

# Microsoft

## Exam Questions SC-100

Microsoft Cybersecurity Architect



### NEW QUESTION 1

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling the VMAccess extension on all virtual machines.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### Explanation:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s> Adaptive Network Hardening:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify>

### NEW QUESTION 2

- (Exam Topic 3)

You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.

You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

- A. the Azure landing zone accelerator
- B. the Azure Will-Architected Framework
- C. Azure Security Benchmark v3
- D. Azure Advisor

**Answer: A**

### NEW QUESTION 3

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling adaptive network hardening.

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

#### Explanation:

JIT:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s>

Adaptive Network Hardening:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify>

### NEW QUESTION 4

- (Exam Topic 3)

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

- Azure IoT Edge devices
- AWS EC2 instances

Which services should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

For the IoT Edge devices:

For the AWS EC2 instances:

For the AWS EC2 instances:

Azure Arc  
Microsoft Defender for Cloud  
Microsoft Defender for Cloud Apps  
Microsoft Defender for Endpoint  
Microsoft Defender for IoT

Azure Arc only  
Microsoft Defender for Cloud and Azure Arc  
Microsoft Defender for Cloud Apps only  
Microsoft Defender for Cloud only  
Microsoft Defender for Endpoint and Azure Arc  
Microsoft Defender for Endpoint only

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
<https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings> <https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations>

**NEW QUESTION 5**

- (Exam Topic 3)  
You have a Microsoft 365 subscription  
You need to recommend a security solution to monitor the following activities:

- User accounts that were potentially compromised
- Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.  
NOTE: Each Correct selection is worth one Point.

**Components**  
A data loss prevention (DLP) policy  
Azure Active Directory (Azure AD) Conditional Access  
Azure Active Directory (Azure AD) Identity Protection  
Microsoft Defender for Cloud  
Microsoft Defender for Cloud Apps

**Answer Area**  
User accounts that were potentially compromised: 

Component

  
Users performing bulk file downloads from SharePoint Online: 

Component

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks> <https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exf> <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users>

**NEW QUESTION 6**

- (Exam Topic 3)  
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.  
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls.  
Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**  
<https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>

**NEW QUESTION 7**

- (Exam Topic 3)  
You have a Microsoft 365 subscription.  
You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.

Which two services should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Microsoft Defender for Cloud Apps
- B. Azure AD Application Proxy
- C. Azure Data Catalog
- D. Azure AD Conditional Access
- E. Microsoft Purview Information Protection

**Answer:** AD

#### NEW QUESTION 8

- (Exam Topic 3)

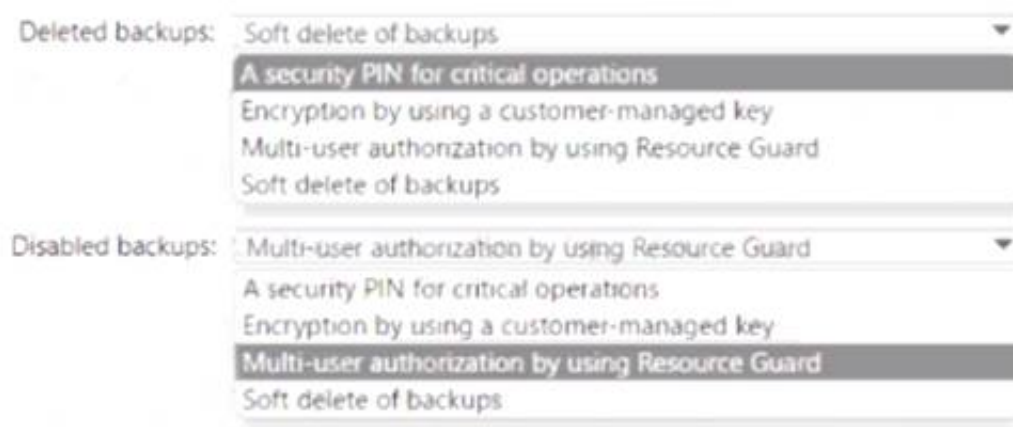
You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

- A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
- A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

What should you use for each risk? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

**Answer Area**



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**



#### NEW QUESTION 9

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.

You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

- A. Azure Monitor webhooks
- B. Azure Logics Apps
- C. Azure Event Hubs
- D. Azure Functions apps

**Answer:** B

**Explanation:**

The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance. Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

#### NEW QUESTION 10

- (Exam Topic 3)

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.



The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure. You plan to deploy Azure virtual machines that will run Windows Server. You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel. How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

EDR:	<input type="checkbox"/> Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD). <input type="checkbox"/> Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps. <input type="checkbox"/> Onboard the servers to Azure Arc. <input type="checkbox"/> Onboard the servers to Defender for Cloud.
SOAR:	<input type="checkbox"/> Configure Microsoft Sentinel analytics rules. <input type="checkbox"/> Configure Microsoft Sentinel playbooks. <input type="checkbox"/> Configure regulatory compliance standards in Defender for Cloud. <input type="checkbox"/> Configure workflow automation in Defender for Cloud.

