Microsoft Azure Security Engineer (AZ-500)

50 Questions & Answers

Welcome to your complete AZ-500 practice question collection.
*This set is designed **not just for testing, but also to teach**, strengthen, and deepen your readiness.*

Learning Objectives and Expectations

You'll get:
- Real-world style questions modeled after Microsoft AZ-500 exam wording and scenario depth.
- Organized by domains with detailed answers and explanations for self-verification.
- Concise explanations that reinforce key Azure security principles and clarify correct logic.

AZ-500 Domains

Each domain is weighted differently on the exam:
- **Domain 1:** Manage Identity and Access (25–30%)
- **Domain 2:** Secure Networking (20–25%)
- **Domain 3:** Secure Compute, Storage, and Databases (20–25%)
- **Domain 4:** Manage Security Operations (25–30%)

Quick Reminder: How the Exam Works

- **Number of Questions:** ~40–60
- **Format:** Multiple choice, multiple select, drag-and-drop, and case studies (no labs as of 2025)
- **Time Limit:** 150 minutes
- **Passing Score:** 700/1000 (≈70%)
- **Test Provider:** Pearson VUE (onsite or online)

Questions by Domain

Domain	Title	Assigned	Numbers
Domain 1	Manage Identity and Access (25–30%)	11 Questions	Q1–Q6, Q19, Q24, Q34, Q35, Q38
Domain 2	Secure Networking (20–25%)	10 Questions	Q7–Q10, Q16–Q18, Q20, Q22, Q26
Domain 3	Secure Compute, Storage, and Databases (20–25%)	12 Questions	Q11–Q15, Q21, Q23, Q25, Q27–Q28, Q31–Q33
Domain 4	Manage Security Operations (25–30%)	17 Questions	Q29–Q30, Q36–Q37, Q39–Q50

Exam Mindset

Remember—you don't need to be perfect to pass!

The AZ-500 passing score is **700/1000 (≈70%)**, so you can miss several challenging or scenario-heavy questions and still succeed. Focus on understanding **Azure security configurations, Defender for Cloud, RBAC, Conditional Access, and NSG/Firewall behavior** rather than memorizing.

Stay calm, analyze scenarios step-by-step, and trust your preparation.

Q1. (Scenario)

A security engineer needs to ensure database operators can manage Azure SQL resources but cannot grant or revoke access to others. Which role should be assigned at the resource group scope to honor least privilege?

A) Owner
B) Contributor
C) User Access Administrator
D) Security Administrator
E) Reader

Answer: B) Contributor
Explanation: Contributor can create and modify resources but cannot manage RBAC assignments, aligning with least privilege.

Q2. (Hotspot)

Evaluate Azure RBAC statements and select Yes or No for each.

Statement	Yes / No
Permissions inherit down the scope hierarchy	
Deny assignments take precedence over allow permissions	
Users can manually create deny assignments	

Answer: Yes, Yes, No
Explanation: Permissions flow Management Group → Subscription → Resource Group → Resource. Deny is evaluated first, and deny assignments are system created, not user authored.

Q3. (Multiple Choice) Select TWO

You must enforce MFA only when a sign-in is deemed risky and keep normal low-risk sign-ins frictionless. Which options meet this requirement?

A) Security Defaults
B) Per-user MFA
C) Conditional Access with Sign-in Risk conditions
D) Identity Protection User Risk policy
E) Enabling MFA inside PIM only

Answer: C) Conditional Access with Sign-in Risk conditions, D) Identity Protection User Risk policy
Explanation: Risk-based CA applies MFA based on sign-in risk, and Identity Protection policies can force password reset or MFA based on user or sign-in risk.

Q4. (Drag & Drop)

Match each risk type to its description.

Risk Type	Description
User Risk	A. Indicates compromised credentials or ongoing account compromise
Sign-in Risk	B. Indicates session anomalies such as impossible travel or TOR usage

Correct Mapping: 1-A 2-B
Explanation: User Risk focuses on the user account compromise; Sign-in Risk assesses the specific session context and anomalies.

