SC-900: Microsoft Security, Compliance, and Identity Fundamentals Sample Questions

Last updated: 1/19/2022

PLEASE COMPLETE THIS SURVEY (https://aka.ms/samplequestions)

Microsoft is exploring the possibility of providing sample questions as an exam preparation resource, and we would like your feedback. While we prefer that you complete the survey after taking the exam, you may complete it at any time. Thank You!

User Guide

These sample questions are intended to provide an overview of the style, wording, and difficulty of the questions that you are likely to experience on this exam. These questions are **not** the same as what you will see on the exam nor is this document illustrative of the length of the exam or its complexity (e.g., you may see additional question types, multiple case studies, and possibly labs). These questions are **examples** only to provide insight into what to expect on the exam and help you determine if additional preparation is required.

In the first section, you will find the questions without answers so that you can test your knowledge. In the second section, the answer, a rationale, and a URL that will link you to additional information is provided immediately below each question.

Contents

Questions

Question # 1 (Multiple Choice)

The zero-trust model operates on the principle of "trust no one, verify everything." You need to implement the zero-trust model in your organization.

Which two options are the guiding principles of a zero-trust model?

A. Verify explicitly
B. Assume breach
C. Role based access
D. Perimeter security

Question # 2 (Matching)

Match the type of attack on the left to the correct description on the right.

Type of attack

A. Brute force attacks
B. Phishing
C. Spear phishing
D. Spray Attacks

Descriptions

______ 1. an attack that tries many passwords against one or more accounts, sometimes using dictionaries of commonly used passwords

______ 2. an attack which attempts to match a username against a list of weak passwords

______ 3. an attack which is received in the form of an email that appears to come from a reputable source

______ 4. a highly targeted form of email attack which can be used to create highly credible emails

Question # 3 (Matching)

Match the Azure Active Directory (Azure AD) device identity on the left to the correct description on the right.

Azure AD device identity

A. Azure AD registered devices
B. Azure AD joined devices
C. Hybrid Azure AD joined devices

Descriptions

______ 1. These devices are owned by an organization and are signed in with an Active Directory Domain Service account belonging to that organization. They exist in the cloud and on-premises.

______ 2. These devices are typically personally owned, rather than by the organization. They are signed in with a personal Microsoft account or another local account.

______ 3. These devices exist only in the cloud and are owned by an organization. They are signed in with an organization Azure AD account.

Question # 4 (Multiple Choice)

You need to look for a hybrid identity solution between Azure Active Directory (Azure AD) and your on-premises active directory. It needs to provide a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers.

Which authentication method should you use?

A. Password Hash synchronization
B. Pass-through authentication
C. Federated authentication
D. Directory synchronization

Question # 5 (Multiple Choice)

To improve identity security within the organization, the security team wants to implement Windows Hello for Business. You need to explain the benefits of Windows Hello for Business.

Which statement is true?

A. Windows Hello is an authentication feature built into Windows Server 2012 R26.
B. Windows Hello is an alternative to multi-factor authentication.
C. Windows Hello is a secure feature that uses PINs and bio-metric data to authenticate users.
D. Windows Hello is a feature only for Azure Active Directory premium customers.

Question # 6 (Multiple Choice)

Sign-in risk is a signal used by Conditional Access policies to decide whether to grant or deny access.

What is a sign-in risk?

A. The probability that the device is owned by the identity owner.
B. The probability that the authentication request is not authorized by the identity owner.
C. The probability that the user is authorized to view data from a particular application.
D. The probability that a given identity or account is compromised.

Question # 7 (Multiple Choice)

Which two Azure Active Directory features can be implemented for end users to see the relevant legal disclaimers or the compliance requirement statement being displayed?

A. Terms of use
B. Conditional Access Policy
C. Privileged Identity Management
D. Identity Protection

Question # 8 (Multiple Choice)

You want to restrict and audit an administrator's access in Azure Active Directory (Azure AD).

Which two Azure AD features can you use to provide just-in-time and audit administrator access to Azure resources?

A. Azure AD conditional access policies
B. Azure AD privileged Identity Management (PIM)
C. Azure AD privileged Access Management (PAM)
D. Azure AD Identity Protection

Question # 9 (Multiple Choice)

Which basic native cost-effective Azure service can be used to filter the traffic to Azure Virtual Machines?

