Report: Active Directory Organizational Units (OUs) and Group Policy Implementation

1. Introduction

In an enterprise environment, properly organizing users, computers, and service accounts within Active Directory (AD) is essential for scalable and secure network administration. Organizational Units (OUs) allow administrators to logically separate and manage AD objects based on departmental structure, functional roles, or security requirements. This enhances clarity, simplifies permission delegation, and facilitates the application of Group Policy Objects (GPOs) to specific groups of users or devices.

This report outlines the process of designing and implementing OUs for core departments—Finance, HR, IT—and a dedicated OU for Service Accounts. Users were moved into appropriate OUs based on departmental affiliation, and a targeted GPO was applied to restrict USB storage for Finance. The configuration was verified using command-line tools to ensure correct policy enforcement.

2. Objective

The primary objective of this task was to establish a clean and manageable AD hierarchy by creating OUs that reflect the organizational structure. This enables more effective administration, policy control, and audit readiness across departments. A structured OU model supports better scalability and delegation of administrative rights within larger organizations.

A secondary objective was to implement security measures through Group Policy, such as restricting USB storage for Finance to protect sensitive financial data. The goal was to ensure that each department receives the required policy controls while keeping administrative overhead low and maintaining clear separation of roles and responsibilities.

Key goals include:

- **Design a Logical OU Structure**
  The first goal was to create OUs for different departments—Finance, HR, IT—and for Service Accounts. This logical division simplifies administration, delegation of control, and targeting of policies to specific groups of users. A well-structured OU hierarchy is the foundation for efficient AD management.

- **Organize Users According to Departments**
  Users were moved into their respective OUs based on their roles and departmental assignments. This ensures that policies can be applied selectively and reduces the risk of misconfiguration. It also aligns user account organization with real-world business functions.

- **Apply Department-Specific GPOs**
  A Group Policy Object was applied to the Finance OU to disable USB storage devices. This targeted control helps protect sensitive financial data from unauthorized extraction or malware infections via removable media. Applying GPOs at the OU level enhances security granularity.

- **Verify GPO Application and Inheritance**
  The gpresult /r command was used to verify whether the GPO was successfully applied to users in the Finance OU. This step ensures that the policy is both linked and enforced, confirming the effectiveness of the configuration. It also helps detect any GPO inheritance issues.

- **Improve Security and Administrative Efficiency**
  Overall, the implementation of structured OUs and targeted GPOs improves security by limiting unnecessary privileges and automating control enforcement. It also enhances administrative efficiency by reducing manual configurations and centralizing policy management.

3. Methodology

The methodology defines the structured process used to implement and verify Organizational Units (OUs) and Group Policies (GPOs) in Active Directory. This approach ensures that user accounts are logically organized and department-specific security policies are effectively applied. The tasks were completed using Active Directory Users and Computers (ADUC), Group Policy Management Console (GPMC), and Windows Command Prompt.

The process was divided into phases, with each phase targeting a specific part of the configuration. Each phase includes multiple steps, where PowerShell or GUI tools were used to configure and validate the setup. Screenshots and practical POC explanations are provided to demonstrate execution and outcomes.

3.1 Creating and Structuring Organizational Units

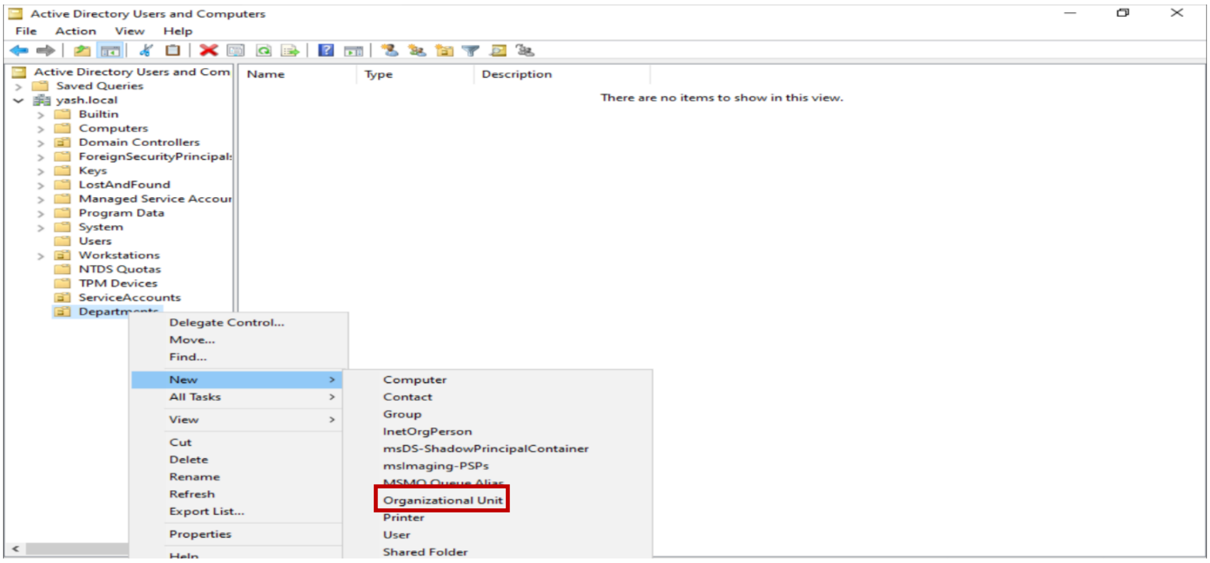
This phase involved designing a departmental OU structure in Active Directory. It lays the groundwork for future GPO applications and administrative delegation. OUs were created for Finance, HR, IT, and ServiceAccounts, providing separation of roles and administrative scope.