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

For SOAR read this <https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks> Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of Microsoft Defender.  
<https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide>

**NEW QUESTION 10**

- (Exam Topic 3)

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure. You need to perform threat modeling by using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure. What should you use to start the threat modeling process?

- A. the STRIDE model  
 B. the DREAD model  
 C. OWASP threat modeling

**Answer: C**

**NEW QUESTION 15**

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DS). You need to recommend an identity security strategy that meets the following requirements:

- Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website
- Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned

The solution must minimize the need to deploy additional infrastructure components. What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

For the customers:	<input type="checkbox"/> Azure AD B2B authentication with access package assignments <input type="checkbox"/> Azure AD B2C authentication <input type="checkbox"/> Federation in Azure AD Connect with Active Directory Federation Services <input type="checkbox"/> Pass-through authentication in Azure AD Connect <input type="checkbox"/> Password hash synchronization in Azure AD Connect
For the partners:	<input type="checkbox"/> Azure AD B2B authentication with access package assignments <input type="checkbox"/> Azure AD B2C authentication <input type="checkbox"/> Federation in Azure AD Connect with Active Directory Federation Services <input type="checkbox"/> Pass-through authentication in Azure AD Connect <input type="checkbox"/> Password hash synchronization in Azure AD Connect

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, application Description automatically generated  
 Box 1 --> <https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview>  
 Box 2 --> <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers>

**NEW QUESTION 20**

- (Exam Topic 3)

You have Microsoft Defender for Cloud assigned to Azure management groups. You have a Microsoft Sentinel deployment. During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.  
NOTE: Each correct selection is worth one point.

- A. workload protections in Defender for Cloud
- B. threat intelligence reports in Defender for Cloud
- C. Microsoft Sentinel notebooks
- D. Microsoft Sentinel threat intelligence workbooks

**Answer:** BD

**Explanation:**

<https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports> <https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

**NEW QUESTION 22**

- (Exam Topic 3)

You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure. During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point

**Answer Area**

Threat modeling:

Actionable intelligence:

Dynamic application security testing (DAST):

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Threat modeling:

Actionable intelligence:

Dynamic application security testing (DAST):

**NEW QUESTION 23**

- (Exam Topic 3)

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. a relying party trust in Active Directory Federation Services (AD FS)
- C. Azure AD Application Proxy
- D. Azure AD B2C

**Answer:** A

**NEW QUESTION 24**

- (Exam Topic 3)

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Manage application identities securely and automatically.
- B. Manage the lifecycle of identities and entitlements
- C. Protect identity and authentication systems.
- D. Enable threat detection for identity and access management.
- E. Use a centralized identity and authentication system.

**Answer:** ACE

**NEW QUESTION 29**

- (Exam Topic 3)

Your company has an on-premises network and an Azure subscription.

The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.

You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.

You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.

What should you include in the recommendation?

- A. a private endpoint
- B. hybrid connections
- C. virtual network NAT gateway integration
- D. virtual network integration

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections>

**NEW QUESTION 30**

- (Exam Topic 3)

You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

- A. Add Microsoft Sentinel data connectors.
- B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
- C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
- D. Obtain Azure Active Directory Premium Plan 2 licenses.

**Answer:** A

**NEW QUESTION 33**

- (Exam Topic 3)

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.

All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

- Ensure that the security operations team can access the security logs and the operation logs.
- Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.

Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
- B. Use the Azure Monitor agent with the multi-homing configuration.
- C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
- D. Create a custom collector that uses the Log Analytics agent.

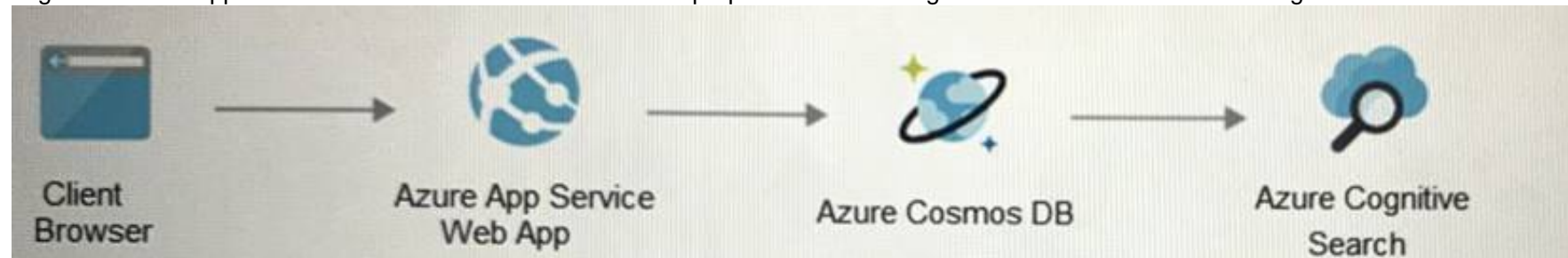
**Answer:** BC

**NEW QUESTION 37**



- (Exam Topic 3)

Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend creating private endpoints for the web app and the database layer. Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

<https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>

**NEW QUESTION 39**

- (Exam Topic 3)

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

- A. Azure Active Directory (Azure AD) Conditional Access App Control policies
- B. OAuth app policies in Microsoft Defender for Cloud Apps
- C. app protection policies in Microsoft Endpoint Manager
- D. application control policies in Microsoft Defender for Endpoint

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/sele>

**NEW QUESTION 42**

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription.