A. Bastion
B. Firewall
C. Network Security Groups
D. DDoS Protection

Question # 10 (Sentence Completion)

Select the answer that correctly completes the sentence.

Your Chief Information Security Officer does not want to allow port 3389/22 for connecting to virtual machines in Azure.

You need to implement _______________service to securely connect (SSH/RDP) into an Azure Linux/Windows machine through the browser and the Azure portal.

A. Azure Bastion Service
B. Azure Firewall
C. Azure Load Balancer
D. Network Security Group

Question # 11 (Multiple Choice)

You need to strengthen your cloud security posture and have a secure score in comparison to industry standards. You also need to view reports of various security configurations done in the environment.

Which tool helps you complete these tasks?

A. Azure Sentinel
B. Microsoft Defender for Cloud
C. Azure Firewall
D. Microsoft 365 Defender

Question # 12 (Sentence Completion)

Select the answer that correctly completes the sentence.

Azure ________________________ is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat protection.

A. Advisor
B. Bastion
C. Monitor
D. Sentinel

Question # 13 (Multiple Choice)

Which three features are additional in Microsoft Defender for Office 365 Plan 2 when compared with the Microsoft Defender for Office 365 Plan 1?

A. Threat Trackers
B. Automated Investigation and response
C. Safe Attachments
D. Anti-phishing Protection
E. Attack Simulator

Question # 14 (Sentence Completion)

Select the answer that correctly completes the sentence.

________________ is one of the tools in the Microsoft 365 Defender portal and is a representation of a company's security posture.

A. Security Center
B. Secure Score
C. Monitor
D. Sentinel

Question # 15 (Multiple Choice)

An organization uses different types of devices, including Windows, iOS, and Android devices. The administrator for that organization wants to create a security baseline profile in Intune that they will apply across the devices.

Which device can the security baseline profile be applied to?

A. Android devices
B. iOS devices
C. Windows devices
D. Android & iOS devices

Question # 16 (Multiple Choice)

What is the preferred way to add Microsoft compliance documents and resources that are relevant to your organization in the Service Trust Portal?

A. Save the documents to your My Library.
B. Print each document so you can easily refer to them.
C. Download each document.
D. Go to the resources section

Question # 17 (Multiple Choice)

Your organization uses Microsoft Teams to collaborate on all projects. The compliance administrator wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session.

Which capability can address this requirement?

A. Use data loss prevention policies
B. Use Records Management capabilities
C. Use retention policies
D. Use Azure Information Protection

Question # 18 (Sentence Completion)

Select the answer that correctly completes the sentence.

You need to control the use of administrator accounts with standing access to sensitive data. This will ensure that administrators only receive the level of access they need and at the correct time.

You will use a(n) _______________.

A. communication compliance
B. audit log
C. role-based access management
D. privileged access management

Question # 19 (Multiple Choice)

You need to use the advanced e-Discovery capability to help your legal team with a case.

Which workflow should you use?

A. Search custodial data, add data to a review set, review and analyze data, add custodians to a case, then finally export and download case data.
B. Add custodians to a case, search custodial sources for relevant data, add data to a review set, review and analyze data, then finally export, and download the case data.
C. Add data to a review set, review and analyze data, add custodians to a case, search custodial sources for relevant data, then finally export and download the case data.

D. Review and analyze data in a review set, add custodians to case, add data to review set, export and download case data

Question # 20 (Matching)

Match the Azure service on the left to the correct description on the right.

Azure service

A. Azure Resource Locks
B. Azure Blueprints
C. Azure Policy
D. Azure Role-based access control

Descriptions

______ 1. manages who has access to Azure resources, what they can do with those resources, and what areas they can access

______ 2. enforces standards and assess compliance across your organization

______ 3. rapidly provisions and runs new environments with the knowledge that they are in line with the organization’s compliance requirements

______4. prevents resources from being accidentally deleted or changed

Questions and Answers

Question # 1 (Multiple Choice)

The zero-trust model operates on the principle of “trust no one, verify everything.” You need to implement the zero-trust model in your organization.

Which two options are the guiding principles of a zero-trust model?

