DUMPSBOSS.

Microsoft Security Compliance and Identity Fundamentals

Microsoft SC-900

Version Demo

Total Demo Questions: 40

Total Premium Questions: 400

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Describe the concepts of security, compliance, and identity	69
Topic 2, Describe the capabilities of Microsoft Entra	130
Topic 3, Describe the capabilities of Microsoft security solutions	110
Topic 4, Describe the capabilities of Microsoft compliance solutions	87
Topic 5, Mix Questions	4
Total	400

QUESTION NO: 1

You need to create a data loss prevention (DLP) policy. What should you use?

A. the Microsoft 365 admin center

B. the Microsoft Endpoint Manager admin center

C. the Microsoft 365 Defender portal

D. the Microsoft Purview portal

ANSWER: D

Explanation:

The Microsoft Purview portal is the appropriate place to create and manage Microsoft 365 data loss prevention (DLP) policies. DLP helps an organization identify, monitor, and protect sensitive information, such as credit card numbers, health information, or government-issued identifiers, when that information is used or shared across supported Microsoft 365 locations. From the portal, an administrator can create a policy by selecting built-in sensitive-information templates or defining policy conditions, then choosing the workloads and locations to protect, including Exchange email, SharePoint sites, OneDrive accounts, Teams chats and channel messages, and endpoint devices where applicable.

The policy configuration also enables the organization to define protective actions, such as blocking sharing, restricting access, showing users policy tips, and sending alerts or incident reports to administrators. Microsoft renamed and consolidated the former Microsoft 365 compliance experiences under Microsoft Purview; therefore, the current portal name is Microsoft Purview portal. For detailed guidance on creating a policy, see Learn about creating and deploying DLP policies. For an overview of DLP capabilities and supported locations, see Learn about data loss prevention.

QUESTION NO: 2

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: A C

Explanation:

Microsoft Purview data loss prevention policies are designed to detect, monitor, and protect sensitive information as users work with it across Microsoft 365 locations, including Exchange Online, SharePoint Online, and OneDrive for Business. **Display policy tips to users who are about to violate your organization's policies.** is supported because DLP rules can show Policy Tips in supported Office apps and services when content contains sensitive information and a user is attempting an action covered by the policy. These tips provide real-time guidance and can warn the user, allow a business justification, or block the action according to the configured rule.

Protect documents in Microsoft OneDrive that contain sensitive information. is also supported because a DLP policy can evaluate files stored in OneDrive for Business for sensitive information types, sensitivity labels, or trainable classifiers. Based on the rule configuration, the policy can restrict access to the file, prevent sharing, notify users or administrators, and generate audit or alert events. This enables organizations to reduce unintended exposure of regulated or confidential data while retaining centralized policy management. See Learn about Microsoft Purview Data Loss Prevention and Create and deploy data loss prevention policies.

QUESTION NO: 3

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: A D

Explanation:

Azure Firewall is a fully stateful, managed network-security service designed to protect resources deployed in Azure virtual networks. It is placed in a dedicated subnet within a virtual network and applies centrally managed network and application rules to traffic moving between protected workloads, the internet, and on-premises networks. This makes Azure virtual networks a protected scope for traffic control: administrators can route traffic through the firewall and enforce rules governing allowed or denied connections.

Azure virtual machines are also protected when their inbound and outbound traffic is routed through Azure Firewall. For example, firewall network rules can restrict which source and destination addresses, ports, and protocols a virtual machine can use, while application rules can control outbound web access. Azure Firewall also provides threat-intelligence-based filtering and supports logging, which helps organizations monitor and protect virtual-machine workloads consistently without deploying a separate firewall appliance on every machine.

Microsoft describes Azure Firewall as a cloud-native service that protects Azure Virtual Network resources and provides centralized traffic filtering. See Azure Firewall overview and Deploy and configure Azure Firewall.

QUESTION NO: 4

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:

A service principal is created in the Microsoft Entra ID tenant when an application is registered. The application registration creates an application object, which defines the application's global identity and configuration, such as its redirect URIs, credentials, and requested permissions. A service principal is the tenant-local representation of that application and is the identity used when the application authenticates, receives permissions, and accesses protected resources in that tenant. This distinction matters because an application object can have service principals in multiple tenants, while each service principal is specific to one tenant. For example, when an organization consents to a multitenant application, a service principal is created in that organization's tenant to represent the application and hold its assigned permissions. Microsoft describes service principals as the security identities used by applications, services, and automation tools to access Azure and Microsoft Entra protected resources without using an interactive user identity. Learn more in Application and service principal objects in Microsoft Entra ID and Managed identities for Azure resources.

QUESTION NO: 5

Which two capabilities are provided by Microsoft Defender for Cloud? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. cloud security posture management

B. cloud workload protection

C. email mailbox retention

D. identity synchronization to on-premises Active Directory

E. Microsoft 365 license assignment

ANSWER: A B

Explanation:

Microsoft Defender for Cloud provides cloud security posture management (CSPM) capabilities and cloud workload protection (CWP) capabilities. Its CSPM capabilities continuously assess Azure, hybrid, and multicloud resources against security recommendations. These recommendations help organizations identify configuration weaknesses and improve their security posture.

Defender for Cloud also provides workload protection plans for supported workloads, such as servers, storage, databases, containers, and APIs. These plans help detect threats affecting protected resources and generate security alerts that can be investigated and remediated. See What is Microsoft Defender for Cloud?.

QUESTION NO: 6

Which two actions can you perform by using Azure Key Vault? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Store Azure Resource Manager (ARM) templates.

