Identity and Access Management (IAM) Project

Active Directory (On-Premises) Deployment For

CyberTech Solutions

Implementation of On-Premises Active Directory for Centralized Identity and Access Management

Organisation: Cybertech

Date: 25 September 2025

Prepared By: Biliaminu B. Salawu (Cybersecurity Analyst)

1. Project Overview

This project focused on deploying an **on-premises Active Directory Domain Controller** to provide centralized **Identity and Access Management (IAM)** for CyberTech Solutions.
The implementation included domain setup, client integration, creation of Organizational Units (OUs) aligned to regional offices, security group design, user provisioning, and enforcement of access control policies using Group Policy Objects (GPOs).

2. Company IT Structure

The simulated environment reflected a small IT services firm with distributed offices:

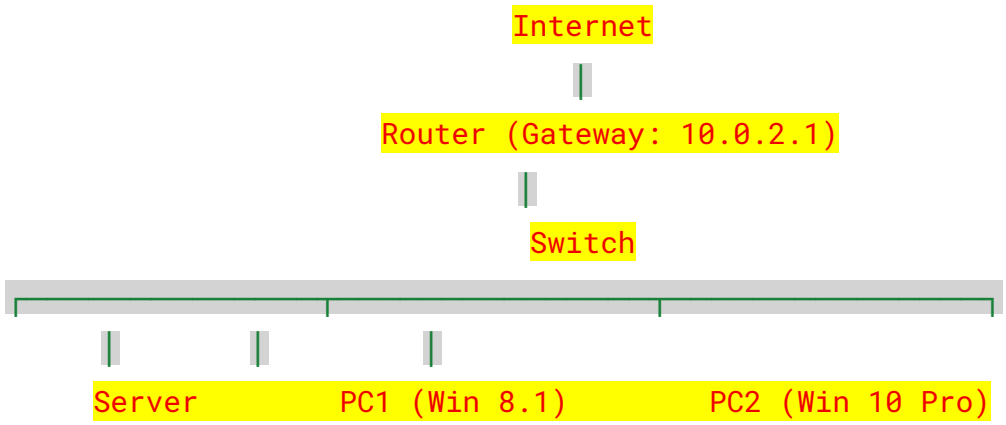
- **1 x Windows Server** – Domain Controller (AD DS + DNS)
- **2 x Client PCs** – Windows 8.1 and Windows 10

- **Three regional OUs** – UK, US, and ABUJA
- **Departmental Groups** – Created within each OU to represent business functions

3. Project Objectives

- Deploy **Active Directory Domain Services (AD DS)** for centralized IAM.
- Configure regional **Organizational Units (OUs)** to mirror company structure.
- Provision **security groups** to manage access by department.
- Create **user accounts** and assign them to relevant groups.
- Apply **Group Policies** to enforce access restrictions.
- Demonstrate IAM governance in an on-premises enterprise setup.

4. Network Design



Device	IP Address	Role
Windows Server	10.0.2.4	AD Domain Controller (DC)
Windows 8.1	DHCP	Client (ABUJA OU – Finance)
Windows 10	DHCP	Client (UK OU – IT)

5. Domain Configuration

- **Domain Name:** `Cybertech.local`

- **Server Name:** `CYBERTECH`
- **Static IP:** `10.0.2.4`
- **Roles Installed:**
    - Active Directory Domain Services (AD DS)
    - DNS Server

6. Organizational Units (OUs) and Groups

The directory structure was created as follows:

```
CyberTech.local
└── Organisational Unit: UK
    ├── Group: IT
    └── Group: Sales

└── Organisational Unit: US
    ├── Group: Procurements
    └── Group: Laboratory

└── Organisational Unit: Abuja
    ├── Group: Finance
    └── Group: Consultation
```

7. Users and Group Memberships

Two test users were provisioned to demonstrate IAM principles:

Username	OUs	Group Membership	Assigned Policy
Bill.IT@cybertech.local	UK OU	IT	**Remove clock from system notification area.**
Biola.finance@cybertech.local	ABUJA	Finance	**Unable to shutdown**

8. Group Policy (GPO) Implementation

Two GPOs were created and linked to specific users through security filtering:

1. **GPO Name:** Remove Calendar Display
    - **Linked To:** UK OU (IT User – Bill)
    - **Policy:**

      User Configuration → Administrative Templates →
    - **Result:** Bill cannot view or enabled Clock and calendar on the assigned PC..

2. **GPO Name:** NoShutdown
3.
    - **Linked To:** ABUJA OU (Finance User – Biola)
    - **Policy:**

      Computer Configuration → Administrative Templates → Start Menu and Taskbar →

      Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands
    - **Result:** Biola cannot shut down the assigned PC.

9. Screenshots (Evidence)

- OU and group structure in ADUC
- GPO editor settings
- User login results showing applied restrictions

(Screenshots stored in project evidence folder)

10. Key Takeaways

- Successfully implemented an **IAM framework** on Active Directory.
- Mapped **business structure (regions and departments)** into OUs and groups.
- Demonstrated **access control enforcement** using Group Policy Objects (GPOs).
- Learned how to provision and manage **users, groups, and security policies**.
- Applied **identity governance principles** in a real-world simulated enterprise environment.