SC-300T00 Microsoft Identity and Access Administrator

1. **Introduction to Identity and Access Management (IAM):**

1.1 Understanding the importance of IAM in modern IT environments.

1.2 Overview of Azure Active Directory (Azure AD) and its role in IAM.

1. **Managing Azure Active Directory (Azure AD):**

2.1Creating and managing user accounts.

2.2 Configuring and customizing security policies.

2.3 Implementing identity synchronization between on premises and Azure AD.

3.**Implementing and Managing Identity Services:**

3.1 Implementing and managing Azure Multi-Factor Authentication (MFA).

3.2 Configuring self-service password reset (SSPR).

3.3 Managing identity governance and lifecycle.

4. Implementing and Managing Access Services:

4.1 Configuring role-based access control (RBAC).

4.2 Implementing Azure AD Privileged Identity Management (PIM).

4.3 Managing access to Azure resources.

5.Implementing Identity Federation and Single Sign-On (SSO):

5.1 Configuring federated identity with Azure AD.

5.2 Implementing and managing SSO for cloud and on premises applications.

6. Monitoring and Auditing Identity and Access:

6.1 Setting up identity and access monitoring.

6.2 Reviewing and analysing audit logs.

6.3 Responding to security incidents related to identity and access.

7. Implementing Conditional Access Policies:

7.1 Configuring conditional access policies for secure access control.

7.2 Enforcing compliance and security policies using conditional access.

8. Implementing Identity Protection and Threat Detection:

8.1 Configuring Azure AD Identity Protection.

8.2 Detecting and responding to identity-related security threats.

9. Identity and Access Management Best Practices:

9.1 Best practices for securing identities and access in Microsoft 365 and Azure.

10. Hands-on Labs and Practical Scenarios:

10.1 Practical exercises and labs to reinforce concepts and skills learned.