B. Implement Azure DDoS Protection.

C. Implement network security groups (NSGs).

D. Store keys.

E. Store secrets.

ANSWER: D E

Explanation:

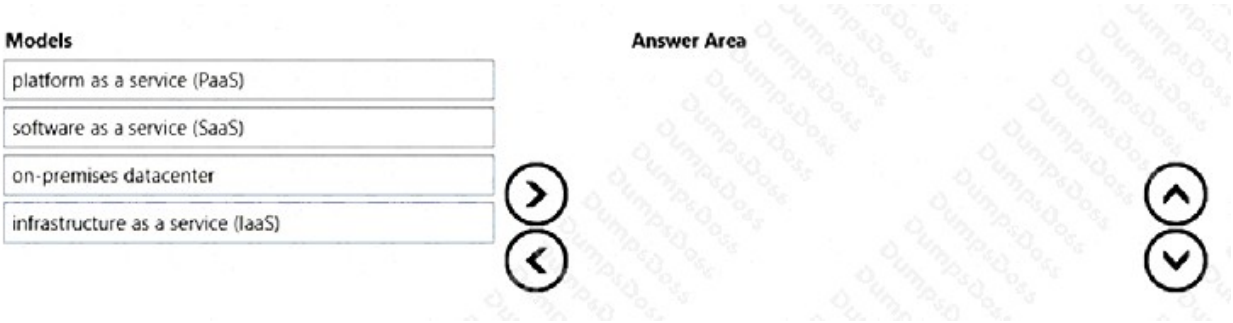
Azure Key Vault is an Azure service designed to securely store and control access to sensitive application and service materials. **Store keys.** is correct because a Key Vault can hold cryptographic keys, including keys that are generated within the vault or imported into it. Key Vault supports key lifecycle and cryptographic operations such as encryption, decryption, signing, verification, wrapping, and unwrapping, subject to the key type and permissions assigned.

Store secrets. is also correct because Key Vault stores secrets such as passwords, connection strings, API keys, tokens, and other sensitive values. Applications can retrieve these values at runtime through authenticated access rather than embedding them in source code or configuration files. Access to keys and secrets is controlled through Azure role-based access control or Key Vault access policies, helping organizations apply least-privilege access and centralize secret management. Key Vault also supports monitoring and lifecycle management features, which help protect sensitive materials used by cloud workloads. Microsoft describes Key Vault as a cloud service for securely storing and accessing secrets, keys, and certificates. For more information, see Azure Key Vault overview and About Azure Key Vault keys.

QUESTION NO: 7 - (DRAG DROP)

You need to identify which cloud service models place the most responsibility on the customer in a shared responsibility model.

in which order should you list the service models from the most customer responsibility (on the top) to the least customer responsibility (on the bottom)? To answer, move all models from the list of models to the answer area and arrange them in the correct order.



ANSWER:

Explanation:

The correct top-to-bottom order is on-premises datacenter, infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). This reflects the progressive transfer of responsibility from the customer to the cloud provider. In an on-premises datacenter, the customer owns and manages the full environment. That includes the physical facilities and hardware, networking, storage, servers, virtualization, operating systems, middleware, runtime, applications, identities, and data. Because the customer is responsible for the complete stack, this model places the greatest responsibility on the customer.

With infrastructure as a service (IaaS), the provider takes responsibility for the physical datacenter, physical network, physical servers, storage, and virtualization layer. The customer continues to configure and operate the guest operating system, network controls, applications, identities, and data. This reduces the customer's responsibilities compared with an on-premises datacenter, while still allowing substantial control over the environment.

With platform as a service (PaaS), the provider additionally manages the platform components required to run applications, such as the operating system, middleware, and runtime. The customer primarily concentrates on deploying and maintaining its applications, protecting data, and managing access. This means the customer has less responsibility than with infrastructure as a service.

With software as a service (SaaS), the provider manages the application and the underlying platform and infrastructure. The customer's main responsibilities are its data, identities, access configuration, and appropriate use of the service. Microsoft describes these boundaries in its shared responsibility in the cloud guidance and its shared responsibility model overview. Consequently, the displayed sequence correctly moves from the most customer responsibility to the least.

QUESTION NO: 8

What Microsoft Purview feature can use machine learning algorithms to detect and automatically protect sensitive items?

A. eDiscovery

B. Data loss prevention

C. Information risks

D. Communication compliance

ANSWER: B

Explanation:

Data loss prevention is correct because Microsoft Purview DLP is designed to identify sensitive information in organizational content and enforce protections when that information is used, shared, or moved in ways that violate policy. DLP policies can inspect data in Microsoft 365 services, on devices, and in supported cloud applications. They use sensitive information types and can use trainable classifiers, which are machine-learning-based models that recognize categories of content from examples rather than relying solely on fixed patterns. This enables organizations to identify sensitive content with greater context and apply automated policy actions.

After a policy detects a matching sensitive item, Purview DLP can automatically protect it by blocking or restricting sharing, preventing copying to removable media or printing on endpoints, displaying policy tips to users, requiring a business justification, and generating alerts or audit events. Administrators define the conditions and enforcement actions centrally, allowing data protection to occur consistently without requiring users to manually classify or secure every item. Microsoft documents DLP capabilities and policy actions in Learn about Microsoft Purview Data Loss Prevention, and describes machine-learning trainable classifiers in Learn about trainable classifiers.

QUESTION NO: 9

To which three locations can a data loss prevention (DLP) policy be applied? Each correct answer presents a complete solution.

NOTE: Each correct answer is worth one point.