Q5. (Case Study)

Admins must elevate to privileged roles only when needed, provide justification, and perform MFA at activation. Activations should expire automatically and optionally require approval.
Which feature should you implement?

A) Access Packages
B) Privileged Identity Management
C) Azure Policy Initiatives
D) Microsoft Sentinel Playbooks
E) Management Groups

Answer: B) Privileged Identity Management
Explanation: PIM provides just-in-time elevation, MFA at activation, time-bound roles, and optional approval workflows.

Q6. (Multiple Choice) Select TWO

You are standardizing identity for app-to-service authentication without storing secrets.
Which two choices meet this goal for Azure services like Key Vault and Storage?

A) Service Principal with client secret stored in code
B) System-assigned Managed Identity
C) User-assigned Managed Identity
D) Shared Access Signature tokens
E) SQL logins with strong passwords

Answer: B) System-assigned Managed Identity, C) User-assigned Managed Identity
Explanation: Managed Identities avoid manual secret management by using auto-rotated credentials managed by Azure.

Q7. (Hotspot)

You are configuring Azure Firewall in a hub-and-spoke design. For each statement, select Yes or No.

Statement	Yes / No
Azure Firewall supports TLS inspection for outbound HTTPS traffic	
It provides built-in IDPS to detect exploits	
It cannot perform DNAT for inbound scenarios	

Answer: Yes, Yes, No
Explanation: Premium SKU supports TLS inspection; Firewall includes IDPS and supports DNAT and SNAT.

Q8. (Multiple Choice) Select TWO

A global retail app must protect public web traffic at Layer 7, minimize latency for worldwide users, and block common web attacks at the edge. Which two services satisfy the requirements?

A) Azure Front Door with WAF
B) Application Gateway WAF in a single region only
C) Azure Firewall only
D) Azure Front Door CDN without WAF
E) ExpressRoute with private peering

Answer: A) Azure Front Door with WAF, B) Application Gateway WAF in a single region only
Explanation: Both provide WAF protections; Front Door adds global edge load balancing and CDN for low latency, while App Gateway is regional.

Q9. (Hotspot)

You attach an NSG to a subnet that hosts web servers. Decide Yes or No.

Statement	Yes / No
Inbound traffic is denied by default	
Outbound traffic is allowed by default	
Rules are evaluated bottom-up with last match winning	

Answer: Yes, Yes, No
Explanation: NSGs deny inbound by default and allow outbound by default. Rules are processed by priority from lowest number to highest; first match applies.

Q10. (Multiple Choice) Select TWO

You must guarantee private access from your VNet to Azure SQL Database with the strongest isolation from the public internet and enforce traffic inspection with your central firewall. Which two configurations meet the requirement?

A) Private Endpoint for SQL plus UDRs to route through the hub firewall
B) Service Endpoint for SQL and allow Azure services toggle
C) Public endpoint with IP firewall rules only
D) Private Endpoint for SQL and disable public network access on the server
E) NAT Gateway for outbound

Answer: A) Private Endpoint for SQL plus UDRs to route through the hub firewall, D) Private Endpoint for SQL and disable public network access on the server
Explanation: Private Endpoints assign a private IP in your VNet, eliminating public exposure; combining with firewall routing or disabling public network access ensures strongest isolation.

Q11. (Scenario)

You must ensure that every newly created resource group in a subscription automatically inherits encryption and tagging policies for compliance. Which Azure governance service enables this consistent configuration at scale?

A) Management Groups
B) Azure Policy Initiatives
C) Azure Blueprints
D) Azure Automation Accounts
E) Resource Locks

Answer: B) Azure Policy Initiatives
Explanation: Policy Initiatives group multiple policy definitions (e.g., encryption + tag requirements) for enforcement across scopes like subscriptions or management groups.

Q12. (Multiple Choice) Select TWO

Your team wants all VMs to auto-install a monitoring agent and deny creation of any without encryption enabled. Which two solutions can enforce these standards?