A. Verify explicitly
B. Assume breach
C. Role based access
D. Perimeter security

Answer:	A, B
Objective:	1.1 Describe security and compliance concepts & methodologies
Rationale:	The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach. **Verify explicitly.** Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies. **Least privileged access**. Limit user access with just-in-time and just-enough access (JIT/JEA), risk based adaptive policies, and data protection to protect both data and productivity. **Assume breach.** Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.
URL:	https://docs.microsoft.com/en-us/learn/modules/describe-security-concepts-methodologies/2-describe-zero-trust-methodology?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.wwl.describe-concepts-of-security-compliance-identity

Question # 2 (Matching)

Match the type of attack on the left to the correct description on the right.

Type of attack

A. Brute force attacks
B. Phishing
C. Spear phishing
D. Spray Attacks

Descriptions

______ 1. an attack that tries many passwords against one or more accounts, sometimes using dictionaries of commonly used passwords

______ 2. an attack which attempts to match a username against a list of weak passwords

______ 3. an attack which is received in the form of an email that appears to come from a reputable source

______ 4. a highly targeted form of email attack which can be used to create highly credible emails

Answer:	A1, B3, C4, D2
Objective:	1.2 Define identity concepts
Rationale:	Password based attacks include password spray attacks and brute force attacks. A **password spray** attack attempts to match a username against a list of weak passwords. **Brute force attacks** try many passwords against one or more accounts, sometimes using dictionaries of commonly used passwords. When a user has assigned a weak password to their account, the hacker will find a match, and gain access to that account **A phishing attack** is when a hacker sends an email that appears to come from a reputable source. The email contains a credible story, such as a security breach, instructing the user to sign in and change their password. Instead of going to a legitimate website, the user is directed to the scammer's website where they enter their username and password. The hacker has now captured the user's identity, and their password **A spear phishing scam** is a variant on phishing. Hackers build databases of information about users, which can be used to create highly credible emails. The email may appear to come from someone in your organization who is requesting information. Although careful scrutiny might uncover the fraud, users might not read it carefully enough and send the requested information or log in to the web site before they realize the fraud. It is called spear phishing because it is highly targeted.
URL:	Protecting your organization against password spray attacks - Microsoft Security Blog https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

Question # 3 (Matching)

Match the Azure Active Directory (Azure AD) device identity on the left to the correct description on the right.

Azure AD device identity

A. Azure AD registered devices
B. Azure AD joined devices
C. Hybrid Azure AD joined devices

Descriptions

______ 1. These devices are owned by an organization and are signed in with an Active Directory Domain Service account belonging to that organization. They exist in the cloud and on-premises.

______ 2. These devices are typically personally owned, rather than by the organization. They are signed in with a personal Microsoft account or another local account.

______ 3. These devices exist only in the cloud and are owned by an organization. They are signed in with an organization Azure AD account.

Answer:	A2, B3, C1
Objective:	2.1 Describe the basic identity services and identity types of Azure AD
Rationale:	**Azure AD registered devices** can be Windows 10, iOS, Android, or macOS devices. Devices that are Azure AD registered are typically owned personally, rather than by

	the organization. They are signed in with a personal Microsoft account or another local account. **Azure AD joined devices** exist only in the cloud. Azure AD joined devices are owned by an organization and signed in with an organization Azure AD account. Users sign into their devices with their Azure AD or synced Active Directory work or school accounts. You can configure Azure AD joined devices for all Windows 10 devices (except Windows 10 Home). **Hybrid Azure AD joined devices** can be Windows 7, 8.1, or 10 or Windows Server 2008 or newer. Devices that are hybrid Azure AD joined are owned by an organization and are signed in with an Active Directory Domain Services account belonging to that organization. They exist in the cloud and on-premises
URL:	What is device identity in Azure Active Directory? | Microsoft Docs Device Identity: https://docs.microsoft.com/en-us/learn/modules/explore-basic-services-identity-types/4-describe-identity-types?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-identity-access-management-solutions

Question # 4 (Multiple Choice)

You need to look for a hybrid identity solution between Azure Active Directory (Azure AD) and your on-premises active directory. It needs to provide a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers.

Which authentication method should you use?

A. Password Hash synchronization
B. Pass-through authentication
C. Federated authentication
D. Directory synchronization

Answer:	B
Objective:	2.1 Describe the basic identity services and identity types of Azure AD
Rationale:	**Pass-through authentication (PTA)**. Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with an on-premises Active Directory, which ensures that the password validation does not happen in the cloud.
URL:	https://docs.microsoft.com/en-us/learn/modules/explore-basic-services-identity-types/6-describe-concept-of-hybrid-identities

Question # 5 (Multiple Choice)

To improve identity security within the organization, the security team wants to implement Windows Hello for Business. You need to explain the benefits of Windows Hello for Business.