A. Microsoft Exchange Online email

B. Microsoft OneDrive accounts

C. Microsoft Exchange Online public folders

D. Microsoft Teams chat and channel messages

E. Microsoft Viva Engage

ANSWER: A B D

Explanation:

Microsoft Purview Data Loss Prevention policies can protect sensitive information in key Microsoft 365 workloads, including Microsoft Exchange Online email, Microsoft OneDrive accounts, and Microsoft Teams chat and channel messages. In Exchange Online, DLP evaluates email messages and their attachments to identify sensitive information and can apply policy actions such as blocking external delivery, showing policy tips, or generating alerts. In OneDrive, DLP scans files stored in users' accounts and can restrict sharing or access when sensitive content is detected. For Teams, DLP evaluates chat and channel messages, helping prevent sensitive information from being shared in conversations and allowing policy actions appropriate to the detected content. These locations enable an organization to apply consistent sensitive-information protections across email, personal cloud storage, and collaboration messaging. Microsoft documents Exchange Online, OneDrive for Business, and Teams as supported Microsoft 365 locations for DLP policy enforcement. See Learn about Microsoft Purview Data Loss Prevention and Create and deploy data loss prevention policies.

QUESTION NO: 10

Which two capabilities are available in Microsoft Sentinel? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. threat hunting

B. security incident management

C. Microsoft 365 document retention

D. password hash synchronization

E. Azure virtual machine disk encryption

ANSWER: A B

Explanation:

Microsoft Sentinel provides threat hunting and security incident management capabilities. Threat hunting enables security analysts to proactively search collected data for suspicious activity by using queries, rather than waiting for an alert to be generated.

Microsoft Sentinel also groups related alerts into incidents to help analysts investigate an attack in context. Incidents provide information about affected entities, alerts, investigation details, and response activities. These capabilities are supported by data ingested through configured data connectors. See What is Microsoft Sentinel?.

QUESTION NO: 11

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: A E

Explanation:

In the Cloud Adoption Framework for Azure, the methodology begins by establishing a strategy and then creating a plan before an organization enters the Ready phase. “Define Strategy” represents the initial strategic work: documenting business motivations, desired outcomes, and the cloud transformation approach. This gives the organization a clear basis for determining what it intends to achieve with cloud adoption.

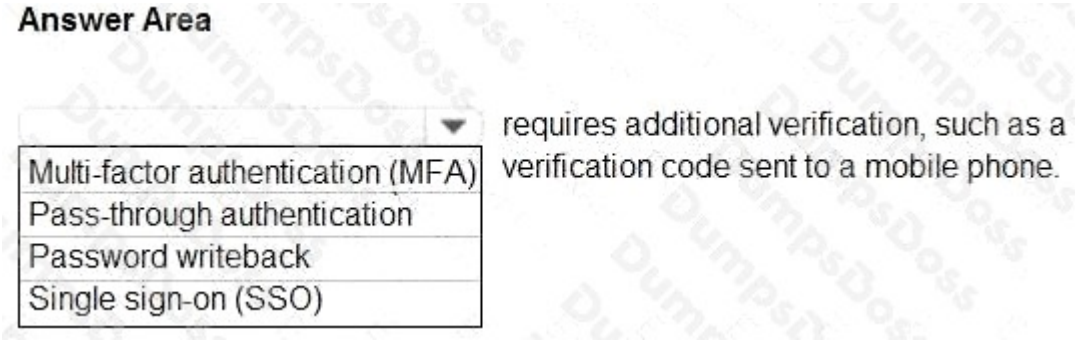
“Plan” follows that strategic work. During planning, teams assess and prioritize the digital estate, identify workloads for migration or innovation, and build an actionable cloud adoption plan. The resulting plan helps determine the resources, sequencing, skills, and organizational preparation required for adoption.

After these activities, the Ready methodology prepares the Azure environment by establishing an Azure landing zone that can support the planned workloads. Microsoft describes the Cloud Adoption Framework methodologies and their sequence in the Cloud Adoption Framework overview. More detail about defining motivations and business outcomes is available in Microsoft’s Strategy methodology guidance.

QUESTION NO: 12 - (SIMULATION)

Select the answer that correctly completes the sentence.

Answer Area



ANSWER: See the explanation for the answer

Explanation:

Answer: Multi-factor authentication (MFA)

Multi-factor authentication requires additional verification during sign-in, such as entering a verification code sent to a mobile phone (or using an authenticator app, fingerprint, or other second factor).

QUESTION NO: 13

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's system can be breached.

E. Use the network as the primary security boundary.

ANSWER: B C D

Explanation:

Zero Trust is founded on the principles of verifying explicitly, using least-privilege access, and assuming breach. **Always verify the permissions of a user explicitly** aligns with verify explicitly: every access request should be evaluated using all relevant available signals, including identity, authentication strength, device state, location, workload, data classification, and risk. Verification is continuous and context-aware rather than being based solely on an initial sign-in.

Always assume that the user's system can be breached reflects the assume-breach principle. This mindset requires organizations to limit blast radius through measures such as segmentation, use telemetry to detect threats, and prepare to respond rapidly to suspicious activity. It treats potential compromise as a condition that security architecture must contain and manage.

Use identity as the primary security boundary is also consistent with Zero Trust because identity is a central control plane for evaluating and enforcing access decisions in modern cloud and hybrid environments. Strong identity controls, including authentication, authorization, and risk-based policy enforcement, help ensure that access is granted only to the appropriate resource, for the appropriate purpose, and under the appropriate conditions. See Microsoft Zero Trust overview and Microsoft guidance for Zero Trust pillars.