A) Azure Policy with deployIfNotExists effect
B) Azure Monitor Workbooks
C) Azure Automation Update Management
D) Defender for Cloud Recommendations + Secure Score
E) Azure Firewall Threat Intelligence filtering

Answer: A) Azure Policy with deployIfNotExists effect, D) Defender for Cloud Recommendations + Secure Score
Explanation: Policies can auto-deploy extensions and enforce encryption; Defender for Cloud identifies and tracks non-compliance via Secure Score.

Q13. (Hotspot)

Review the statements about Microsoft Defender for Cloud.

Statement	Yes / No
It provides a unified Secure Score across subscriptions	
It replaces Azure Policy as the compliance engine	
It maps posture to frameworks like CIS and NIST	

Answer: Yes, No, Yes

Explanation: Defender for Cloud aggregates Secure Score and compliance data but relies on Azure Policy for enforcement.

Q14. (Multiple Choice) Select TWO

You need centralized visibility into all NSG Flow Logs and Key Vault diagnostic data for alerting and investigation. Which two components are required?

A) Azure Monitor
B) Log Analytics Workspace
C) Network Watcher only
D) Azure Storage Account for archival logs
E) Microsoft Sentinel Workspace

Answer: A) Azure Monitor, B) Log Analytics Workspace

Explanation: Azure Monitor collects metrics and routes them to a Log Analytics Workspace for retention and KQL analysis; Sentinel can later consume that workspace.

Q15. (Drag & Drop)

Match each Defender for Cloud plan to what it protects.

Plan	Scope
Defender for Servers	A. VMs and hybrid servers – JIT access and vulnerability assessment
Defender for Storage	B. Blob and File shares – detect malware and exfiltration
Defender for Key Vault	C. Alerts on unusual secret access
Defender for Databases	D. SQL/CosmosDB threat detection

Correct Mapping: 1-A 2-B 3-C 4-D

Explanation: Each Defender plan focuses on its corresponding Azure service type.

Q16. (Scenario)

A company runs several AKS clusters and must prevent pods from running with privileged containers while continuously scanning images. Which combined configuration meets this requirement?

A) Network Policies + Private Link
B) Defender for Containers + Azure Policy for AKS
C) Defender for Servers Plan 2 + JIT Access
D) Azure Monitor Container Insights only
E) Manual kubectl auditing

Answer: B) Defender for Containers + Azure Policy for AKS

Explanation: Defender for Containers handles image scanning and runtime protection, while Azure Policy enforces Kubernetes security controls (e.g., disallow privileged containers).

Q17. (Multiple Choice) Select TWO

You must ensure sensitive blob data cannot be accessed publicly and that all transfers use HTTPS. Which two configurations achieve this?

A) Enable Secure Transfer Required on the Storage Account
B) Add a Private Endpoint to the Storage Account
C) Use Service Endpoints only
D) Allow public blob access for faster content delivery
E) Assign Storage Blob Data Reader role to Everyone

Answer: A) Enable Secure Transfer Required, B) Add a Private Endpoint to the Storage Account
Explanation: Secure Transfer enforces HTTPS; Private Endpoints restrict traffic to the VNet and remove public exposure.

Q18. (Hotspot)

You enabled Defender for SQL on Azure SQL Database.

Statement	Yes / No
Defender for SQL adds Advanced Threat Protection for anomaly detection	
It requires TDE to be enabled first	
It can send alerts to Log Analytics or Event Hub	

Answer: Yes, No, Yes
Explanation: Defender for SQL includes ATP for threat detection and exports alerts to monitoring destinations; it operates independently of TDE.

Q19. (Multiple Choice) Select TWO

Security operations must automatically disable accounts after five failed logins from foreign locations and open incidents for review. Which two features enable this workflow?

A) Microsoft Sentinel Analytics Rule + Playbook
B) Azure Policy with Deny effect
C) Defender for Cloud Alerts + Secure Score
D) Identity Protection Risk Policy
E) Microsoft Entra Access Reviews

Answer: A) Microsoft Sentinel Analytics Rule + Playbook, D) Identity Protection Risk Policy
Explanation: Sentinel detects brute-force patterns and triggers Playbooks for automated response; Identity Protection can flag risky sign-ins and block accounts.

