Latest Version: 22.0

Question: 1

A company plans to migrate to Microsoft 365.
You need to advise the company about how Microsoft provides protection in a multitenancy environment. What are three ways that Microsoft provides protection? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Customer content at rest is encrypted on the server by using BitLocker.
B. Microsoft Azure AD provides authorization and role based access control at the tenant layer.
C. Customer content at rest is encrypted on the server by using transport layer security (TLS).
D. Microsoft Azure AD provides authorization and role based access control at the transport layer.
E. Mailbox databases in Microsoft Exchange Online contain only mailboxes from a single tenant.
F. Mailbox databases in Microsoft Exchange Online contain mailboxes from multiple tenants.

Answer: ABF

Question: 2

You are the Microsoft 365 administrator for a company.
Your company plans to open a new office in the United Kingdom.
You need to provide penetration test and security assessment reports (or the new office.
Where can you locate the required reports?

A. Data Governance page of the Security and Compliance portal.
B. Compliance Manager page of the Services Trust portal
C. Data Loss Prevention page of the Security and Compliance portal
D. Regional Compliance page of the Services Trust portal

Answer: D

Question: 3

HOTSPOT
An organization plans to deploy Microsoft Intune.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

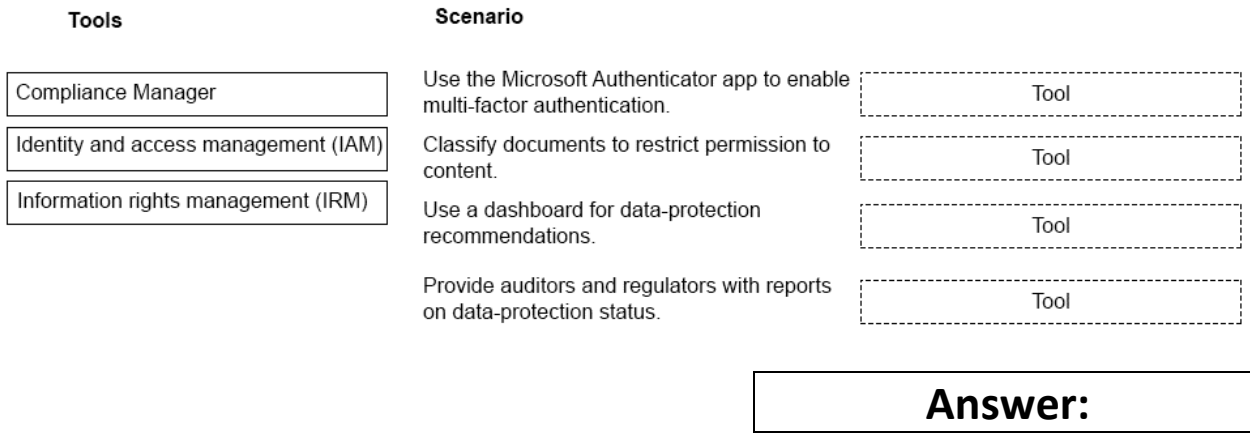
Statement	Yes	No
Data protection can be selectively applied to applications.	○	○
Microsoft intune can define where corporate data is stored.	○	○
Once a device is registered with Microsoft Intune, device wipe will include the user's personal data.	○	○

Answer:

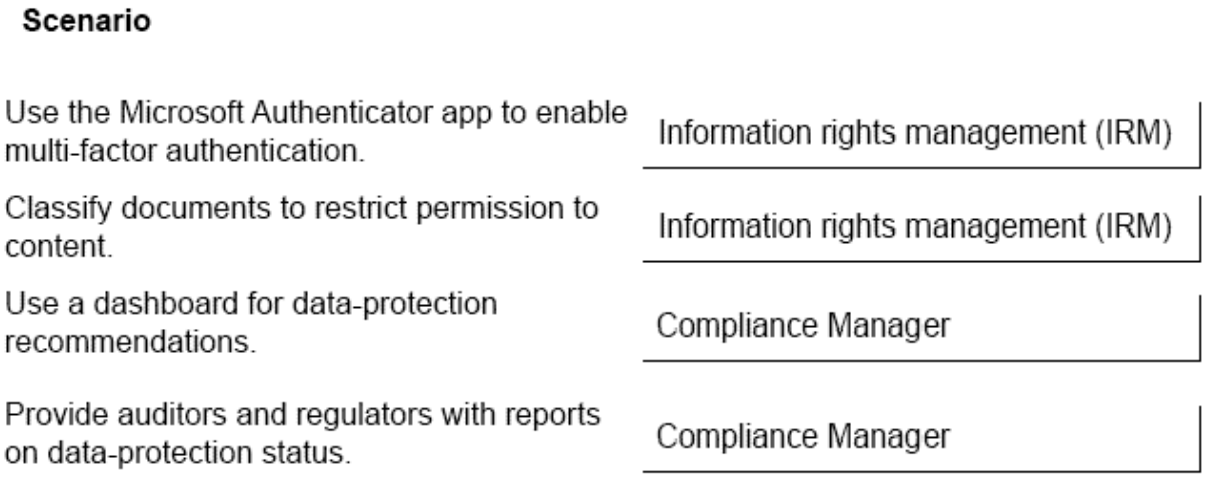
Statement	Yes	No
Data protection can be selectively applied to applications.	○	○
Microsoft intune can define where corporate data is stored.	○	○
Once a device is registered with Microsoft Intune, device wipe will include the user's personal data.	○	○

Question: 4

DRAG DROP
Your company has a Microsoft 365 subscription.
You need to implement security policies to ensure that sensitive data is protected.
Which tools should you use? To answer, drag the appropriate tools to the correct scenarios. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



References:
https://docs.microsoft.com/en-us/azure/information-protection/help-users
https://docs.microsoft.com/en-us/office365/securitycompliance/compliance-manageroverview#controls

Question: 5

HOTSPOT
You are planning a Microsoft Azure AD solution for a company.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statement	Yes	No
You can manage Azure AD-joined machines by using group policy.	○	○
Azure AD requires integration with Active Directory Domain Services by using secure lightweight Directory Access Protocol (LDAP).	○	○
Azure AD supports Azure AD Authentication Library (ADAL) authentication.	○	○

Answer:

YES
NO
NO

Yes – https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy
Settings for user and computer objects in Azure Active Directory Domain Services (Azure AD DS) are often managed using Group Policy Objects (GPOs).
Yes – https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps
To communicate with your Azure Active Directory Domain Services (Azure AD DS) managed domain, the Lightweight Directory Access Protocol (LDAP) is used. By default, the LDAP traffic isn't encrypted, which is a security concern for many environments.
Yes – https://docs.microsoft.com/en-us/azure/active-directory/azuread-dev/active-directoryauthentication-libraries
The Azure Active Directory Authentication Library (ADAL) v1.0 enables application developers to authenticate users to cloud or on-premises Active Directory (AD), and obtain tokens for securing API calls.