QUESTION NO: 14

What are three uses of Microsoft Cloud App Security? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. to discover and control the use of shadow IT

B. to provide secure connections to Azure virtual machines

C. to protect sensitive information hosted anywhere in the cloud

D. to provide pass-through authentication to on-premises applications

E. to prevent data leaks to noncompliant apps and limit access to regulated data

ANSWER: A C E

Explanation:

Microsoft Cloud App Security, now named Microsoft Defender for Cloud Apps, is a cloud access security broker (CASB) that provides visibility, control, and protection for cloud app use. Its Cloud Discovery capability analyzes traffic information to discover and control the use of shadow IT, helping organizations identify unsanctioned cloud services, assess their risk, and apply governance actions. Defender for Cloud Apps also helps to protect sensitive information hosted anywhere in the cloud through app-connected visibility and controls, including detection of sensitive data and application of policies across supported SaaS services. In addition, it can prevent data leaks to noncompliant apps and limit access to regulated data by using app governance and session controls. For example, organizations can monitor or block activities such as downloading sensitive files, applying labels, or transferring content to unmanaged apps or devices, based on the configured policy and user context. These capabilities support discovery, data protection, and real-time control of cloud applications and their data. Microsoft documents these core CASB capabilities, including Cloud Discovery, information protection, and threat protection, in its Defender for Cloud Apps overview. See also the Cloud Discovery risk assessment documentation for how discovered cloud apps are evaluated and governed.

QUESTION NO: 15

What is an example of encryption at rest?

A. encrypting communications by using a site-to-site VPN

B. encrypting a virtual machine disk

C. accessing a website by using an encrypted HTTPS connection

D. sending an encrypted email

ANSWER: B

Explanation:

Encrypting a virtual machine disk is an example of encryption at rest because the data is protected while it is stored on persistent media rather than while it is moving across a network. A virtual machine's managed disks contain operating-system files, application files, and potentially sensitive business data. Applying disk encryption protects that stored content from unauthorized access if the underlying storage media is accessed outside the expected authorization path. In Azure, Azure Disk Encryption can encrypt supported virtual machine OS and data disks, using BitLocker for Windows and DM-Crypt for Linux. Azure also provides server-side encryption for managed disks, which encrypts data at rest and is enabled by default for managed disks. Encryption at rest is a foundational data-protection control: it helps ensure stored data remains unreadable without the appropriate cryptographic keys, while normal authorized workloads can continue to use the data. For more information, see Azure Disk Encryption overview and Azure data encryption at rest.

QUESTION NO: 16

Which two actions can Microsoft Purview communication compliance help an organization perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Detect potentially inappropriate workplace communications.

B. Enable reviewers to investigate policy matches.

C. Encrypt Azure virtual machine disks.

D. Assign Azure resource roles to administrators.

E. Deploy operating system updates to devices.

ANSWER: A B

Explanation:

Microsoft Purview communication compliance helps organizations detect potentially inappropriate or risky communications in supported communication channels. Policies can identify messages that may contain harassment, threats, adult content, or information that could indicate regulatory compliance concerns.

Communication compliance also provides a review workflow. Authorized reviewers can investigate policy matches, review the relevant communication, and take actions such as resolving the item, escalating it, or notifying the sender. This supports investigations while limiting access to communications to users assigned appropriate review permissions. See Learn about communication compliance.

QUESTION NO: 17

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: D

Explanation:

180 days is correct. Microsoft 365 E3 includes Microsoft Purview Audit (Standard), also commonly called Basic Audit. Audit (Standard) provides access to the unified audit log so organizations can investigate user and administrator activity across Microsoft 365 services, including Microsoft Entra ID, Exchange Online, SharePoint Online, OneDrive, Microsoft Teams, and Microsoft Purview. Under the current Microsoft licensing and retention model, Audit (Standard) retains audit records for 180 days by default. Therefore, activity captured in the unified audit log under the Microsoft 365 E3 subscription is available for searches and investigations during that 180-day retention period. Organizations that require longer retention, advanced auditing events, or other enhanced audit capabilities can evaluate Microsoft Purview Audit (Premium), but the described Basic Audit scenario uses the standard 180-day retention period. Microsoft documents the Audit (Standard) retention policy and licensing capabilities in its Microsoft Purview Audit solutions overview. For the current retention periods and audit log management details, see Manage audit log retention policies.

QUESTION NO: 18

What should you use in the Microsoft 365 security center to view security trends and track the protection status of identities?

A. Attack simulator

B. Reports

C. Hunting

D. Incidents

ANSWER: B

Explanation:

Reports is the correct choice because the reporting experience in the Microsoft 365 security center, now incorporated into the Microsoft Defender portal, provides summarized security data that helps organizations understand their security posture over time. Its purpose is to present dashboards and visualizations for trends, status, and outcomes across protected workloads rather than merely displaying individual events. For identity protection, these views can help security teams monitor relevant identity-related security signals and assess whether protections are being applied effectively across the organization. This trend-focused, organization-level perspective supports operational security decisions: teams can review changes over time, identify areas that need attention, and communicate protection status to stakeholders. Microsoft documents the Reports area as the location for viewing security reports in the Defender portal and describes its role in providing visibility into security information across Microsoft security workloads. The naming of the portal has evolved, but the reporting capability remains the appropriate feature for this requirement. See Reports in the Microsoft Defender portal and Microsoft Defender portal overview.

QUESTION NO: 19

Which Microsoft Defender for Office 365 feature can help protect users from malicious URLs in email messages and Microsoft Teams messages?

A. Safe Links

B. Safe Attachments

C. Attack surface reduction rules

D. Microsoft Defender for Identity

ANSWER: A

Explanation:

Safe Links is correct because it helps protect users from malicious web links in supported email and collaboration workloads. Safe Links scans URLs and can rewrite them so that Microsoft Defender for Office 365 can evaluate the destination when the user selects the link.

If the destination is determined to be malicious, Safe Links can block the user from accessing it. This time-of-click protection is important because a website that appears safe when a message is delivered can later be changed to host malicious content. See Safe Links in Microsoft Defender for Office 365.

QUESTION NO: 20

Which two signals can Microsoft Entra Conditional Access evaluate when making an access decision? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. device state

B. location

C. virtual machine size

D. Azure subscription type

E. resource group name

ANSWER: A B

Explanation:

Conditional Access evaluates signals associated with a sign-in and then applies configured access controls. **Device state** is a supported signal. For example, a policy can require that a device be marked compliant by Microsoft Intune before a user can access a cloud application.