Q20. (Scenario)

After enabling JIT VM access in Defender for Servers, an admin requests temporary SSH access to a VM for 2 hours. What happens when the timer expires?

A) Session continues until logout but port remains open
B) Defender for Cloud closes the port rule in NSG automatically
C) VM restarts to apply lockdown rules
D) Port stays open until manually removed
E) NSG logs are deleted for privacy

Answer: B) Defender for Cloud closes the port rule in NSG automatically
Explanation: JIT access temporarily opens management ports and automatically removes rules when the approved time expires.

Q21. (Scenario)

A security engineer must ensure that all VM disks are encrypted using customer-managed keys to meet regulatory requirements. What is the most appropriate configuration?

A) Azure Disk Encryption using Platform-Managed Keys
B) Customer-Managed Keys stored in Azure Key Vault
C) BitLocker with local certificate storage
D) Transparent Data Encryption
E) Server-side encryption with Microsoft-managed keys

Answer: B) Customer-Managed Keys stored in Azure Key Vault
Explanation: CMKs give full lifecycle control and meet compliance frameworks requiring key ownership. Keys reside in Key Vault or Managed HSM

Q22. (Multiple Choice) Select TWO

You need to restrict access to an internal web API hosted on Azure App Service so that only traffic from your corporate network reaches it. Which two controls should be used?

A) Private Endpoint for App Service
B) Access Restrictions by IP range
C) NSG on the App Service
D) WAF on Azure Front Door
E) Application Gateway with WAF in Detection mode

Answer: A) Private Endpoint for App Service, B) Access Restrictions by IP range
Explanation: App Service supports network isolation via Private Endpoints and IP-based Access Restrictions; NSGs don’t apply directly to PaaS apps

Q23. (Hotspot)

Examine the following about Azure Disk Encryption.

Statement	Yes / No
ADE can use BitLocker for Windows and DM-Crypt for Linux	
It stores encryption keys in Azure Key Vault	
It automatically enables soft delete for recovery	

Answer: Yes, Yes, No

Explanation: ADE leverages BitLocker/DM-Crypt with keys in Key Vault but soft delete is unrelated; that applies to Key Vault objects, not ADE itself

Q24. (Multiple Choice) Select TWO

Which two features strengthen container workload security in Azure Kubernetes Service (AKS)?

A) Azure AD integration for kubectl authentication
B) Privileged containers for admin access
C) Defender for Containers image scanning
D) Public cluster API endpoints
E) Network Policies restricting pod traffic

Answer: A) Azure AD integration for kubectl authentication, C) Defender for Containers image scanning

Explanation: Azure AD integration secures access, while Defender for Containers scans images and detects runtime anomalies

Q25. (Drag & Drop)

Match each encryption model with its description.

Encryption Model	Description
TDE	A. Encrypts database files transparently at rest
Always Encrypted	B. Keeps encryption keys client-side to protect sensitive columns
Double Encryption	C. Encrypts data at both storage and volume layers

Correct Mapping: 1-A 2-B 3-C

Explanation: TDE secures data files, Always Encrypted protects columns end-to-end, and Double Encryption provides layered defense

Q26. (Scenario)

Your team must visualize traffic between application tiers and identify excessive open ports. Which tool in Azure provides this analysis?

A) Network Watcher – Topology
B) Traffic Analytics in Network Watcher
C) NSG Flow Logs alone
D) Azure Firewall Logs
E) Sentinel Workbooks

Answer: B) Traffic Analytics in Network Watcher

Explanation: Traffic Analytics processes NSG Flow Logs to show communication patterns, allowing optimization of rules and segmentation

Q27. (Multiple Choice) Select TWO

You need to correlate Azure AD sign-in logs and Defender for Cloud alerts for advanced incident response. Which two services enable this?