Which statement is true?

A. Windows Hello is an authentication feature built into Windows Server 2012 R26.
B. Windows Hello is an alternative to multi-factor authentication.
C. Windows Hello is a secure feature that uses PINs and bio-metric data to authenticate users.
D. Windows Hello is a feature only for Azure Active Directory premium customers.

Answer:	C
Objective:	2.2 Describe the authentication capabilities of Azure AD
Rationale:	Windows Hello, an authentication feature built into Windows 10, replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a bio-metric or PIN.
URL:	https://docs.microsoft.com/en-us/learn/modules/explore-authentication-capabilities/4-describe-windows-hello-for-business

Question # 6 (Multiple Choice)

Sign-in risk is a signal used by Conditional Access policies to decide whether to grant or deny access.

What is a sign-in risk?

A. The probability that the device is owned by the identity owner.
B. The probability that the authentication request is not authorized by the identity owner.
C. The probability that the user is authorized to view data from a particular application.
D. The probability that a given identity or account is compromised.

Answer:	B
Objective:	2.3 Describe the access management capabilities of Azure AD
Rationale:	Sign-in risk is the real-time calculation that a given authentication request was made by the specific user's identity. Real-time sign-in risk detection- Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to perform password changes or multifactor authentication to reduce their risk level or be blocked from access until an administrator takes manual action. Sign-in risk is independent of device, access rights and only works on signals like: Anonymous IP address, Atypical travel, Anomalous Token, Token Issuer Anomaly, Malware linked IP address, Suspicious browser, Unfamiliar sign-in properties, Admin confirmed user compromised, Malicious IP address, Suspicious inbox manipulation rules, Password spray, Impossible travel, New country, Activity from anonymous IP address, Suspicious inbox forwarding, Azure AD threat intelligence.
URL:	https://docs.microsoft.com/en-us/learn/modules/explore-access-management-capabilities/2-describe-conditional-access-its-benefits https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Question # 7 (Multiple Choice)

Which two Azure Active Directory features can be implemented for end users to see the relevant legal disclaimers or the compliance requirement statement being displayed?

A. Terms of use
B. Conditional Access Policy
C. Privileged Identity Management
D. Identity Protection

Answer:	A, B
Objective:	2.4 Describe the identity protection & governance capabilities of Azure AD
Rationale:	**Conditional Access policies** are used to require a terms of use statement being displayed and ensuring the user has agreed to those terms before accessing an application. Admins can then view who has agreed to terms of use, and who has declined. **Azure AD terms of use** allow information to be presented to users before they access data or an application. Terms of use ensure users read relevant disclaimers for legal or compliance requirements.
URL:	https://docs.microsoft.com/en-us/learn/modules/describe-identity-protection-governance-capabilities/3-describe-what-entitlement-management-access-reviews

Question # 8 (Multiple Choice)

You want to restrict and audit an administrator's access in Azure Active Directory (Azure AD).

Which two Azure AD features can you use to provide just-in-time and audit administrator access to Azure resources?

A. Azure AD conditional access policies
B. Azure AD privileged Identity Management (PIM)
C. Azure AD privileged Access Management (PAM)
D. Azure AD Identity Protection

Answer:	B, C
Objective:	2.4 Describe the identity protection & governance capabilities of Azure AD
Rationale:	Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Privileged Access Management (PAM) is a solution that helps organizations restrict privileged access within an existing and isolated Active Directory environment. PAM adds auditing, alerts, and reports of privileged access requests. You can review the history of privileged access and see who performed an activity. You can decide whether the activity is valid or not and easily identify unauthorized activity, such as an attempt to add a user directly to a privileged group in the original forest. This step is

	important not only to identify malicious software but also for tracking "inside" attackers.
URL:	https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure PIM-MS learn- https://docs.microsoft.com/en-us/learn/modules/describe-identity-protection-governance-capabilities/4-describe-privileged-identity-management Privileged Access Management for Active Directory Domain Services | Microsoft Docs

Question # 9 (Multiple Choice)

Which basic native cost-effective Azure service can be used to filter the traffic to Azure Virtual Machines?

