365 sensitivity labels?

- A. how long files must be preserved
- B. when to archive an email message
- C. which watermark to add to files
- D. where to store files

Answer: C

Explanation:

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

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

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 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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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"/>

NEW QUESTION 8

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 9

Which Azure Active Directory (Azure AD) feature can you use to restrict Microsoft Intune- managed devices from accessing corporate resources?

- A. network security groups (NSGs)
- B. Azure AD Privileged Identity Management (PIM)
- C. conditional access policies
- D. resource locks

Answer: B

NEW QUESTION 10

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:

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 checked="" type="radio"/>	<input type="radio"/>
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 10

What is a function of Conditional Access session controls?

- A. prompting multi-factor authentication (MFA)
- B. enable limited experiences, such as blocking download of sensitive information
- C. enforcing device compliance
- D. enforcing client app compliance

Answer: A

Explanation:

Conditional Access session controls enable user app access and sessions to be monitored and controlled in real time based on access and session policies. Based on this definition, the best answer for your question is B. enable limited experiences, such as blocking download of sensitive information.
<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

NEW QUESTION 14

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 16

DRAG DROP

Match the Microsoft 365 insider risk management workflow step to the appropriate task.

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

NOTE: Each correct match is worth one point.

Steps	Answer Area
Action	Review and filter alerts
Investigate	Create cases in the Case dashboard
Triage	Send a reminder of corporate policies to users

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Steps	Answer Area	
Action	Triage	Review and filter alerts
Investigate	Investigate	Create cases in the Case dashboard
Triage	Action	Send a reminder of corporate policies to users

NEW QUESTION 17

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 DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	<input type="radio"/>	<input type="radio"/>
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	<input type="radio"/>	<input type="radio"/>
Azure DDoS Protection Standard protects against protocol attacks.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area		
Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	<input type="radio"/>	<input checked="" type="radio"/>
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	<input type="radio"/>	<input checked="" type="radio"/>
Azure DDoS Protection Standard protects against protocol attacks.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 20

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining

availability.

availability.

confidentiality.

integrity.

transparency.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining

availability.

availability.

confidentiality.

integrity.

transparency.

NEW QUESTION 21

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 a hybrid identity in an on-premises Active Directory that syncs to Azure AD.		<input type="radio"/>	<input type="radio"/>
User accounts created in Azure AD sync automatically to an on-premises Active Directory.		<input type="radio"/>	<input type="radio"/>
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.		<input type="radio"/>	<input type="radio"/>

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 26

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

Explanation:

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

NEW QUESTION 31

You plan to implement a security strategy and place multiple layers of defense throughout a network infrastructure. Which security methodology does this represent?

- A. threat modeling
- B. identity as the security perimeter
- C. defense in depth
- D. the shared responsibility model

Answer: C

Explanation:

Reference:
<https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth>

NEW QUESTION 36

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
Communication compliance is configured by using the Microsoft 365 admin center.	<input type="radio"/>	<input type="radio"/>
Microsoft SharePoint Online supports communication compliance.	<input type="radio"/>	<input type="radio"/>
Communication compliance can remediate compliance issues.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

Communication compliance is configured by using the Microsoft 365 admin center.

Yes

☒

No

☐

Microsoft SharePoint Online supports communication compliance.

☒☐

Communication compliance can remediate compliance issues.

☐☒

NEW QUESTION 41

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).

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

Which three statements accurately describe the guiding principles of Zero Trust? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Define the perimeter by physical locations.
- B. Use identity as the primary security boundary.
- C. Always verify the permissions of a user explicitly.
- D. Always assume that the user system can be breached.
- E. Use the network as the primary security boundary.

Answer: BCD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/security/zero-trust/>

NEW QUESTION 48

HOTSPOT

Select the answer that correctly completes the sentence.

access

object

privileged access

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the lifecycle process.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

access

object

privileged access

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the lifecycle process.

NEW QUESTION 52

HOTSPOT

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

NOTE: Each correct selection is worth one point.

er Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

er Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input checked="" type="radio"/>
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	<input checked="" type="radio"/>	<input type="radio"/>
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 54

HOTSPOT

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

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"/>

NEW QUESTION 55

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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.