A) Azure Monitor Metrics
B) Microsoft Sentinel
C) Log Analytics Workspace
D) Azure Policy Initiatives
E) Azure Lighthouse

Answer: B) Microsoft Sentinel, C) Log Analytics Workspace
Explanation: Sentinel consumes data from Log Analytics to perform SIEM correlation and SOAR automation

Q28. (Hotspot)

Consider Defender for Cloud Secure Score.

Statement	Yes / No
It quantifies posture compliance by weighting resolved controls	
It replaces the need for Azure Policy	
It helps prioritize remediation actions	

Answer: Yes, No, Yes
Explanation: Secure Score tracks completion of recommendations and assists prioritization but relies on Azure Policy for enforcement

Q29. (Multiple Choice) Select TWO

A SOC analyst wants automated mitigation when Sentinel detects brute-force logins. Which two components must be configured?

A) Analytics Rule detecting failed sign-ins
B) Logic App Playbook for automatic response
C) Workbooks dashboard only
D) Defender for Cloud Policy Initiative
E) Azure AD Access Review

Answer: A) Analytics Rule detecting failed sign-ins, B) Logic App Playbook for automatic response
Explanation: Sentinel's SOAR capability depends on detection via analytics rules and remediation through Playbooks

Q30. (Scenario)

An organization needs to monitor suspicious activities like data exfiltration, lateral movement, and insider threats across Azure and on-premises environments. Which service fulfills this need?

A) Azure Policy
B) Microsoft Defender for Cloud
C) Microsoft Sentinel
D) Network Watcher
E) Defender for Storage

Answer: C) Microsoft Sentinel
Explanation: Sentinel is a cloud-native SIEM/SOAR aggregating multi-source telemetry for advanced threat detection and hunting

Q31. (Scenario)

A compliance team must prove that all Key Vault access events are logged and retained for 90 days. What should be configured first?

A) Azure Monitor metrics alerts
B) Diagnostic Settings on the Key Vault
C) Defender for Key Vault plan
D) Log Analytics Workspace retention policy
E) Activity Logs in the subscription

Answer: B) Diagnostic Settings on the Key Vault
Explanation: Diagnostic Settings export AuditEvent logs to Log Analytics, Storage, or Event Hub, ensuring compliance visibility. Defender for Key Vault alerts on anomalies but doesn’t enable logging

Q32. (Multiple Choice) Select TWO

You must automatically quarantine blobs if malware is uploaded to a Storage Account. Which two Defender for Cloud features enable this?

A) Defender for Storage plan
B) Malware scanning alerts
C) Azure Policy Initiatives
D) Logic App automation triggered by alerts
E) Secure Transfer Required

Answer: A) Defender for Storage plan, D) Logic App automation triggered by alerts
Explanation: Defender for Storage detects malicious uploads; Logic Apps can act automatically on the generated alert. Azure Policy does not perform runtime detection

Q33. (Hotspot)

Evaluate statements about Microsoft Sentinel components.

Statement	Yes / No
Analytics Rules generate incidents from query results	
Playbooks are used for automated response	
Workbooks store raw log data	

Answer: Yes, Yes, No

Explanation: Analytics Rules detect threats, Playbooks run SOAR workflows, and Workbooks visualize data from Log Analytics but don't store it

Q34. (Multiple Choice) Select TWO

You need to minimize credential exposure and ensure services authenticate securely to Key Vault. Which two options meet this goal?

A) Assign Managed Identities to resources
B) Use Service Principal with client secret
C) Grant Key Vault access via Azure RBAC roles
D) Use Access Policies only
E) Use Storage Account keys for authentication

Answer: A) Assign Managed Identities to resources, C) Grant Key Vault access via Azure RBAC roles

Explanation: Managed Identities authenticate without credentials, and modern RBAC is the preferred access control method over legacy Access Policies

Q35. (Scenario)

You must restrict VM administrators from accessing production resources outside approved hours and log elevations. What combination should be used?