You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.

You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.

Which two components should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. data loss prevention (DLP) policies
- B. sensitivity label policies
- C. retention label policies
- D. eDiscovery cases

**Answer: AB**

**Explanation:**

Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate. Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used alongside capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.

<https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/> <https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?vie>

**NEW QUESTION 44**

- (Exam Topic 3)

You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.

You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:

- Automatically identify threats found in AWS CloudTrail events.
- Enforce security settings on AWS virtual machines by using Azure policies.

What should you include in the solution for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Automatically identify threats:

Microsoft Defender for Cloud

Azure Arc

Azure Log Analytics

Microsoft Defender for Cloud

Microsoft Sentinel

Enforce security settings:

Microsoft Sentinel

Azure Arc

Azure Log Analytics

Microsoft Defender for Cloud

Microsoft Sentinel

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Automatically identify threats:

Microsoft Defender for Cloud

Azure Arc

Azure Log Analytics

Microsoft Defender for Cloud

Microsoft Sentinel

Enforce security settings:

Microsoft Sentinel

Azure Arc

Azure Log Analytics

Microsoft Defender for Cloud

Microsoft Sentinel

NEW QUESTION 48

- (Exam Topic 3)

You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:

- Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- Users will authenticate by using Azure Active Directory (Azure AD) user accounts. You need to recommend an access security architecture for App1.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To enable Azure AD authentication for App1, use:

Azure AD application

Azure AD Application Proxy

Azure Application Gateway

A managed identity in Azure AD

Microsoft Defender for App

To implement access requests for App1, use:

An access package in Identity Governance

An access policy in Microsoft Defender for Cloud Apps

An access review in Identity Governance

Azure AD Conditional Access App Control

An OAuth app policy in Microsoft Defender for Cloud Apps

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1 is the Azure AD Application

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

Box 2 is Access Package in Identity Governance

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cr>

NEW QUESTION 52

- (Exam Topic 3)

Your company has devices that run either Windows 10, Windows 11, or Windows Server. You are in the process of improving the security posture of the devices.

You plan to use security baselines from the Microsoft Security Compliance Toolkit.

What should you recommend using to compare the baselines to the current device configurations?

- A. Microsoft Intune
- B. Policy Analyzer
- C. Local Group Policy Object (LGPO)
- D. Windows Autopilot

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework>

**NEW QUESTION 54**

- (Exam Topic 3)

Your company has Microsoft 365 E5 licenses and Azure subscriptions.

The company plans to automatically label sensitive data stored in the following locations:

- Microsoft SharePoint Online
- Microsoft Exchange Online
- Microsoft Teams

You need to recommend a strategy to identify and protect sensitive data.

Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Scopes	Answer Area
Files and emails	SharePoint Online: Scope
Groups and sites	Microsoft Teams: Scope
Schematized data assets	Exchange Online: Scope

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Groups and sites Box 2: Groups and sites Box 3: Files and emails –

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

**NEW QUESTION 58**

- (Exam Topic 3)

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?

- A. From Defender for Cloud, review the Azure security baseline for audit report.
- B. From Defender for Cloud, review the secure score recommendations.
- C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
- D. From Defender for Cloud, enable Defender for Cloud plans.

**Answer:** C

**Explanation:**

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regula>

**NEW QUESTION 63**

- (Exam Topic 2)

To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Security Assertion Markup Language (SAML)
- B. NTLMv2
- C. certificate-based authentication
- D. Kerberos

**Answer:** AD

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-o> <https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-w> <https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain>

**NEW QUESTION 64**

- (Exam Topic 2)

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

**Answer Area**

For connectivity from App Service web apps to virtual machines, use:	<input type="checkbox"/> Private endpoints <input type="checkbox"/> Service endpoints <input type="checkbox"/> Virtual network integration
For connectivity from virtual machines to App Service web apps, use:	<input type="checkbox"/> Private endpoints <input type="checkbox"/> Service endpoints <input type="checkbox"/> Virtual network integration

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Virtual Network Integration - correct

Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network.

Box 2: Private Endpoints. - correct

You can use Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link.

**NEW QUESTION 68**

- (Exam Topic 1)

You need to recommend a solution to meet the compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

To enforce compliance to the regulatory standard, create:	<input type="checkbox"/> An Azure Automation account <input type="checkbox"/> A blueprint <input type="checkbox"/> A managed identity <input type="checkbox"/> Workflow automation
To exclude TestRG from the compliance assessment:	<input type="checkbox"/> Edit an Azure blueprint <input type="checkbox"/> Modify a Defender for Cloud workflow automation <input type="checkbox"/> Modify an Azure policy definition <input type="checkbox"/> Update an Azure policy assignment

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1 = A Blueprint

Box 2 = Update an Azure Policy assignment

<https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#update-assignment-with> <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure>

while it is in policy assignment

- <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure>

**NEW QUESTION 70**

- (Exam Topic 1)

You need to recommend a solution to meet the security requirements for the virtual machines. What should you include in the recommendation?