Location is also a supported signal. Administrators can define named locations, such as trusted corporate network ranges or countries and regions, and use those locations as conditions in a policy. Conditional Access can then require multifactor authentication, block access, or apply another control when users sign in from an in-scope location. See What is Conditional Access?.

QUESTION NO: 21

Which Microsoft Purview data classification type supports the use of regular expressions?

A. exact data match (EDM)

B. fingerprint classifier

C. sensitive information types (SITs)

D. trainable classifier

ANSWER: C

Explanation:

sensitive information types (SITs) is correct because Microsoft Purview uses sensitive information types to identify and classify sensitive data in content such as documents, email, and Teams messages. A sensitive information type can be built from one or more patterns, and those patterns can include regular expressions (regex) to detect data with a defined textual structure. For example, a regex can recognize strings that follow the expected format of an identification number, account number, or other organization-specific value. Purview evaluates the configured pattern alongside supporting evidence, such as keywords, checksums, or confidence levels, when applicable, to improve detection quality.

Microsoft provides many built-in sensitive information types and also allows organizations to create custom sensitive information types. When creating a custom type, regex is a key mechanism for defining a pattern that identifies data matching the organization's required format. These classifications can then be used by Microsoft Purview capabilities, including data loss prevention and sensitivity labeling, to help discover, protect, and govern sensitive information consistently. See Learn about sensitive information types and Create custom sensitive information types.

QUESTION NO: 22

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

Explanation:

2 is correct because multi-factor authentication requires a user to prove their identity with at least two independent authentication factors. These factors are commonly categorized as something the user knows, such as a password or PIN; something the user has, such as a phone, hardware token, or authenticator app; and something the user is, such as a biometric characteristic. In Microsoft Entra ID, formerly Azure Active Directory, MFA normally combines the user's primary sign-in credential with an additional verification method. For example, a user might enter a password and then approve a notification in Microsoft Authenticator, provide a time-based code, use a passkey, or satisfy another approved second-factor method. The security value comes from requiring this additional, distinct proof of identity, so compromise of a password alone is not sufficient to complete the sign-in. Microsoft describes MFA as requiring two or more verification methods and recommends it as a foundational protection for identities and organizational resources. See How multifactor authentication works in Microsoft Entra ID and Authentication methods in Microsoft Entra ID.

QUESTION NO: 23

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: B C

Explanation:

Security defaults provide a Microsoft-managed baseline of identity protections for an Azure AD tenant, now called Microsoft Entra ID. A core protection is that users assigned administrator roles must perform Azure Multi-Factor Authentication (MFA) whenever they sign in. This reduces the risk that a compromised administrator password can be used to take control of tenant resources, settings, identities, or data. Security defaults also require users to register for Azure MFA. Registration ensures that users have a verification method available before a sign-in event requires MFA, such as when Microsoft detects elevated sign-in risk or when accessing an application under the security-defaults policy. The registration requirement applies broadly to users, while the administrator requirement ensures particularly sensitive privileged accounts receive MFA protection on every sign-in. These controls are configured automatically when security defaults are enabled; organizations that need more granular targeting, exclusions, or authentication requirements can instead use Conditional Access policies with appropriate licensing. Microsoft documents the security-defaults protections, including mandatory MFA for administrators and MFA registration for all users, at Security defaults in Microsoft Entra ID. Additional implementation guidance is available at How Microsoft Entra multifactor authentication works.

QUESTION NO: 24 - (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
Security defaults require an Azure Active Directory (Azure AD) Premium license.	○	○
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	○	○
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	○	○

ANSWER:

Answer:

Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	○	○
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	○	○
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	○	○

Answer:

Explanation:

 Security defaults require an Azure Active Directory (Azure AD) Premium license. No Security defaults can be enabled for a single Azure Active Directory (Azure AD) user. No When Security defaults are enabled, all administrators must use multi-factor authentication (MFA). YesMicrosoft explains that Security defaults are baseline identity protections that are “available to all tenants at no additional cost” and are intended to “help protect your organization from common identity-related attacks.” They are a tenant-wide setting: Microsoft states that security defaults are “either on or off for the entire tenant” and “can’t be customized or targeted to specific users or groups.” If you require per-user or granular targeting, Microsoft directs customers to use Conditional Access policies instead.A core behavior of security defaults is enforcing MFA: “All users are required to register for Azure AD Multi-Factor Authentication,” and “administrators are required to perform MFA.” In addition, security defaults “block legacy authentication” and apply other baseline requirements, but they do not enable premium features such as Azure AD Identity Protection or PIM. Summarizing the implications for the statements: no premium license is required; you cannot enable security defaults for just one user because the control is global; and when enabled, administrators must use MFA, with Microsoft recommending exclusion only for a break-glass account if necessary.

Explanation:

Security defaults provide Microsoft’s baseline identity protections for a Microsoft Entra tenant. They are intended to help organizations protect accounts from common identity attacks, especially password spray, credential theft, and use of legacy authentication methods. Security defaults do not require a Microsoft Entra ID Premium license. Microsoft makes this baseline capability available to tenants at no additional cost, so an organization can enable these protections even when it does not have Premium licensing.

Security defaults are configured for the whole tenant. The setting is either enabled or disabled at the tenant level and is not designed for assignment to a particular user, group, or application. This makes it a simple baseline control for organizations that do not need custom access-policy logic. Organizations that need to scope requirements to selected users, groups, applications, locations, devices, or risk conditions would use Conditional Access instead, subject to the applicable licensing requirements.

