Cyber Shujaa

Cloud Security Specialist

Assignment 19 -AZ-500 Learning Path: Cloud Governance

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Assignment 19 -AZ-500 Learning Path: Cloud Governance **0**
Introduction **2**
Microsoft cloud security benchmark: Access, Data, Identity, Network, Endpoint, Governance, Recovery, Incident, and Vulnerability Management. 2
Azure governance 4
Create, assign, and interpret security policies and initiatives in Azure Policy. 5
Azure Blueprints 5
Configure security settings by using Azure Blueprint 6
Deploy secure infrastructures by using a landing zone 6
Azure Key Vault 7
Azure Key Vault Security 7
Azure Key Vault authentication 7
Conclusion **8**

Introduction

This module equips us with the knowledge and skills to effectively plan, implement, and manage security governance in Azure, ensuring compliance with organizational policies and best practices.

Microsoft cloud security benchmark: Access, Data, Identity, Network, Endpoint, Governance, Recovery, Incident, and Vulnerability Management.

The Microsoft Cloud Security Benchmark (MCSB) is a comprehensive framework that provides prescriptive best practices and security recommendations for hardening cloud environments. It aligns with industry standards (e.g., NIST, CIS, ISO) and covers nine critical security domains:

Access Control
Principle: Enforce least-privilege access.
Key Controls:

- Microsoft Entra ID Conditional Access: Require MFA, device compliance, and risk-based sign-ins.
- Role-Based Access Control (RBAC): Limit permissions using predefined roles (e.g., Reader, Contributor).
- Privileged Identity Management (PIM): Just-in-time (JIT) elevation for admin roles.

Tools: Microsoft Entra ID, Azure PIM.

Data Protection
Principle: Encrypt data at rest and in transit.
Key Controls:

- Azure Storage Service Encryption (SSE): Auto-encryption for Blob, Files, etc.
- Azure Key Vault: Centralized management of encryption keys.
- Data Loss Prevention (DLP): Policies to prevent sensitive data leaks (e.g., credit card numbers).

Tools: Azure Key Vault, Microsoft Purview, Azure Information Protection.

Identity Security
Principle: Secure authentication and authorization.
Key Controls:

- Multi-Factor Authentication (MFA): Mandatory for all users.
- Passwordless Authentication: FIDO2 keys or Windows Hello.
- Identity Governance: Regular access reviews (e.g., MS Entra ID Access Reviews).

Tools: Microsoft Entra ID, Defender for Identity.

Network Security
Principle: Segment and monitor network traffic.
Key Controls:

- Zero Trust Architecture: Micro-segmentation, deny-by-default.
- Azure Firewall & NSGs: Filter inbound/outbound traffic.
- DDoS Protection: Mitigate volumetric attacks.

Tools: Azure Firewall, Azure DDoS Protection, Microsoft Defender for Cloud.

Endpoint Security
Principle: Secure devices accessing cloud resources.
Key Controls:

- Microsoft Defender for Endpoint: EDR/XDR for threat detection.
- Device Compliance Policies: Enforce encryption and OS updates.
- Mobile Device Management (MDM): Intune for BYOD/CYOD.

Tool: Microsoft Intune, Defender for Endpoint.

Governance & Compliance
Principle: Continuous policy enforcement.
Key Controls:

- Azure Policy: Enforce rules (e.g., "No public blob storage").
- Microsoft Defender for Cloud: Regulatory compliance dashboards.
- Cloud Security Posture Management (CSPM): Detect misconfigurations.

Tools: Azure Policy, Defender for Cloud.

Recovery & Business Continuity
Principle: Ensure resilience against outages/attacks.
Key Controls:

- Backup & Disaster Recovery: Azure Backup, Site Recovery.
- Geo-Redundancy: Paired regions for failover.
- Ransomware Protection: Immutable backups.

Tools: Azure Backup, Azure Site Recovery.

Incident Response
Principle: Detect, respond, and recover from breaches.
Key Controls:

- Microsoft Sentinel: SIEM for threat detection.
- Automated Playbooks: Respond to alerts (e.g., quarantine compromised devices).
- Forensic Investigation: Log retention (Azure Monitor Logs).

Tools: Microsoft Sentinel, Defender XDR.

Vulnerability Management
Principle: Proactively patch and assess risks.
Key Controls:

- Microsoft Defender Vulnerability Management: Prioritize CVEs.
- Patch Management: Automatic updates via Intune/Update Manager.
- Container Security: Scan images in ACR.

Tools: Defender Vulnerability Management, Azure Update Manager.

Azure governance

Governance in Azure is one aspect of Azure Management. This unit covers the different areas of management for deploying and maintaining our resources in Azure.