- A. an Azure Bastion host
- B. a network security group (NSG)
- C. just-in-time (JIT) VM access
- D. Azure Virtual Desktop

**Answer: A**

**Explanation:**

The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image."

<https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image>

**NEW QUESTION 73**

- (Exam Topic 1)

You need to recommend a solution to meet the security requirements for the InfraSec group. What should you use to delegate the access?

- A. a subscription

- B. a custom role-based access control (RBAC) role
- C. a resource group
- D. a management group

**Answer:** B

#### NEW QUESTION 75

- (Exam Topic 3)

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Azure AD Conditional Access integration with user flows and custom policies
- B. Azure AD workbooks to monitor risk detections
- C. custom resource owner password credentials (ROPC) flows in Azure AD B2C
- D. access packages in Identity Governance
- E. smart account lockout in Azure AD B2C

**Answer:** AC

#### Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management>

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow>

#### NEW QUESTION 78

- (Exam Topic 3)

Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:

- Computers that run either Windows 10 or Windows 11
- Tablets and phones that run either Android or iOS

You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored. What should you include in the recommendation?

- A. eDiscovery
- B. retention policies
- C. Compliance Manager
- D. Microsoft Information Protection

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 79

- (Exam Topic 3)

Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool. Which type of diagram should you create?

- A. data flow
- B. system flow
- C. process flow
- D. network flow

**Answer:** A

#### Explanation:

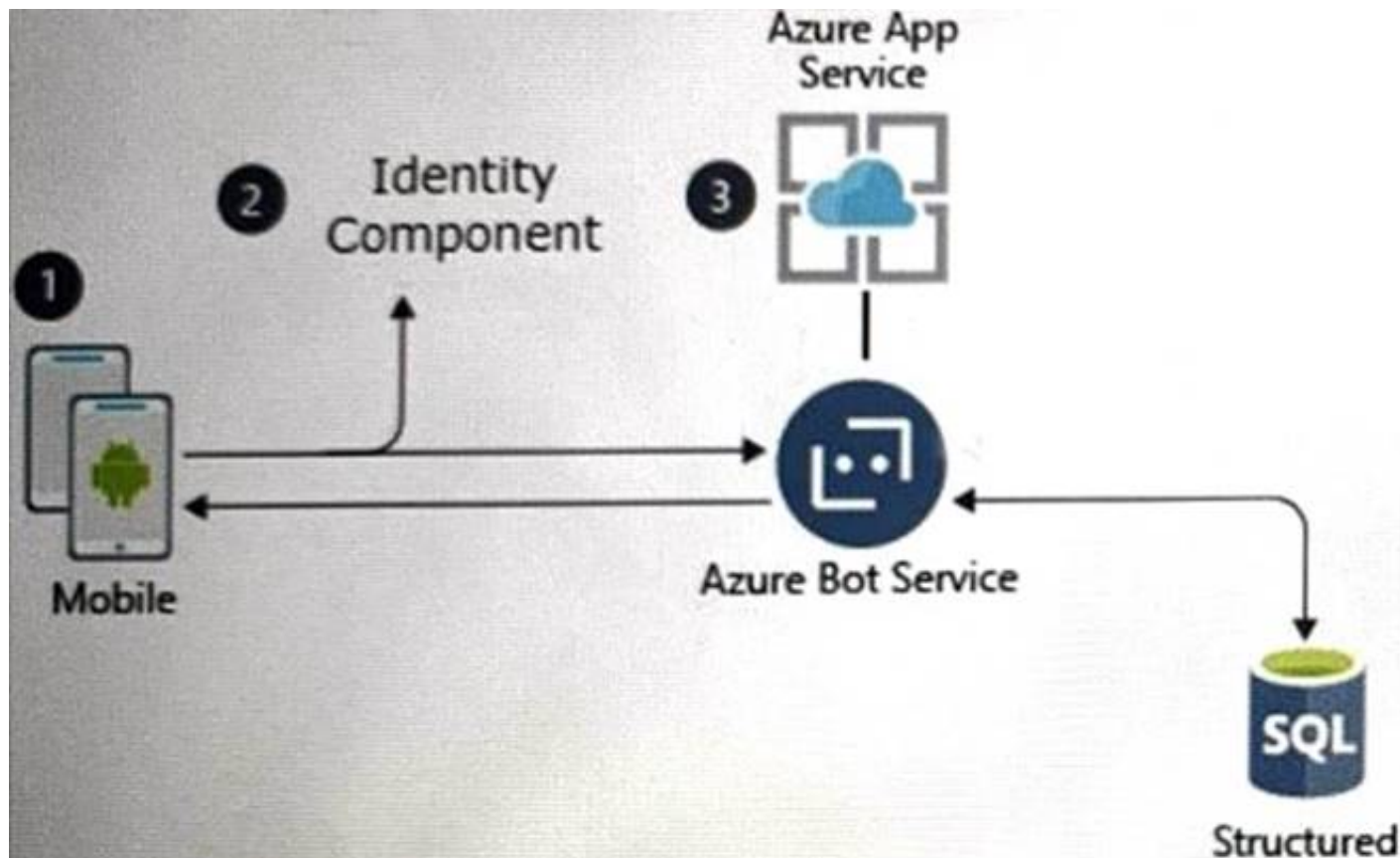
<https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram> <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started?source=recommen>

#### NEW QUESTION 82

- (Exam Topic 3)

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.