A key protection included with security defaults is multifactor authentication for administrator accounts. Administrative roles have elevated permissions and are especially valuable targets for attackers, so security defaults require administrators to use MFA. Users are also prompted to register for MFA as needed, helping establish stronger sign-in verification across the tenant. Security defaults additionally block legacy authentication protocols, which helps reduce the chance that older sign-in methods can bypass modern authentication protections. Microsoft documents these behaviors in its security defaults overview and its guidance on how multifactor authentication works.

QUESTION NO: 25

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.

F. Use least-privilege access.

ANSWER: C D F

Explanation:

The Zero Trust model is founded on three principles: verify explicitly, use least-privilege access, and assume breach. “Always verify the permissions of a user explicitly” represents the verify-explicitly principle: access decisions should be based on all relevant available signals, including identity, authentication strength, device state, location, workload, data classification, and detected risk. Verification is continuous rather than a one-time event at a network boundary.

“Always assume that the user system can be breached” reflects the assume-breach principle. Zero Trust designs controls with the expectation that an attacker may already have obtained access to an account, device, application, or network segment. This drives segmentation, monitoring, encryption, and limiting the potential blast radius of a compromise.

“Use least-privilege access” completes the model. Users, devices, and applications receive only the access needed to perform their current task, ideally through just-in-time and just-enough access mechanisms. Permissions should be constrained by policy and risk signals, reducing exposure to sensitive resources. Microsoft describes these three principles in its Zero Trust overview and explains their application in the Zero Trust architecture.

QUESTION NO: 26

Which two Azure resources can a network security group (NSG) be associated with? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. a network interface

B. an Azure App Service web app

C. a virtual network

D. a virtual network subnet

E. a resource group

ANSWER: A D

Explanation:

An NSG can be associated directly with **a network interface** and **a virtual network subnet**. Associating an NSG to a network interface applies its inbound and outbound security rules to traffic for that specific network interface. This enables granular protection for an individual virtual machine or other resource that has a network interface in an Azure virtual network.

Associating an NSG with a subnet applies the NSG’s rules to traffic entering or leaving network interfaces in that subnet. This supports consistent traffic filtering for a group of resources deployed into the same subnet. Azure evaluates applicable NSG rules for both the subnet and the network interface when both have NSGs assigned, allowing administrators to apply broad subnet-level controls alongside more specific interface-level controls. NSGs use allow and deny rules based on properties such as direction, protocol, source and destination addresses, ports, and priority. For additional details, see Network security groups and How network security groups work.

QUESTION NO: 27

Which Microsoft Purview feature allows users to identify content that should be protected?

A. Sensitivity Labels

B. Insider Risks

C. Data Loss prevention

D. eDiscovery

ANSWER: A

Explanation:

Sensitivity Labels is correct because Microsoft Purview Information Protection uses sensitivity labels to classify and identify organizational content according to its sensitivity, such as Public, General, Confidential, or Highly Confidential. Users can select and apply an appropriate label to documents, emails, meetings, and other supported content, thereby making its protection requirements clear. Labels can also be configured to apply protection actions automatically, including encryption, content markings such as headers or watermarks, and access restrictions. Organizations can publish labels to users, recommend labels based on detected sensitive information, or automatically apply labels when policy conditions are met. This enables people and organizations to identify content requiring protection at the point where it is created, edited, or shared, while applying consistent information-protection policies across Microsoft 365 services and supported apps. Microsoft describes sensitivity labels as a foundational capability for classifying and protecting data throughout its lifecycle. For configuration and use details, see Microsoft Purview sensitivity labels and Learn about sensitivity labels.

QUESTION NO: 28

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. text message (SMS)

B. Microsoft Authenticator app

C. email verification

D. phone call

E. security question

ANSWER: A B D

Explanation:

Azure Multi-Factor Authentication supports verification through text message (SMS), the Microsoft Authenticator app, and phone call. With text message (SMS), Microsoft Entra ID sends a one-time passcode to the user's registered mobile number, which the user enters to complete sign-in. The Microsoft Authenticator app can provide an approval notification or generate a time-based one-time passcode; number matching can add an important verification step to push notifications. A phone call can also be placed to a registered telephone number, allowing the user to complete the voice-call verification process. These methods are configured as authentication methods in Microsoft Entra ID and can be used to satisfy an MFA requirement, subject to the organization's enabled authentication-method policies and user registration. Microsoft documents the available methods and their use in the authentication methods overview. For implementation details and method-specific MFA behavior, see How Microsoft Entra MFA works.

QUESTION NO: 29 - (SIMULATION)

Select the answer that correctly completes the sentence.

Answer Area

Federation is used to establish [multi-factor authentication (MFA) / a trust relationship / user account synchronization / a VPN connection] between organizations.

ANSWER: See the explanation for the answer

Explanation:

Select: `a trust relationship`

The completed sentence is: **"Federation is used to establish a trust relationship between organizations."**

Federation allows one organization to trust authentication performed by another organization, enabling users to access resources using their existing identities. It is not MFA, account synchronization, or a VPN connection.

QUESTION NO: 30

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:

Microsoft 365 sensitivity labels classify and help protect organizational content according to its sensitivity, such as Public, General, Confidential, or Highly Confidential. A label can be configured to apply content markings to documents and emails, including a watermark. Administrators can define the watermark text, font size, font color, and layout, and the marking is then applied to supported files when users apply the label. This provides a visible indication of the content's sensitivity, helping users handle the file appropriately even when it is printed or shared. Sensitivity labels can also apply encryption and access restrictions, headers and footers, and—in supported scenarios—container settings for Teams, Microsoft 365 Groups, and SharePoint sites. Watermarks are therefore a directly configurable protection setting within a sensitivity label. Microsoft documents the available label settings, including content marking configuration, in its sensitivity-label documentation. See Microsoft Purview sensitivity labels and Use sensitivity labels with Microsoft 365 apps.