Monitor
Monitoring is collecting and analyzing data to audit the performance, health, and availability of our resources. An effective monitoring strategy helps us understand the operation of components and increase our uptime with notifications.

Configure
Configure refers to the initial deployment and configuration of resources and ongoing maintenance. Automation of these tasks allows us to eliminate redundancy, minimize our time and effort, and increase our accuracy and efficiency.

Govern
Governance provides mechanisms and processes to maintain control over our applications and resources in Azure. It involves planning our initiatives and setting strategic priorities. Governance in Azure is primarily implemented with two services: Azure Policy and Azure Cost Management.

Secure
Manage the security of our resources and data. A security program involves assessing threats, collecting and analyzing data, and compliance of your applications and resources. Security monitoring and threat analysis are provided by Microsoft Defender for Cloud, which includes unified security management and advanced threat protection across hybrid cloud workloads.

Protect
Protection refers to keeping your applications and data available, even with outages that are beyond our control. Protection in Azure is provided by two services: Azure Backup provides backup and recovery of our data, either in the cloud or on-premises. Azure Site Recovery provides business continuity and immediate recovery during a disaster.

Migrate
Migration refers to transitioning workloads currently running on-premises to the Azure cloud. Azure Migrate is a service that helps us assess the migration suitability of on-premises virtual machines to Azure. Azure Site Recovery migrates virtual machines from on-premises or from Amazon Web Services. Azure Database Migration Service assists us in migrating database sources to Azure Data platforms.

Create, assign, and interpret security policies and initiatives in Azure Policy.

Azure Policy allows organizations to enforce governance and compliance across Azure resources.
Azure Initiatives are collections of multiple Azure Policy definitions grouped to achieve a broader compliance goal.
Security Policies in Azure Policy focus on enforcing security-related configurations, such as access control, encryption, and network security.

We use Azure Initiatives when managing multiple related policies together, such as PCI-DSS compliance or ISO 27001 security standards. On the other hand, we use Security Policies when enforcing specific security rules, like restricting public IPs, requiring encryption, or enforcing MFA.

Azure Blueprints

Azure Blueprints is a service that enables organizations to define a repeatable set of governance resources, policies, and ARM templates to standardize cloud environments. It packages together Azure Policy assignments, role-based access controls (RBAC), Resource Manager templates (ARM templates), and resource groups into a single blueprint, ensuring consistent deployment of compliant infrastructure. Blueprints help enforce organizational standards, such as security baselines, naming conventions, and compliance requirements, by automatically applying these configurations when new subscriptions or environments are created.

Unlike Azure Policy, which focuses on enforcing rules individually, Azure Blueprints provides a holistic approach by orchestrating multiple governance components into a unified deployment model. Blueprints are versioned, allowing updates to be tracked and rolled out systematically. Common use cases include creating landing zones for new projects, enforcing regulatory standards (like ISO 27001), or setting up development/test environments with pre-approved configurations.

Configure security settings by using Azure Blueprint

To configure security settings using Azure Blueprint, administrators should first define their compliance requirements and security standards that align with organizational policies. This involves creating a blueprint that includes various components such as policies, role assignments, and resource groups. Once the blueprint is created, it can be assigned to specific Azure subscriptions, ensuring that all resources deployed within those subscriptions adhere to the defined security settings.

The process begins by identifying the necessary security policies that need to be enforced. Administrators can then create a blueprint that encapsulates these policies along with any required role assignments and resource configurations. After the blueprint is prepared, it can be published and assigned to the relevant Azure environments, ensuring that all resources comply with the established security guidelines and compliance requirements.

Deploy secure infrastructures by using a landing zone

Azure Landing Zones provide a scalable, secure foundation for cloud workloads by implementing best practices in governance, security, and compliance. Landing zones are preconfigured environments that align with the Cloud Adoption Framework (CAF) and ensure consistency across subscriptions. Key components include:

- Identity & access management (Azure AD, RBAC, Conditional Access)
- Network security (hub-spoke architecture, Azure Firewall, NSGs)
- Policy enforcement (Azure Policy for compliance)
- Monitoring & logging (Azure Monitor, Microsoft Sentinel)

An Azure landing zone consists of platform landing zones and application landing zones.

Platform landing zone: A platform landing zone is a subscription that provides shared services (identity, connectivity, management) to applications in application landing zones. Consolidating these shared services often improves operational efficiency. One or more central teams manage the platform landing zones.

Application landing zone: An application landing zone is a subscription for hosting an application. You pre-provision application landing zones through code and use management groups to assign policy controls to them.