NEW QUESTION 59

In the Microsoft Cloud Adoption Framework for Azure, which two phases are addressed before the Ready phase? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Plan
- B. Manage
- C. Adopt
- D. Govern
- E. Define Strategy

Answer: AE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview>

NEW QUESTION 62

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 65

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 70

Which Microsoft Defender for Cloud metric displays the overall security health of an Azure subscription?

- A. resource health
- B. secure score
- C. the status of recommendations
- D. completed controls

Answer: B

NEW QUESTION 73

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.

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 75

HOTSPOT

Select the answer that correctly completes the sentence.

In the Microsoft 365 Defender portal, an incident is a collection of correlated

alerts
events
vulnerabilities
Microsoft Secure Score improvement actions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

In the Microsoft 365 Defender portal, an incident is a collection of correlated

alerts
events
vulnerabilities
Microsoft Secure Score improvement actions

NEW QUESTION 77

Which two tasks can you implement by using data loss prevention (DLP) policies in Microsoft 365? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Display policy tips to users who are about to violate your organization's policies.
- B. Enable disk encryption on endpoints.
- C. Protect documents in Microsoft OneDrive that contain sensitive information.
- D. Apply security baselines to devices.

Answer: AC

Explanation:

Reference:

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

NEW QUESTION 82

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 85

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
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input type="radio"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	<input type="radio"/>	<input checked="" type="radio"/>
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input checked="" type="radio"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 88

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

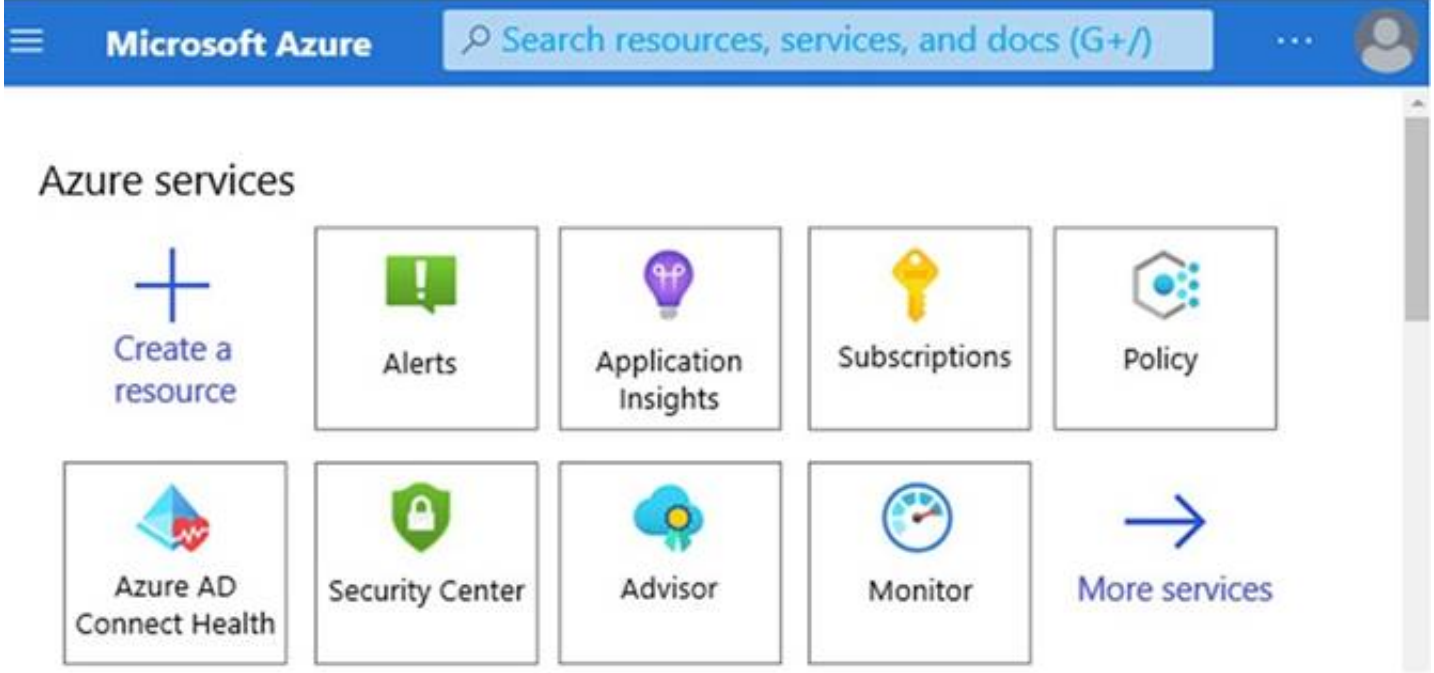
Explanation:

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 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"/>

NEW QUESTION 93

HOTSPOT

Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Security Center

NEW QUESTION 97

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

NEW QUESTION 102

What can you use to provide threat detection for Azure SQL Managed Instance?