QUESTION NO: 31

In a Core eDiscovery workflow, what should you do before you can search for content?

A. Create an eDiscovery hold.

B. Run Express Analysis.

C. Configure attorney-client privilege detection.

D. Export and download results.

ANSWER: A

Explanation:

Create an eDiscovery hold. In the Core eDiscovery workflow, a hold is applied early in an investigation to preserve potentially relevant electronic content in the locations associated with custodians or other data sources. A hold helps ensure that content matching the investigation's scope is retained, even if a user later edits or deletes it or if a retention policy would otherwise remove it. This preservation step is important because search results are most useful when the underlying evidence remains available and unchanged while the organization assesses the matter.

After the case is set up and the appropriate users have access, the organization identifies relevant people and locations and creates the hold. It can then create and run content searches against the preserved data, review the results, and export content when needed. Microsoft documents eDiscovery (Standard), formerly called Core eDiscovery, as a workflow that includes creating a case, placing custodians and content locations on hold, then creating searches to locate responsive content. For details, see Microsoft's eDiscovery (Standard) workflow documentation and Microsoft's guidance for creating holds in eDiscovery.

QUESTION NO: 32

What should you create to search and export content preserved in an eDiscovery hold?

A. a Microsoft SharePoint Online site

B. a case

C. a Microsoft Exchange Online public folder

D. Azure Files

ANSWER: B

Explanation:

You should create **a case** in Microsoft Purview eDiscovery. A case is the central workspace used to manage an investigation, litigation matter, or other legal/compliance request. It organizes the people who need access to the matter and provides the place to manage eDiscovery activities, including holds, searches, review-related workflows, and exports. After content locations or custodians are placed on hold, the case lets authorized eDiscovery users create and run searches against the preserved data. Search results can then be exported for downstream legal review or production, subject to the organization's permissions and eDiscovery configuration. Using a case also keeps the matter's data and actions logically separated from other investigations, which supports organized handling of sensitive information. Microsoft describes eDiscovery cases as containers for managing legal matters and the associated holds, searches, and exports. For more information, see Microsoft Purview eDiscovery (Standard) and Learn about eDiscovery cases.

QUESTION NO: 33

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 virtual machines is correct because Azure Bastion is a managed service designed to provide secure Remote Desktop Protocol (RDP) and Secure Shell (SSH) connectivity to virtual machines. A user connects through the Azure portal, or supported native-client connections, to a Bastion host deployed in the virtual network. The Bastion host then connects privately to the target virtual machine, so the VM does not need a public IP address and its RDP or SSH ports do not need to be exposed directly to the internet. This architecture reduces the attack surface associated with direct remote-administration access while allowing authorized administrators to manage Windows and Linux virtual machines. Azure Bastion supports connections to Azure VMs in the virtual network where Bastion is deployed and, depending on the configured SKU and network topology, can also support connectivity across peered virtual networks. The key resource type it provides interactive RDP/SSH access to is therefore an Azure virtual machine. Microsoft describes Bastion as a fully managed platform-as-a-service offering that provides secure, seamless RDP and SSH access to VMs without exposing them through public IP addresses. See Azure Bastion overview and Connect to a Windows VM using Azure Bastion.

QUESTION NO: 34

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

NOTE: Each correct selection is worth one point.

A. automated investigation and remediation

B. transport encryption

C. shadow IT detection

D. attack surface reduction

ANSWER: A D

Explanation:

Microsoft Defender for Endpoint includes automated investigation and remediation and attack surface reduction as core endpoint-security capabilities. Automated investigation and remediation uses security alerts and telemetry to investigate potential threats, determine their scope, and take remediation actions automatically or with analyst approval, depending on the organization's automation settings. This helps security operations teams prioritize incidents and reduce the time needed to contain and remediate threats. Attack surface reduction is a set of preventive controls that reduces opportunities for malware and adversaries to compromise devices. Through attack surface reduction rules and related protections, organizations can block risky behaviors and techniques commonly used in attacks, such as suspicious script activity, credential theft behaviors, and malicious content launched from productivity applications. These capabilities work together across the endpoint lifecycle: attack surface reduction helps prevent compromises, while automated investigation and remediation helps detect, investigate, and respond when suspicious activity occurs. Microsoft documents both capabilities as part of Defender for Endpoint's prevention, detection, investigation, and response functionality. For details, see Microsoft Defender for Endpoint overview and Automated investigation and remediation.

QUESTION NO: 35

Which security feature is available in the free mode of Microsoft Defender for Cloud?

A. vulnerability scanning of virtual machines

B. secure score

C. just-in-time (JIT) VM access to Azure virtual machines

D. threat protection alerts

ANSWER: B

Explanation:

secure score is available through Microsoft Defender for Cloud's foundational cloud security posture management capabilities, which are provided at no cost. Secure score gives an at-a-glance, measurable view of an organization's security posture by evaluating Azure resources against security recommendations. It assigns points for healthy resources and improvement actions, then presents an overall score and actionable recommendations that help teams prioritize the changes most likely to reduce risk. This makes it useful even before an organization enables paid Defender for Cloud protection plans: security administrators can identify configuration gaps, track posture improvements over time, and focus remediation work according to the potential security impact. Microsoft describes secure score as a central posture-management capability that reflects the health of an environment and supports prioritization of security recommendations. The free foundational CSPM offering includes this visibility for Azure resources, while organizations can separately enable paid plans when they need advanced workload-protection capabilities. See Microsoft's cloud security posture management overview and secure score documentation for details.

QUESTION NO: 36

Which compliance feature should you use to identify documents that are employee resumes?