Azure Key Vault

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to control access to tightly, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed hardware security module (HSM) pools. Vaults support storing software and HSM-backed keys, secrets, and certificates. Managed HSM pools only support HSM-backed keys.

Azure Key Vault Security

Azure Key Vault provides centralized management of cryptographic keys and secrets, ensuring secure access and compliance. Key features include role-based access control (RBAC) to restrict permissions, soft delete and purge protection to prevent accidental data loss, and firewall integration to limit access to trusted networks. This unit emphasizes audit logging via Azure Monitor, enabling tracking of all vault operations for security and compliance reviews.

Additionally, the module covers best practices such as rotating keys regularly, using private endpoints for secure connectivity, and enabling Microsoft Defender for Key Vault to detect suspicious activities.

Azure Key Vault authentication

Microsoft Entra ID handles authentication for Key Vault, using security principals to manage access. These security principles include:

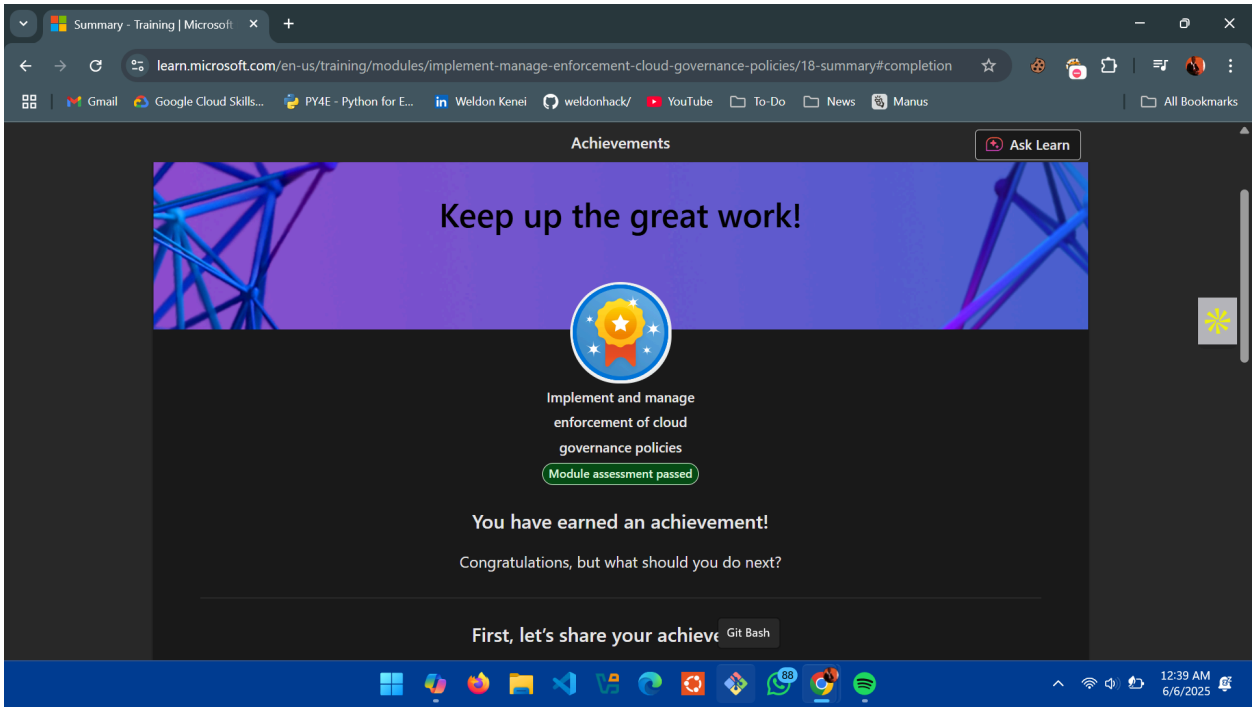
- Users (individuals with Entra ID profiles),
- Groups (collections of users with shared permissions), and
- Service Principals (representing applications or services).

Azure assigns each security principal a unique object ID for identification. Service principals use an object ID (like a username) and a client secret (like a password) for authentication.

For applications, managed identities are recommended—they allow Azure to internally manage authentication without manual credential handling. If managed identity isn’t possible, the application must be registered with Entra ID, creating an associated application object across tenants.

Conclusion

To conclude, this module has equiped us with the knowledge and expertise necessary to implement and manage security governance in Azure effectively, align with organizational policies, proactively identify and remediate multicloud security risks, maintain compliance using tools like Azure Policy and Azure Blueprint, protect against external threats with Microsoft Defender for Cloud, and ensure cloud resilience through assessments, key management, and advanced threat protection.



https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/NVKSYJHF?sharingId=1C66F93EC0530812