A. Bastion
B. Firewall
C. Network Security Groups
D. DDoS Protection

Answer:	C
Objective:	3.1 Describe basic security capabilities in Azure
Rationale:	Network Security Group -Network security groups (NSGs) let you allow or deny network traffic to and from Azure resources that exist in your Azure virtual network, for example, a virtual machine. When you create an NSG, it can be associated with multiple subnets or network interfaces in your VNet. An NSG consists of rules that define how the traffic is filtered.
URL:	https://docs.microsoft.com/en-us/learn/modules/describe-basic-security-capabilities-azure/2-describe-azure-network-security-groups

Question # 10 (Sentence Completion)

Select the answer that correctly completes the sentence.

Your Chief Information Security Officer does not want to allow port 3389/22 for connecting to virtual machines in Azure.

You need to implement _______________service to securely connect (SSH/RDP) into an Azure Linux/Windows machine through the browser and the Azure portal.

A. Azure Bastion Service
B. Azure Firewall
C. Azure Load Balancer
D. Network Security Group

Answer:	A
Objective:	3.1 Describe basic security capabilities in Azure

Rationale:	Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. This article shows you how to securely and seamlessly SSH to your Linux VMs in an Azure virtual network. You can connect to a VM directly from the Azure portal. When using Azure Bastion, VMs don’t require a client, agent, or additional software
URL:	https://docs.microsoft.com/en-us/azure/bastion/bastion-connect-vm-ssh Azure Bastion- https://docs.microsoft.com/en-us/learn/modules/describe-basic-security-capabilities-azure/5-describe-what-azure-bastion?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-security-solutions

Question # 11 (Multiple Choice)

You need to strengthen your cloud security posture and have a secure score in comparison to industry standards. You also need to view reports of various security configurations done in the environment.

Which tool helps you complete these tasks?

A. Azure Sentinel
B. Microsoft Defender for Cloud
C. Azure Firewall
D. Microsoft 365 Defender

Answer:	B
Objective:	3.2 Describe security management capabilities of Azure
Rationale:	**Microsoft Defender for Cloud** is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms. Defender for Cloud provides the tools needed to harden your resources, track your security posture, protect against cyberattacks, and streamline security management. Because it's natively integrated, deployment of Defender for Cloud is easy, providing you with simple auto provisioning to secure your resources by default.
URL:	https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction Microsoft Defender for Cloud- https://docs.microsoft.com/en-us/learn/modules/describe-security-management-capabilities-of-azure/3-describe-defender-cloud Microsoft Sentinel- https://docs.microsoft.com/en-us/learn/modules/describe-security-capabilities-of-azure-sentinel/

Question # 12 (Sentence Completion)

Select the answer that correctly completes the sentence.

Azure _______________________ is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat protection.

A. Advisor
B. Bastion
C. Monitor
D. Sentinel

Answer:	D
Objective:	3.3 Describe security capabilities of Azure Sentinel
Rationale:	Azure Sentinel – Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.
URL:	https://docs.microsoft.com/en-us/azure/sentinel/overview Microsoft Sentinel- https://docs.microsoft.com/en-us/learn/modules/describe-security-capabilities-of-azure-sentinel/

Question # 13 (Multiple Choice)

Which three features are additional in Microsoft Defender for Office 365 Plan 2 when compared with the Microsoft Defender for Office 365 Plan 1?

A. Threat Trackers
B. Automated Investigation and response
C. Safe Attachments
D. Anti-phishing Protection
E. Attack Simulator

Answer:	A, B, E
Objective:	3.4 Describe threat protection with Microsoft 365 Defender
Rationale:	Microsoft Defender for Office 365 Plan 2 includes all the core features of Plan 1, and provides automation, investigation, remediation, and simulation tools to help protect your Office 365 suite: • **Threat Trackers:** Provide the latest intelligence on prevailing cybersecurity issues and allow an organization to take countermeasures before there's an actual threat. • **Threat Explorer:** A real-time report that allows you to identify and analyze recent threats. • **Automated investigation and response (AIR):** Includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually. A security playbook can start an automated investigation, provide detailed results, and recommend actions that the security team can approve or reject.