A. pre-trained classifiers

B. Content explorer

C. Activity explorer

D. eDiscovery

ANSWER: A

Explanation:

Pre-trained classifiers is the correct feature because Microsoft Purview includes ready-made trainable classifiers designed to recognize common categories of business content, including resumes. These classifiers use machine learning to evaluate a document's content and characteristics, rather than requiring an organization to build keyword queries or manually review every file. The Resume classifier can identify documents that resemble employment resumes based on the learned structure and language typically found in that document type.

After publishing a pre-trained classifier, an organization can use it as a condition in Microsoft Purview solutions such as retention labels, sensitivity labels, data loss prevention policies, and communication compliance policies. This allows resume-related content to be located and governed consistently across supported Microsoft 365 locations. Microsoft documents that built-in trainable classifiers are available out of the box and lists Resume among the pre-trained classifier types. For implementation details and the available classifiers, see Learn about trainable classifiers and Get started with trainable classifiers.

QUESTION NO: 37

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:

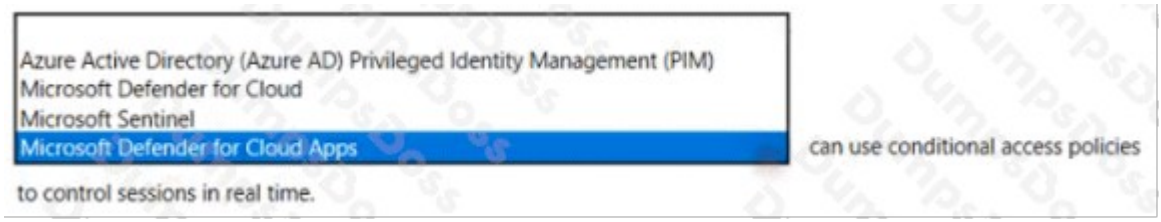
Microsoft Service Trust Portal is correct because it is Microsoft's central resource for transparency information about the security, privacy, compliance, and reliability practices used for Microsoft cloud services. Organizations can use the portal to

review how services such as Microsoft 365, Azure, and Dynamics 365 align with regulatory standards and frameworks, including International Organization for Standardization standards. The portal provides access to compliance documentation such as audit reports, certifications, attestations, and other materials that help customers evaluate Microsoft's control environment and support their own compliance assessments.

Many of these documents are available through the Service Trust Portal's compliance offerings and may require authentication and acceptance of a nondisclosure agreement, depending on the document. This makes the portal particularly useful for compliance officers, risk teams, auditors, and procurement stakeholders who need authoritative evidence of Microsoft's cloud compliance commitments. Microsoft describes the Service Trust Portal as a place to access compliance-related information and documents for its cloud services. For details, see Microsoft Service Trust Portal documentation and Microsoft Service Trust Portal.

QUESTION NO: 38 - (HOTSPOT)

Select the answer that correctly completes the sentence.



ANSWER:



Explanation:

Microsoft Defender for Cloud Apps is the correct completion because it works with Microsoft Entra Conditional Access through Conditional Access App Control to provide real-time session controls. This capability lets an organization apply controls after a user has signed in to a supported cloud application, rather than relying only on a decision made before access is granted. For example, a policy can monitor a session, block downloads, prevent copying sensitive data, require a watermark, or restrict uploads when a session has conditions that require additional protection.

These controls are especially useful for protecting data in browser-based sessions, including scenarios involving unmanaged devices or users who need limited access to corporate information. Conditional Access provides the policy signal and access context, while Microsoft Defender for Cloud Apps enforces the relevant in-session controls through its reverse-proxy-based Conditional Access App Control integration. This is why the product fits the statement that conditional access policies can be used to control sessions in real time. Microsoft's documentation describes how Conditional Access App Control integrates with Conditional Access and how organizations can configure session policies in Defender for Cloud Apps to monitor and control user activity during a session.

QUESTION NO: 39

You plan to move resources to the cloud.

You are evaluating the use of Infrastructure as a service (IaaS),

Platform as a service (PaaS), and Software as a service (SaaS) cloud models.

You plan to manage only the data, user accounts, and user devices for a cloud-based app.

Which cloud model will you use?

A. IaaS

B. SaaS

C. PaaS

ANSWER: B

Explanation:

SaaS is the appropriate cloud service model when the organization intends to manage only its data, user accounts, and user devices. In a Software as a Service offering, the cloud provider operates and maintains the application itself as well as the supporting platform, operating system, servers, storage, networking, and physical datacenter infrastructure. The customer consumes a complete, ready-to-use application over the internet, typically through a web browser or client app.

The customer still has important responsibilities in this model. These include deciding what organizational data is stored in the service, managing identities and access permissions for users, configuring tenant-level settings, and securing the devices used to access the application. This responsibility split directly matches the stated requirement. Common SaaS examples include Microsoft 365 services, where Microsoft manages the underlying service infrastructure and customers manage their users, information, and endpoint access.

Microsoft describes SaaS as a model that provides complete applications managed by the service provider, while customers are responsible for their data, identities, and devices. See Microsoft's shared responsibility guidance and Azure shared responsibility in the cloud.

QUESTION NO: 40

Which two capabilities are provided by Microsoft Defender for Office 365? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Safe Links

B. anti-phishing protection

C. Azure virtual network segmentation

D. Azure SQL vulnerability assessment

E. privileged role activation

ANSWER: A B

Explanation:

Safe Links helps protect users from malicious URLs in email messages and supported Office applications. It checks URLs at the time a user selects them and can block access when the destination is determined to be malicious.

Anti-phishing protection helps identify phishing attempts, including messages that impersonate users, domains, or trusted organizations. Policies can be configured to take actions such as quarantining detected messages and notifying users or administrators. These capabilities help protect email and collaboration workloads from phishing-based threats. See Safe Links in Microsoft Defender for Office 365 and Anti-phishing protection in Microsoft Defender for Office 365.