You need to design an identity strategy for the app. The solution must meet the following requirements:

- Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
- Be managed separately from the identity store of the customer.
- Support fully customizable branding for each app.

Which service should you recommend to complete the design?

- A. Azure Active Directory (Azure AD) B2C
- B. Azure Active Directory (Azure AD) B2B
- C. Azure AD Connect
- D. Azure Active Directory Domain Services (Azure AD DS)

**Answer: A**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow> <https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow>

#### NEW QUESTION 87

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically. What should you use?

- A. the regulatory compliance dashboard in Defender for Cloud
- B. Azure Policy
- C. Azure Blueprints
- D. Azure role-based access control (Azure RBAC)

**Answer: B**

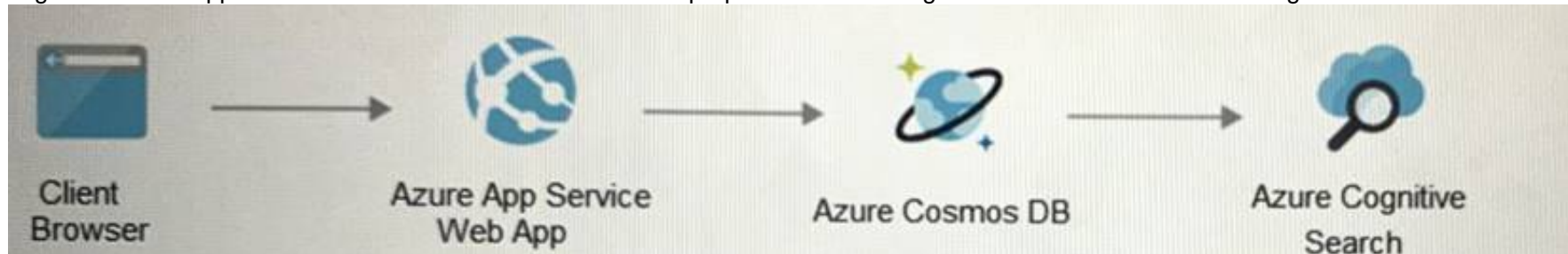
**Explanation:**

<https://azure.microsoft.com/en-us/blog/simplifying-your-environment-setup-while-meeting-compliance-needs-w>

#### NEW QUESTION 92

- (Exam Topic 3)

Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF).

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

#### NEW QUESTION 93

- (Exam Topic 3)

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1. What should you include in the design?

- A. Azure AD Application Proxy
- B. connected apps in Microsoft Defender for Cloud Apps
- C. Microsoft Entra Identity Governance
- D. access policies in Microsoft Defender for Cloud Apps

**Answer:** C

#### NEW QUESTION 94

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling just-in-time (JIT) VM access on all virtual machines.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

#### Explanation:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s>

#### NEW QUESTION 97

- (Exam Topic 3)

Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD). You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications. What should you include in the recommendation?

- A. activity policies in Microsoft Defender for Cloud Apps
- B. sign-in risk policies in Azure AD Identity Protection
- C. device compliance policies in Microsoft Endpoint Manager
- D. Azure AD Conditional Access policies
- E. user risk policies in Azure AD Identity Protection