A) Privileged Identity Management (PIM) with time-bound eligibility
B) Azure Policy with deny effect
C) Azure Monitor scheduled alerts
D) Defender for Servers Plan 1
E) Conditional Access named locations

Answer: A) Privileged Identity Management (PIM) with time-bound eligibility
Explanation: PIM enforces Just-In-Time role activation and audits each activation, supporting MFA and justification

Q36. (Multiple Choice) Select TWO

To align with CIS benchmarks, you must enforce resource tagging and deny creation of unencrypted storage. Which two governance features should you use?

A) Azure Policy Definitions with deny effect
B) Management Groups for scope assignment
C) Blueprints (deprecated) for legacy governance
D) Defender for Cloud Recommendations only
E) Resource Locks

Answer: A) Azure Policy Definitions with deny effect, B) Management Groups for scope assignment
Explanation: Policies apply governance rules while Management Groups propagate those policies consistently across subscriptions

Q37. (Hotspot)

Defender for Cloud and Azure Policy relationship:

Statement	Yes / No
Defender for Cloud uses Azure Policy for compliance evaluation	
Defender for Cloud can enforce configuration changes directly without Policy	
Secure Score derives from Policy compliance results	

Answer: Yes, No, Yes
Explanation: Defender for Cloud relies on Azure Policy for evaluations and uses results to calculate Secure Score and recommendations

Q38. (Multiple Choice) Select TWO

A SOC analyst wants to detect impossible travel sign-ins and TOR logins using Entra ID signals. Which two services provide this capability?

A) Identity Protection (risk sign-in policies)
B) Conditional Access sign-in risk controls
C) Microsoft Sentinel KQL queries only
D) Defender for Key Vault
E) Azure Policy Audit rules

Answer: A) Identity Protection (risk sign-in policies), B) Conditional Access sign-in risk controls
Explanation: Identity Protection detects sign-in anomalies such as impossible travel, and Conditional Access can react to those risk levels

Q39. (Scenario)

Your organization wants a single pane of glass showing Secure Score, Defender alerts, and Sentinel incidents. What should you build?

A) Azure Dashboard
B) Microsoft Sentinel Workbook connected to Defender for Cloud
C) Azure Monitor metric alert panel
D) Application Insights overview
E) Network Watcher Topology

Answer: B) Microsoft Sentinel Workbook connected to Defender for Cloud
Explanation: Sentinel Workbooks visualize data from multiple sources including Defender for Cloud and Secure Score, enabling custom SOC dashboards

Q40. (Multiple Choice) Select TWO

To automate incident response and remediation in Azure, which two tools work together?

A) Microsoft Sentinel Playbooks (Logic Apps)
B) Azure Policy Initiatives
C) Defender for Cloud Workflow Automations
D) Azure Firewall Threat Intelligence
E) Resource Graph queries

Answer: A) Microsoft Sentinel Playbooks (Logic Apps), C) Defender for Cloud Workflow Automations
Explanation: Sentinel Playbooks execute SOAR actions; Defender for Cloud Workflow Automations trigger Logic Apps on security alerts for end-to-end remediation flows

Q41. (Scenario)

After a ransomware incident, your SOC must analyze how many alerts were ignored due to misconfigured severity filters. Which Azure service provides this historical alert data?

A) Microsoft Sentinel
B) Azure Monitor Metrics
C) Log Analytics Workspace
D) Azure Policy
E) Microsoft Purview

Answer: A) Microsoft Sentinel
Explanation: Sentinel retains all alert and incident history for review, allowing investigation of SOC workflows and misclassification of severity levels

Q42. (Multiple Choice) Select TWO

You want Sentinel to detect insider data theft attempts from Storage Accounts and immediately revoke user tokens. Which two configurations achieve this?

A) Defender for Storage alerts
B) Sentinel Analytics Rule ingesting Storage logs
C) Logic App Playbook disabling user accounts
D) Azure Monitor Metric Alerts
E) Resource Locks on the storage container

Answer: B) Sentinel Analytics Rule ingesting Storage logs, C) Logic App Playbook disabling user accounts
Explanation: Sentinel analyzes Storage logs for anomalies and triggers Playbooks for automated token revocation via Entra ID API calls

Q43. (Hotspot)

Review Sentinel automation statements.

