Azure Identity and Security Workshop Training

Duration: **1 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Azure Identity and Security Workshop is a **one-day immersive, hands-on programme** designed to introduce participants to key identity, access and security capabilities available within Microsoft Azure.

Rather than focusing solely on security concepts, the workshop gives learners practical exposure to how important Azure security features can be implemented and used within a cloud environment.

The programme covers key areas ranging from user identity creation and privileged access management to Multi-Factor Authentication and Role-Based Access Control. Participants also explore features such as Azure Policies and Conditional Access, developing a broader understanding of how identity and access controls can be combined to strengthen an Azure environment.

Prerequisites

Participants should have a **fundamental understanding of Microsoft Azure** before attending. This knowledge may be gained through Azure Fundamentals training or equivalent practical experience.

MFA Requirement

The workshop requires the use of **Multi-Factor Authentication (MFA)**. Participants should therefore ensure that the required MFA application is installed on their mobile device and ready to use before attending the course.

Who Should Attend

This workshop is suitable for individuals who want to:

- Develop an understanding of Microsoft Azure identity and security features
- Learn how access can be managed within Azure environments
- Gain practical exposure to Azure security controls
- Build foundational knowledge of identity security for cloud and IT operations

Azure Identity and Security Workshop Training

Duration: **1 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of the workshop, participants will be able to:

- Understand how user identities and accounts are created within Azure
- Recognise how Privileged Identity Management can support the control of privileged access
- Understand how Multi-Factor Authentication strengthens account security
- Explain the purpose of Self-Service Password Reset
- Understand how RBAC controls access to Azure resources through roles
- Recognise how Azure Policies can be used to apply organisational rules to resources
- Understand how Conditional Access supports condition-based access decisions
- Develop a broader understanding of how Azure identity and security capabilities can work together to create a more controlled access model

Training Outline

1. User Identity and Account Creation

Explore the user and account management processes that form the foundation of identity management in Azure.

- Creating user identities
- Managing user accounts
- The role of identities in accessing Azure resources
- Fundamental account management concepts

2. Privileged Identity Management (PIM)

Examine how PIM can help organisations manage access associated with privileged roles.

- Understanding privileged access
- Managing privileged roles
- Controlling elevated access
- The role of PIM within Azure security

3. Multi-Factor Authentication (MFA)

Explore how additional authentication factors can strengthen user account security beyond passwords alone.

- Understanding MFA
- The purpose of multiple authentication factors
- Applying MFA to user access
- Strengthening identity security

4. Self-Service Password Reset

Review the capabilities that allow users to handle password reset activities more independently.

- Self-Service Password Reset concepts

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- User password reset processes
- Its role within identity management

5. Role-Based Access Control (RBAC)

Learn how access to Azure resources can be managed according to assigned roles.

- Core RBAC concepts
- Role-based access management
- User and resource authorisation
- Creating controlled access to Azure resources

6. Azure Policies

Explore how Azure Policies can support consistent resource management through defined rules.

- The purpose of policy-based management
- Applying rules to Azure resources
- Supporting organisational standards
- Maintaining greater control over cloud resources

7. Conditional Access

Examine how access decisions can be controlled according to defined conditions.

- Conditional Access concepts
- Condition-based access management
- Combining identity and access controls
- Strengthening access security within Azure environments

Hands-On Learning

This programme is delivered as an **interactive workshop rather than a theory-only course**. Throughout the one-day session, participants explore key Azure identity and security capabilities and gain practical exposure to their implementation.

The workshop focuses on helping learners understand the fundamental tools available for making user access within Azure more secure, controlled and manageable.