**Answer:** A

#### Explanation:

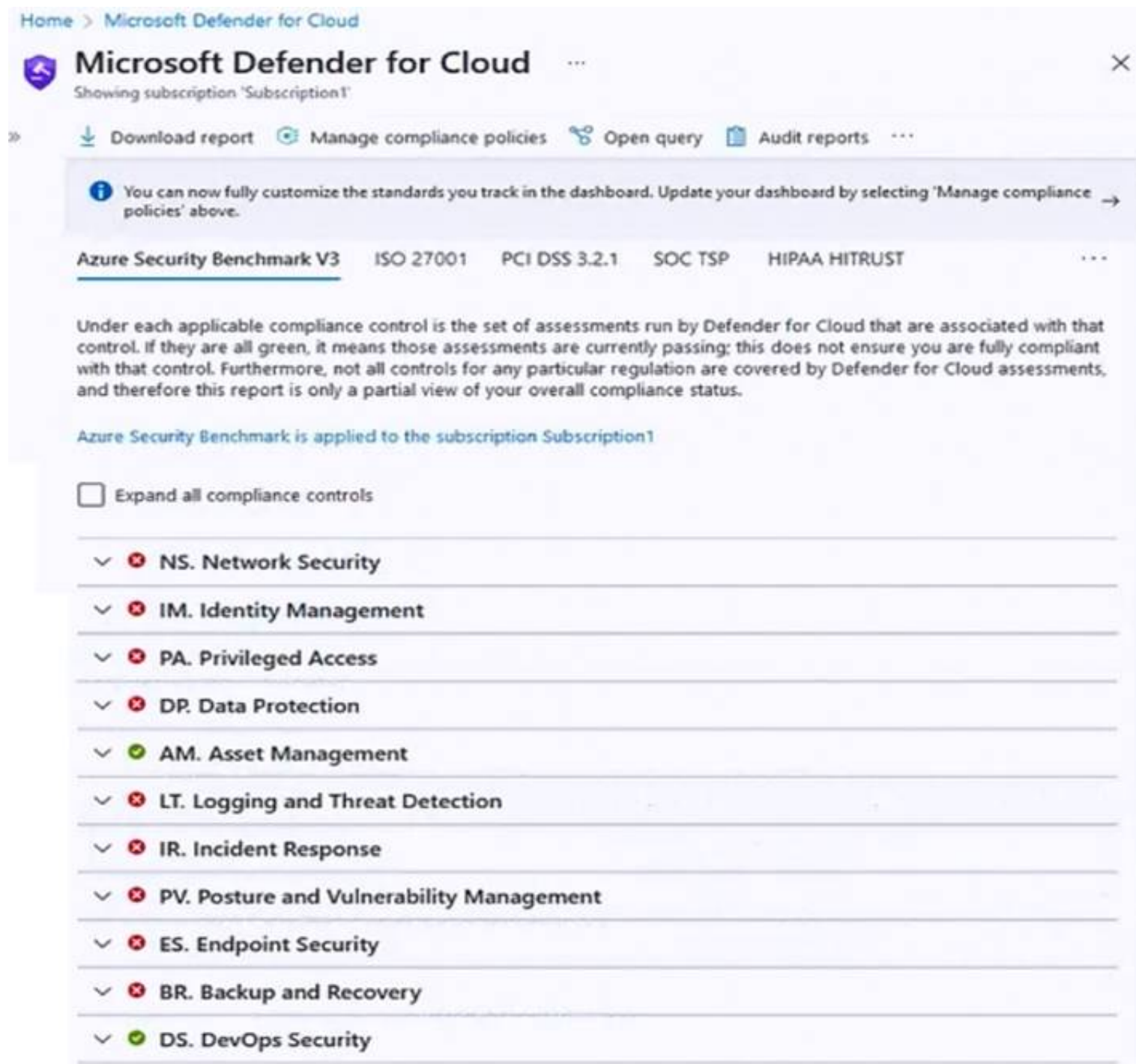
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-locate-trusted-ip-rules> <https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules>

#### NEW QUESTION 101

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.



You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

- A. Data Protection
- B. Incident Response
- C. Posture and Vulnerability Management
- D. Asset Management
- E. Endpoint Security

**Answer:** E

**Explanation:**

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security>

#### NEW QUESTION 106

- (Exam Topic 3)

Your company, named Contoso. Ltd... has an Azure AD tenant named contoso.com. Contoso has a partner company named Fabrikam. Inc. that has an Azure AD tenant named fabrikam.com. You need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:

- Follow the principle of least privilege.
- Minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Role to assign to the Fabrikam helpdesk users for contoso.com: Password Administrator

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use: A custom role

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords: Password Administrator

- A. Mastered
- B. Not Mastered



**Answer:** A

**Explanation:**

Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com: Password Administrator  
Directory Readers  
Helpdesk Administrator  
Password Administrator

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use: A custom role  
A custom role  
An access package  
An administrative unit

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords: Password Administrator  
Directory Readers  
Helpdesk Administrator  
Password Administrator

### NEW QUESTION 108

- (Exam Topic 3)

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices. You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.

What should you include in the response plan?

- A. controlled folder access
- B. application isolation
- C. memory scanning
- D. machine isolation
- E. user isolation

**Answer:** D

### NEW QUESTION 112

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Service: Microsoft Defender for Office 365  
Azure AD Identity Protection  
Microsoft Defender for DNS  
Microsoft Defender for Office 365  
Microsoft Purview

Policy type: Anti-phishing  
Anti-phishing  
Anti-spam  
Data loss prevention (DLP)  
Insider risk management

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Service: Microsoft Defender for Office 365  
Azure AD Identity Protection  
Microsoft Defender for DNS  
Microsoft Defender for Office 365  
Microsoft Purview

Policy type: Anti-phishing  
Anti-phishing  
Anti-spam  
Data loss prevention (DLP)  
Insider risk management



### NEW QUESTION 116

- (Exam Topic 3)

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

- Prevent the need to enable ports 3389 and 22 from the internet.
- Only provide permission to connect the virtual machines when required.
- Ensure that administrators use the Azure portal to connect to the virtual machines.

Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
- B. Configure Azure VPN Gateway.
- C. Enable Just Enough Administration (JEA).
- D. Enable just-in-time (JIT) VM access.
- E. Configure Azure Bastion.