Statement	Yes / No
Playbooks can be manually run on an incident	
Analytics Rules use KQL queries for detections	
Workbooks automatically remediate alerts	

Answer: Yes, Yes, No
Explanation: Playbooks can run manually or automatically; Analytics Rules use KQL; Workbooks visualize data but don’t perform remediation

Q44. (Multiple Choice) Select TWO

You must standardize incident handling across teams and ensure each alert follows a consistent process for containment and recovery. Which two approaches support this?

A) Define Sentinel Playbooks per alert type
B) Document IR Runbooks for SOC operators
C) Enable Azure Policy Initiatives for IR
D) Use Management Groups for incident routing
E) Store Key Vault logs in Storage Account

Answer: A) Define Sentinel Playbooks per alert type, B) Document IR Runbooks for SOC operators
Explanation: Playbooks automate SOAR response; Runbooks define manual and automated response procedures, ensuring standardized incident lifecycle handling

Q45. (Drag & Drop)

Match each IR phase with its goal.

Phase	Goal
Preparation	A. Develop policies, train teams, and configure playbooks
Detection	B. Identify threats via alerts and SIEM rules
Containment	C. Isolate affected resources and block access
Eradication	D. Remove threats and malware artifacts
Recovery	E. Restore systems and re-enable access

Correct Mapping: 1-A 2-B 3-C 4-D 5-E
Explanation: These follow Microsoft's standard IR lifecycle for SOC operations in Defender and Sentinel

Q46. (Scenario)

After containment of a malware outbreak, the SOC team must document findings and update detection rules to prevent recurrence. Which IR phase is this?

A) Preparation
B) Lessons Learned
C) Recovery
D) Eradication
E) Post-Analysis

Answer: B) Lessons Learned
Explanation: The Lessons Learned phase finalizes the incident response cycle by improving detections and policies for future resilience

Q47. (Multiple Choice) Select TWO

The governance team wants to classify and audit sensitive data across Azure and Microsoft 365. Which two tools provide these capabilities?

A) Microsoft Purview Information Protection
B) Azure Policy Compliance Reports
C) Azure Blueprints (legacy)
D) Defender for Cloud Secure Score
E) Microsoft Purview Data Map and Catalog

Answer: A) Microsoft Purview Information Protection, E) Microsoft Purview Data Map and Catalog
Explanation: Purview delivers data classification and lineage visibility across cloud and on-prem sources

Q48. (Hotspot)

Governance best practices — select Yes or No for each.

Statement	Yes / No
Review Secure Score regularly to track improvements	
Assign Global Admin rights to SOC analysts for faster response	
Enable Diagnostic Logs on critical resources	

Answer: Yes, No, Yes
Explanation: Security teams should review Secure Score, never give Global Admin to SOC analysts, and enable diagnostic logging for visibility

Q49. (Multiple Choice) Select TWO

Which two actions help ensure continuous security improvement in Azure?

A) Automate remediation via Logic Apps and Policy remediation tasks
B) Manually track incidents in Excel only
C) Conduct quarterly Access Reviews for privileged users
D) Disable Defender for Cloud to reduce noise
E) Ignore Low severity alerts

Answer: A) Automate remediation via Logic Apps and Policy remediation tasks, C) Conduct quarterly Access Reviews for privileged users
Explanation: Automation and regular reviews are key to governance and compliance in Azure security operations

Q50. (Scenario)

Your CISO requires monthly proof that critical resources meet Azure Security Benchmark controls and that non-compliance is auto-remediated. What combination achieves this?

A) Defender for Cloud Regulatory Compliance Dashboard + Policy Remediation Tasks
B) Azure Monitor Metrics + Alerts
C) Microsoft Purview Sensitivity Labels + Secure Score
D) Resource Locks + Manual audits
E) Azure Blueprints only

Answer: A) Defender for Cloud Regulatory Compliance Dashboard + Policy Remediation Tasks
Explanation: Defender for Cloud monitors benchmarks like CIS and ASB, while Policy Remediation Tasks enforce and auto-fix non-compliance issues