	- **Attack Simulator:** Allows you to run realistic attack scenarios in your organization to identify vulnerabilities.
URL:	https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365?view=o365-worldwide MS- Learn- https://docs.microsoft.com/en-us/learn/modules/describe-threat-protection-with-microsoft-365-defender/4-describe-defender-office

Question # 14 (Sentence Completion)

Select the answer that correctly completes the sentence.

________________ is one of the tools in the Microsoft 365 Defender portal and is a representation of a company's security posture.

A. Security Center
B. Secure Score
C. Monitor
D. Sentinel

Answer:	B
Objective:	3.5 Describe security management capabilities of Microsoft 365
Rationale:	Microsoft Secure Score, one of the tools in the Microsoft 365 Defender portal, is a representation of a company's security posture. The higher the score, the better your protection. Secure Score helps organizations: - Report on the current state of their security posture. - Improve their security posture by providing discoverability, visibility, guidance, and control. - Compare benchmarks and establish key performance indicators (KPIs).
URL:	Microsoft Secure Score | Microsoft Docs Microsoft Sentinel- https://docs.microsoft.com/en-us/learn/modules/describe-security-capabilities-of-azure-sentinel/

Question # 15 (Multiple Choice)

An organization uses different types of devices, including Windows, iOS, and Android devices. The administrator for that organization wants to create a security baseline profile in Intune that they will apply across the devices.

Which device can the security baseline profile be applied to?

A. Android devices
B. iOS devices
C. Windows devices
D. Android & iOS devices

Answer:	C
Objective:	3.6 Describe endpoint security with Microsoft Intune
Rationale:	Security baseline settings are used only on devices running Windows 10 version 1809 or later.
URL:	https://docs.microsoft.com/en-us/learn/modules/describe-endpoint-security-with-microsoft-intune/3-intune Manage security baselines- https://docs.microsoft.com/en-us/learn/modules/describe-endpoint-security-with-microsoft-intune/3-intune?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-security-solutions

Question # 16 (Multiple Choice)

What is the preferred way to add Microsoft compliance documents and resources that are relevant to your organization in the Service Trust Portal?

A. Save the documents to your My Library.
B. Print each document so you can easily refer to them.
C. Download each document.
D. Go to the resources section

Answer:	A
Objective:	4.1 Describe the compliance management capabilities in Microsoft
Rationale:	Save the documents to My Library: Allows you to add documents and resources that are relevant to your organization, everything is in one place. You can also opt to have email notifications sent when a document is updated, as well as the frequency you receive notifications.
URL:	Service Trust Portal (microsoft.com) MS learn link- https://docs.microsoft.com/en-us/learn/modules/describe-compliance-management-capabilities-microsoft/2a-describe-offerings-of-service-trust-portal

Question # 17 (Multiple Choice)

Your organization uses Microsoft Teams to collaborate on all projects. The compliance administrator wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session.

Which capability can address this requirement?

A. Use data loss prevention policies
B. Use Records Management capabilities
C. Use retention policies
D. Use Azure Information Protection

Answer:	A
Objective:	4.2 Describe information protection and governance capabilities of Microsoft 365
Rationale:	With data loss prevention policies, administrators can now define policies that can prevent users from sharing sensitive information in a Microsoft Teams chat session or Teams channel, whether this information is in a message, or in a file. Records Management or Retention policies/AIP will not let you do this
URL:	https://docs.microsoft.com/en-us/learn/modules/describe-information-protection-governance-capabilities-microsoft-365/5-describe-data-loss-prevention

Question # 18 (Sentence Completion)

Select the answer that correctly completes the sentence.

You need to control the use of administrator accounts with standing access to sensitive data. This will ensure that administrators only receive the level of access they need and at the correct time.

You will use a(n) _______________.

A. communication compliance
B. audit log
C. role-based access management
D. privileged access management

Answer:	D
Objective:	4.3 Describe insider risk capabilities in Microsoft 365
Rationale:	You can use privileged access management to require users to request just-in-time access to complete certain tasks. Privileged access management allows granular access control over privileged admin tasks in Microsoft 365. It can help protect organizations from breaches that use existing privileged admin accounts with standing access to sensitive data, or access to critical configuration settings.
URL:	https://docs.microsoft.com/en-us/learn/modules/describe-insider-risk-capabilities-microsoft-365/5-describe-privileged-access-management