**Answer:** DE

#### Explanation:

<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

### NEW QUESTION 118

- (Exam Topic 3)

Your company wants to optimize using Azure to protect its resources from ransomware.

You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Azure Backup:	<div>Encryption by using platform-managed keys</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>
Azure Storage:	<div>Immutable storage</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

**Answer Area**

Azure Backup:	<div>Encryption by using platform-managed keys</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>
Azure Storage:	<div>Immutable storage</div> <div>Access policies</div> <div>Access tiers</div> <div>Encryption by using platform-managed keys</div> <div>Immutable storage</div> <div>A security PIN</div>

### NEW QUESTION 121

- (Exam Topic 3)

You have legacy operational technology (OT) devices and IoT devices.

You need to recommend best practices for applying Zero Trust principles to the OT and IoT devices based on the Microsoft Cybersecurity Reference Architectures (MCRA). The solution must minimize the risk of disrupting business operations.

Which two security methodologies should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point

- A. passive traffic monitoring
- B. active scanning
- C. threat monitoring
- D. software patching

**Answer:** CD

### NEW QUESTION 122

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

The Chief Compliance Officer plans to enhance privacy management in the working environment. You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:

- Identify unused personal data and empower users to make smart data handling decisions.
- Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
- Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

- A. Microsoft Viva Insights
- B. Advanced eDiscovery
- C. Privacy Risk Management in Microsoft Priva
- D. communication compliance in insider risk management

**Answer: C**

**Explanation:**

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you: Detect overexposed personal data so that users can secure it. Spot and limit transfers of personal data across departments or regional borders. Help users identify and reduce the amount of unused personal data that you store.

<https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management>

**NEW QUESTION 123**

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure.

The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network.

The company's security policy prevents the use of personal devices for accessing company data and applications.

You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.

What should you include in the recommendation?

- A. Migrate the on-premises applications to cloud-based applications.
- B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
- C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
- D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop> <https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide> <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-c>

**NEW QUESTION 125**

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services {AD DS} domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.

You plan to remove all the domain accounts from the Administrators group on the Windows computers. You need to recommend a solution that will provide users with administrative access to the Windows

computers only when access is required. The solution must minimize the lateral movement of ransomware

attacks if an administrator account on a computer is compromised.

What should you include in the recommendation?

- A. Local Administrator Password Solution (LAPS)
- B. Privileged Access Workstations (PAWs)
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure AD identity Protection

**Answer: A**

**NEW QUESTION 130**

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are designing the encryption standards for data at rest for an Azure resource.

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses Microsoft-managed keys.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**NEW QUESTION 133**

- (Exam Topic 3)

Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be

scanned during the following two phases:

Uploading the code to repositories Building containers

Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.

**Answer Area**

Uploading code to repositories:

- Azure Boards
- Azure Pipelines
- GitHub Enterprise
- Microsoft Defender for Cloud

Building containers:

- Azure Boards
- Azure Pipelines
- GitHub Enterprise
- Microsoft Defender for Cloud

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec> <https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-conta>

#### NEW QUESTION 134

- (Exam Topic 3)

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity. You are informed about incidents that relate to compromised identities. You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?

- A. standalone sensors
- B. honeypot entity tags
- C. sensitivity labels
- D. custom user tags

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeypot-activity> The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

#### NEW QUESTION 136

- (Exam Topic 3)

Your company is moving a big data solution to Azure.

The company plans to use the following storage workloads:

- Azure Storage blob containers
- Azure Data Lake Storage Gen2
- Azure Storage file shares
- Azure Disk Storage

Which two storage workloads support authentication by using Azure Active Directory (Azure AD)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Azure Disk Storage
- B. Azure Storage blob containers
- C. Azure Storage file shares
- D. Azure Data Lake Storage Gen2

**Answer:** BD

**Explanation:**

<https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory> <https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-acc>

#### NEW QUESTION 138

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

- A. data classification content explorer
- B. data loss prevention (DLP)
- C. eDiscovery
- D. Information Governance

**Answer:** B



**NEW QUESTION 142**

- (Exam Topic 3)

You have a hybrid cloud infrastructure.

You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

App1:

Azure AD B2B authentication with Conditional Access

Azure AD B2C custom policies with Conditional Access

Azure Application Gateway Web Application Firewall policies

Azure Firewall

Azure VPN Gateway with network security group rules

Azure VPN Point-to-Site connections

App2:

Azure AD B2B authentication with Conditional Access

Azure AD B2C custom policies with Conditional Access

Azure Application Gateway Web Application Firewall policies

Azure Firewall

Azure VPN Gateway with network security group rules

Azure VPN Point-to-Site connections

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text Description automatically generated with medium confidence

**NEW QUESTION 145**

- (Exam Topic 3)

Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII). The company plans to use Microsoft Information Protection for the PII data store in Azure. You need to recommend a solution to discover PII data at risk in the Azure resources.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

To connect the Azure data sources to

Microsoft Information Protection:

Azure Purview

Endpoint data loss prevention

Microsoft Defender for Cloud Apps

Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

Azure Monitor

Endpoint data loss prevention

Microsoft Defender for Cloud

Microsoft Defender for Cloud Apps

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Prioritize security actions by data sensitivity,

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection>. As to Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics (Azure resources as well): <https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azu>



### NEW QUESTION 150

- (Exam Topic 3)

You have an Azure subscription that contains a Microsoft Sentinel workspace.

