



**Vendor:** Microsoft

**Exam Code:** SC-900

**Exam Name:** Microsoft Security, Compliance, and Identity  
Fundamentals

**Version:** DEMO

### QUESTION 1

Which score measures an organization's progress in completing actions that help reduce risks associated to data protection and regulatory standards?

- A. Microsoft Secure Score
- B. Productivity Score
- C. Secure score in Azure Security Center
- D. Compliance score

**Answer: D**

**Explanation:**

Compliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide#understanding-your-compliance-score>

### QUESTION 2

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

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

**Answer: D**

**Explanation:**

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

Reference:

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

### QUESTION 3

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>

#### QUESTION 4

Which statement represents a Microsoft privacy principle?

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

**Answer: B**

**Explanation:**

Then, Strong legal protections. Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

<https://privacy.microsoft.com/en-US/#whatinformationwecollectmodule>

#### QUESTION 5

What does Conditional Access evaluate by using Azure Active Directory (Azure AD) Identity Protection?

- A. user actions
- B. group membership
- C. device compliance
- D. user risk

**Answer: D**

**Explanation:**

Its's user risk including the below:

- Anonymous IP address use
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

#### QUESTION 6

Which type of alert can you manage from the Microsoft 365 Defender portal?

- A. Microsoft Defender for Storage
- B. Microsoft Defender for SQL
- C. Microsoft Defender for Endpoint
- D. Microsoft Defender for IoT

**Answer: C**

**Explanation:**

The Alerts queue shows the current set of alerts. You get to the alerts queue from Incidents & alerts > Alerts on the quick launch of the Microsoft 365 Defender portal.

Alerts from different Microsoft security solutions like Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft 365 Defender appear here.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts>

## QUESTION 7

Drag and Drop Question

You are evaluating the compliance score in Compliance Manager.

Match the compliance score action subcategories to the appropriate actions.

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

NOTE: Each correct match is worth one point.

Action Subcategories		Answer Area
Corrective		Action subcategory Encrypt data at rest.
Detective		Action subcategory Perform a system access audit.
Preventative		Action subcategory Make configuration changes in response to a security incident.

**Answer:**

Action Subcategories		Answer Area
	Preventative	Encrypt data at rest.
	Detective	Perform a system access audit.
	Corrective	Make configuration changes in response to a security incident.

### Explanation:

Box 1: Preventative

Preventative actions address specific risks. For example, protecting information at rest using encryption is a preventative action against attacks and breaches.

Separation of duties is a preventative action to manage conflict of interest and guard against fraud.

Box 2: Detective

Detective actions actively monitor systems to identify irregular conditions or behaviors that represent risk, or that can be used to detect intrusions or breaches.

Examples include system access auditing and privileged administrative actions. Regulatory compliance audits are a type of detective action used to find process issues.

Box 3: Corrective

Corrective actions try to keep the adverse effects of a security incident to a minimum, take corrective action to reduce the immediate effect, and reverse the damage if possible. Privacy incident response is a corrective action to limit damage and restore systems to an operational state after a breach.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation>

#### QUESTION 8

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: C**

**Explanation:**

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal.

<https://docs.microsoft.com/zh-tw/azure/bastion/bastion-overview>

#### QUESTION 9

Which service includes the Attack simulation training feature?

- A. Microsoft Defender for Cloud Apps
- B. Microsoft Defender for Office 365
- C. Microsoft Defender for Identity
- D. Microsoft Defender for SQL

**Answer: B**

**Explanation:**

Attack simulation training in Microsoft Defender for Office 365 Plan 2 or Microsoft 365 E5 lets you run benign cyberattack simulations in your organization. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training>

#### QUESTION 10

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:**

Zero Trust is a security strategy. It is not a product or a service, but an approach in designing and implementing the following set of security principles:

- Verify explicitly

- Use least privilege access
- Assume breach

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

### QUESTION 11

Hotspot Question

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 use the insider risk management solution to detect phishing scams.	<input type="radio"/>	<input type="radio"/>
You can access the insider risk management solution from the Microsoft 365 compliance center.	<input type="radio"/>	<input type="radio"/>
You can use the insider risk management solution to detect data leaks by unhappy employees.	<input type="radio"/>	<input type="radio"/>

**Answer:**

#### Answer Area

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

#### Explanation:

Box 1: No

Phishing scams are external threats.

Box 2: Yes

Insider risk management is a compliance solution in Microsoft 365.

Box 3: Yes

Insider risk management helps minimize internal risks from users. These include:

- Leaks of sensitive data and data spillage
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide>

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

### QUESTION 12

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>

### QUESTION 13

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

**NOTE:** Each correct selection is worth one point.

- A. Configure external access for partner organizations.
- B. Export risk detection to third-party utilities.
- C. Automate the detection and remediation of identity based-risks.
- D. Investigate risks that relate to user authentication.
- E. Create and automatically assign sensitivity labels to data.

**Answer:** CDE

**Explanation:**

Identity Protection allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to other tools.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

#### QUESTION 14

You have a Microsoft 365 E3 subscription.

You plan to audit user activity by using the unified audit log and Basic Audit.

For how long will the audit records be retained?

- A. 15 days
- B. 30 days
- C. 90 days
- D. 180 days

**Answer: C**

#### Explanation:

Microsoft 365 unified auditing helps to track activities performed in the different Microsoft 365 services by both users and admins. Basic auditing is enabled by default for most Microsoft 365 organizations. In the Basic audit, audit records are retained and searchable for the last 90 days.

<https://o365reports.com/2021/07/07/microsoft-365-retrieve-audit-log-for-1-year-for-all-subscriptions/>

#### QUESTION 15

To which type of resource can Azure Bastion provide secure access?

- A. Azure Files
- B. Azure SQL Managed Instances
- C. Azure virtual machines
- D. Azure App Service

**Answer: C**

#### Explanation:

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

Reference:

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

#### QUESTION 16

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>

## QUESTION 17

Hotspot Question

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 add a resource lock to an Azure subscription.	<input type="radio"/>	<input type="radio"/>
You can add only one resource lock to an Azure resource.	<input type="radio"/>	<input type="radio"/>
You can delete a resource group containing resources that have resource locks.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
You can add a resource lock to an Azure subscription.	<input checked="" type="radio"/>	<input type="radio"/>
You can add only one resource lock to an Azure resource.	<input type="radio"/>	<input checked="" type="radio"/>
You can delete a resource group containing resources that have resource locks.	<input type="radio"/>	<input checked="" type="radio"/>

### Explanation:

If you have a Delete lock on a resource and attempt to delete its resource group, the whole delete operation is blocked. Even if the resource group or other resources in the resource group aren't locked, the deletion doesn't happen. You never have a partial deletion.

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

## Thank You for Trying Our Product

### Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



**10% Discount Coupon Code: ASTR14**