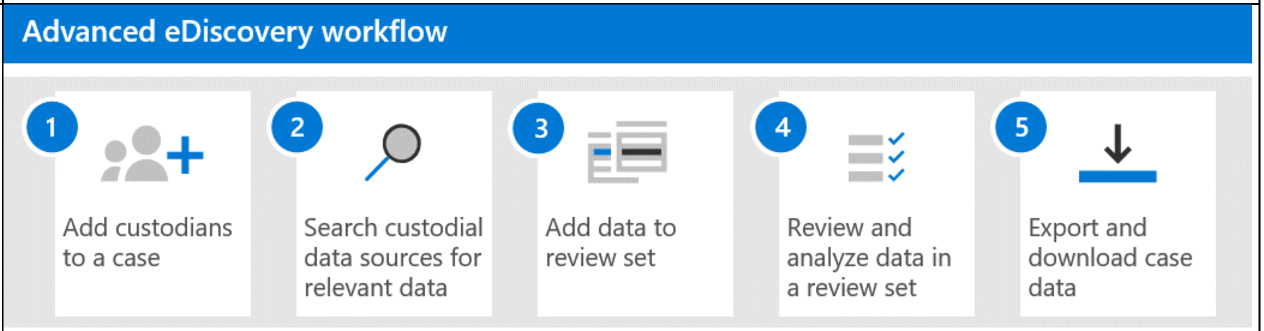
Question # 19 (Multiple Choice)

You need to use the advanced e-Discovery capability to help your legal team with a case.

Which workflow should you use?

A. Search custodial data, add data to a review set, review and analyze data, add custodians to a case, then finally export and download case data.
B. Add custodians to a case, search custodial sources for relevant data, add data to a review set, review and analyze data, then finally export, and download the case data.
C. Add data to a review set, review and analyze data, add custodians to a case, search custodial sources for relevant data, then finally export and download the case data.

D. Review and analyze data in a review set, add custodians to case, add data to review set, export and download case data

Answer:	B
Objective:	4.4 Describe the eDiscovery and audit capabilities of Microsoft 365
Rationale:	 Advanced eDiscovery workflow 1 Add custodians to a case 2 Search custodial data sources for relevant data 3 Add data to review set 4 Review and analyze data in a review set 5 Export and download case data The Advanced eDiscovery workflow.
URL:	[Describe the advanced eDiscovery workflow - Learn | Microsoft Docs]

Question # 20 (Matching)

Match the Azure service on the left to the correct description on the right.

Azure service

A. Azure Resource Locks
B. Azure Blueprints
C. Azure Policy
D. Azure Role-based access control

Descriptions

______ 1. manages who has access to Azure resources, what they can do with those resources, and what areas they can access

______ 2. enforces standards and assess compliance across your organization

______ 3. rapidly provisions and runs new environments with the knowledge that they are in line with the organization's compliance requirements

______4. prevents resources from being accidentally deleted or changed

Answer:	A4, B3, C2, D1
Objective:	4.5 Describe resource governance capabilities in Azure
Rationale:	**Resource locks** can be used to prevent resources from being accidentally deleted or changed. Even with role-based access control policies in place there is still a risk that people with the right level of access could delete a critical resource. Azure Resource Manager locks prevent users from accidentally deleting or modifying a critical resource, and can be applied to a subscription, a resource group, or a resource **Azure Blueprints** provide a way to define a repeatable set of Azure resources. Azure Blueprints enable development teams to rapidly provision and run new environments, with the knowledge that they're in line with the organization's compliance

	requirements. Teams can also provide Azure resources across several subscriptions simultaneously, meaning they can achieve shorter development times and quicker delivery. **Azure Policy** is designed to help enforce standards and assess compliance across your organization. Through its compliance dashboard, you can access an aggregated view to help evaluate the overall state of the environment. You can drill down to a per-resource, or per-policy level granularity. You can also use capabilities like bulk remediation for existing resources and automatic remediation for new resources, to resolve issues rapidly and effectively **Azure RBAC** manages who has access to Azure resources, what they can do with those resources, and what areas they can access. If actions need to be controlled, then you would use Azure RBAC.
URL:	Understand how effects work - Azure Policy | Microsoft Docs Lock resources to prevent changes - Azure Resource Manager | Microsoft Docs Overview of Azure Blueprints - Azure Blueprints | Microsoft Docs What is Azure role-based access control (Azure RBAC)? | Microsoft Docs