Your on-premises network contains firewalls that support forwarding event logs in the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls.

You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel. What should you include in the recommendation?

- A. an Azure logic app
- B. an on-premises Syslog server
- C. an on-premises data gateway
- D. Azure Data Factory

**Answer:** B

### NEW QUESTION 151

- (Exam Topic 3)

You plan to automate the development and deployment of a Node.js-based app by using GitHub. You need to recommend a DevSecOps solution for the app. The solution must meet the following requirements:

- Automate the generation of pull requests that remediate identified vulnerabilities.
- Automate vulnerability code scanning for public and private repositories.
- Minimize administrative effort.
- Minimize costs.

What should you recommend using? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**



- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

A close up of a text Description automatically generated

### NEW QUESTION 155

- (Exam Topic 3)

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.

You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attack surface. What should you include in the recommendation?

- A. Azure Firewall Premium
- B. Azure Application Gateway Web Application Firewall (WAF)
- C. network security groups (NSGs)
- D. Azure Traffic Manager and application security groups

**Answer:** D

#### Explanation:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection>

### NEW QUESTION 157

- (Exam Topic 3)

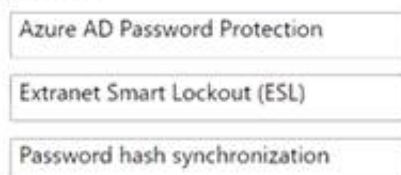
You have a hybrid Azure AD tenant that has pass-through authentication enabled. You are designing an identity security strategy.

You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.

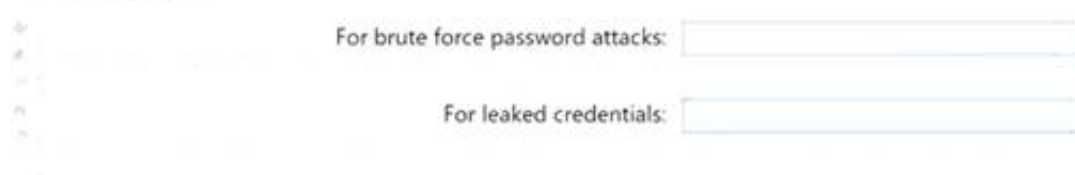
What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Features**



**Answer Area**

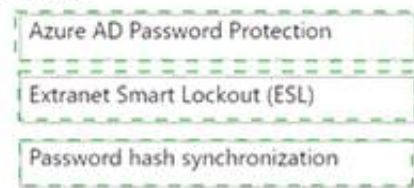


- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Features



Answer Area



#### NEW QUESTION 160

- (Exam Topic 3)

You have 50 Azure subscriptions.

You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.

NOTE: Each correct selection is worth one point.

- A. Assign an initiative to a management group.
- B. Assign a policy to each subscription.
- C. Assign a policy to a management group.
- D. Assign an initiative to each subscription.
- E. Assign a blueprint to each subscription.
- F. Assign a blueprint to a management group.

**Answer:** AF

**Explanation:**

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview> <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>  
<https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001> <https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

#### NEW QUESTION 161

- (Exam Topic 3)

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.

All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.

You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.

Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Use Azure Monitor notifications when backup configurations change.
- B. Require PINs for critical operations.
- C. Perform offline backups to Azure Data Box.
- D. Encrypt backups by using customer-managed keys (CMKs).
- E. Enable soft delete for backups.

**Answer:** AB

**Explanation:**

<https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware> 'You need to recommend which CONTROLS must be enabled to ENSURE that Azure Backup can be used to RESTORE the resources in the event of a successful ransomware attack.' Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.

#### NEW QUESTION 163

- (Exam Topic 3)

You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts. You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts. Which two configurations should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Enable Microsoft Defender for Cosmos DB.
- B. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.
- C. Disable local authentication for Azure Cosmos DB.
- D. Enable Microsoft Defender for Identity.
- E. Send the Azure Cosmos DB logs to a Log Analytics workspace.

**Answer:** BC

**Explanation:**

<https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs>

#### NEW QUESTION 164

- (Exam Topic 3)

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.

You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.

What should you include in the recommendation?

- A. Apply read-only locks on the storage accounts.
- B. Set the AllowShareKeyAccess property to false.
- C. Set the AllowBlobPublicAccess property to false.
- D. Configure automated key rotation.

**Answer:** A

**Explanation:**

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

**NEW QUESTION 166**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SC-100 Practice Exam Features:

- \* SC-100 Questions and Answers Updated Frequently
- \* SC-100 Practice Questions Verified by Expert Senior Certified Staff
- \* SC-100 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* SC-100 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SC-100 Practice Test Here](#)**