- A. Microsoft Secure Score
- B. application security groups
- C. Microsoft Defender for Cloud
- D. Azure Bastion

Answer: C

NEW QUESTION 105

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 106

Which type of identity is created when you register an application with Active Directory (Azure AD)?

- A. a user account
B. a user-assigned managed identity
C. a system-assigned managed identity
D. a service principal

Answer: D

Explanation:

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

NEW QUESTION 108

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 110

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 115

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

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

is stored on an external device.
is stored on a local device only.
is stored in Azure Active Directory (Azure AD).
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 120

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>

NEW QUESTION 125

HOTSPOT

Select the answer that correctly completes the sentence.

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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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.

NEW QUESTION 128

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: AD

Explanation:

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

NEW QUESTION 131

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 133

HOTSPOT

Select the answer that correctly completes the sentence.

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

Compliance score

Microsoft Purview compliance portal reports

The Trust Center

Trust Documents

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Compliance score

Microsoft Purview compliance portal reports

The Trust Center

Trust Documents

NEW QUESTION 135

When you enable Azure AD Multi-Factor Authentication (MFA), how many factors are required for authentication?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

NEW QUESTION 138

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 143

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 asses 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 144

HOTSPOT

Select the answer that correctly completes the sentence.

<div><div>A domain controller</div><div>Active Directory Domain Services (AD DS)</div><div>Azure Active Directory (Azure AD) Privilege Identity Management (PIM)</div><div>Federation</div></div>	provides single sign-on (SSO) capabilities across multiple identity providers.
---	--

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

<div><div>A domain controller</div><div>Active Directory Domain Services (AD DS)</div><div>Azure Active Directory (Azure AD) Privilege Identity Management (PIM)</div><div>Federation</div></div>	provides single sign-on (SSO) capabilities across multiple identity providers.
---	--

NEW QUESTION 146

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 150

When security defaults are enabled for an Azure Active Directory (Azure AD) tenant, which two requirements are enforced? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. All users must authenticate from a registered device.
- B. Administrators must always use Azure Multi-Factor Authentication (MFA).
- C. Azure Multi-Factor Authentication (MFA) registration is required for all users.
- D. All users must authenticate by using passwordless sign-in.
- E. All users must authenticate by using Windows Hello.

Answer: BC

Explanation:

Security defaults make it easy to protect your organization with the following preconfigured security settings:

- ? Requiring all users to register for Azure AD Multi-Factor Authentication.
- ? Requiring administrators to do multi-factor authentication.
- ? Blocking legacy authentication protocols.
- ? Requiring users to do multi-factor authentication when necessary.
- ? Protecting privileged activities like access to the Azure portal.

Reference:

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

NEW QUESTION 152

Which three authentication methods can be used by Azure Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. phone call
- B. text message (SMS)
- C. email verification
- D. Microsoft Authenticator app
- E. security question

Answer: ABD

NEW QUESTION 153

HOTSPOT

Select the answer that correctly completes the sentence.

An Azure resource can use a system-assigned

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

 to access Azure services.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

An Azure resource can use a system-assigned

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

 to access Azure services.

NEW QUESTION 154

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 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"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 155

What can you use to scan email attachments and forward the attachments to recipients only if the attachments are free from malware?

- A. Microsoft Defender for Office 365
B. Microsoft Defender Antivirus
C. Microsoft Defender for Identity
D. Microsoft Defender for Endpoint

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description>

NEW QUESTION 158

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"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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.

NEW QUESTION 163

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
Global administrators are exempt from conditional access policies	<input type="radio"/>	<input type="radio"/>
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	<input type="radio"/>	<input type="radio"/>
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Global administrators are exempt from conditional access policies	<input type="radio"/>	<input checked="" type="radio"/>
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 164

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 166

.....

Relate Links

100% Pass Your SC-900 Exam with ExamBible 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/>