- **Create OUs for Departments and Service Accounts**

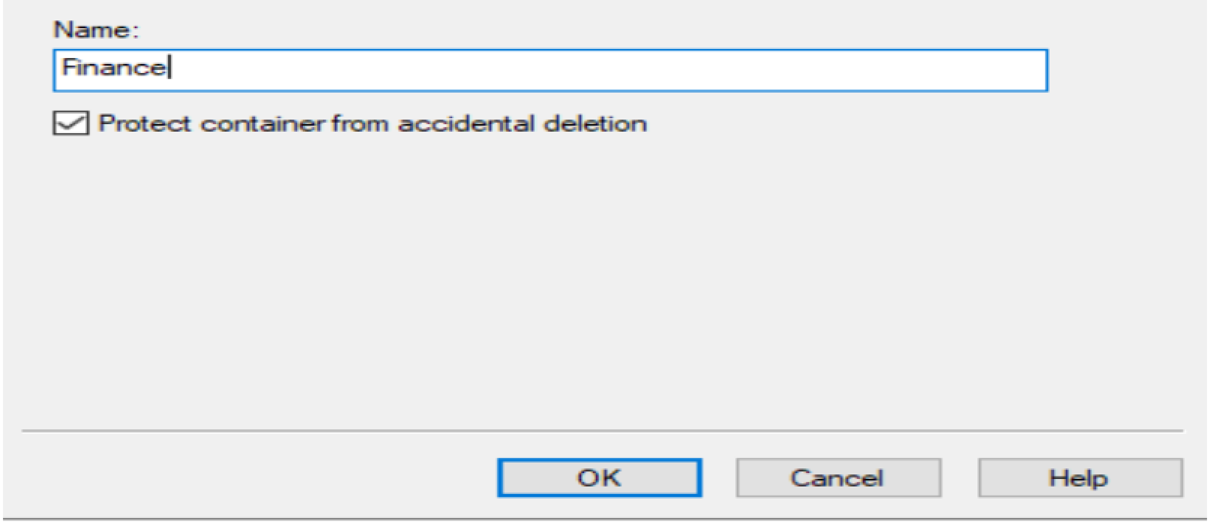
  Using Active Directory Users and Computers, new Organizational Units were created under the domain root. Each OU was named after a department: Finance, HR, IT, and one specifically for Service Accounts. This allowed logical grouping and future GPO targeting for department-specific needs.

  To create the Organizational Units (OUs), the Active Directory Users and Computers (ADUC) console was accessed through Win+R (dsa.msc). Under the domain root (e.g., yash.local), each OU was created by right-clicking the domain, selecting New → Organizational Unit, and naming them according to the department: Finance, HR, IT, and ServiceAccounts. This established a structured foundation for departmental organization and policy targeting.

(Created OUs in Departments OU.)

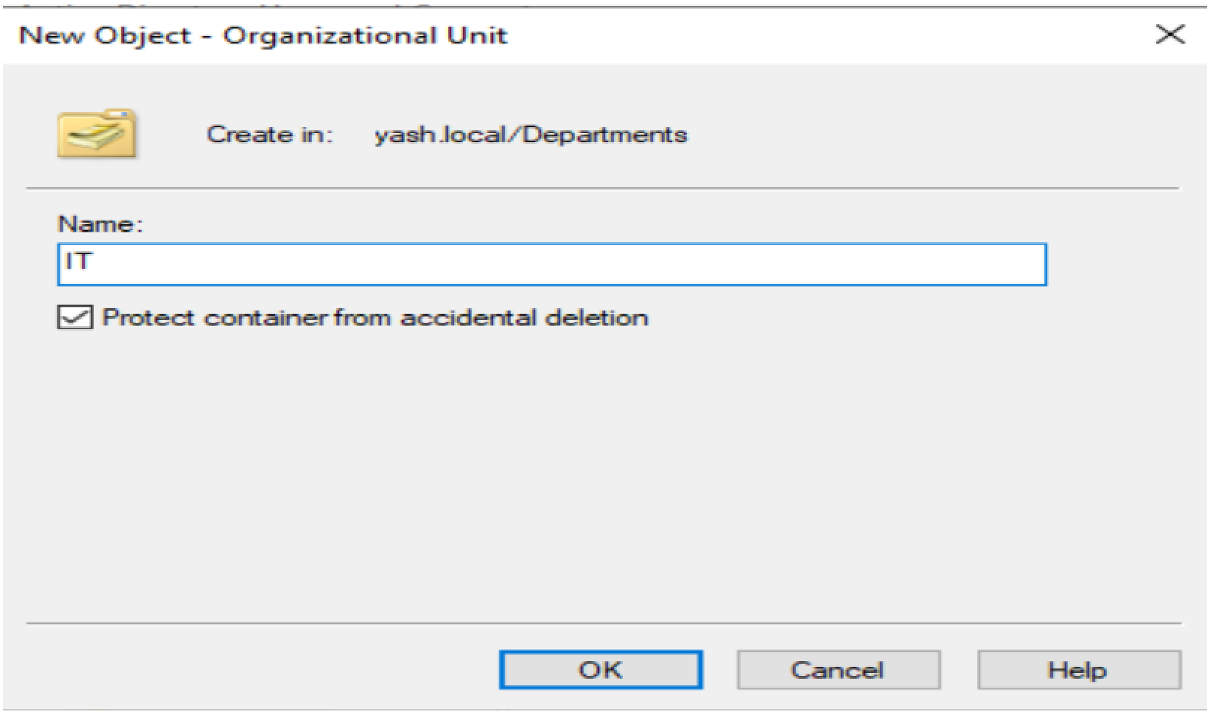


(Created a OU-Finance)


Name: Finance

☑ Protect container from accidental deletion

(Created a OU-IT)



New Object - Organizational Unit

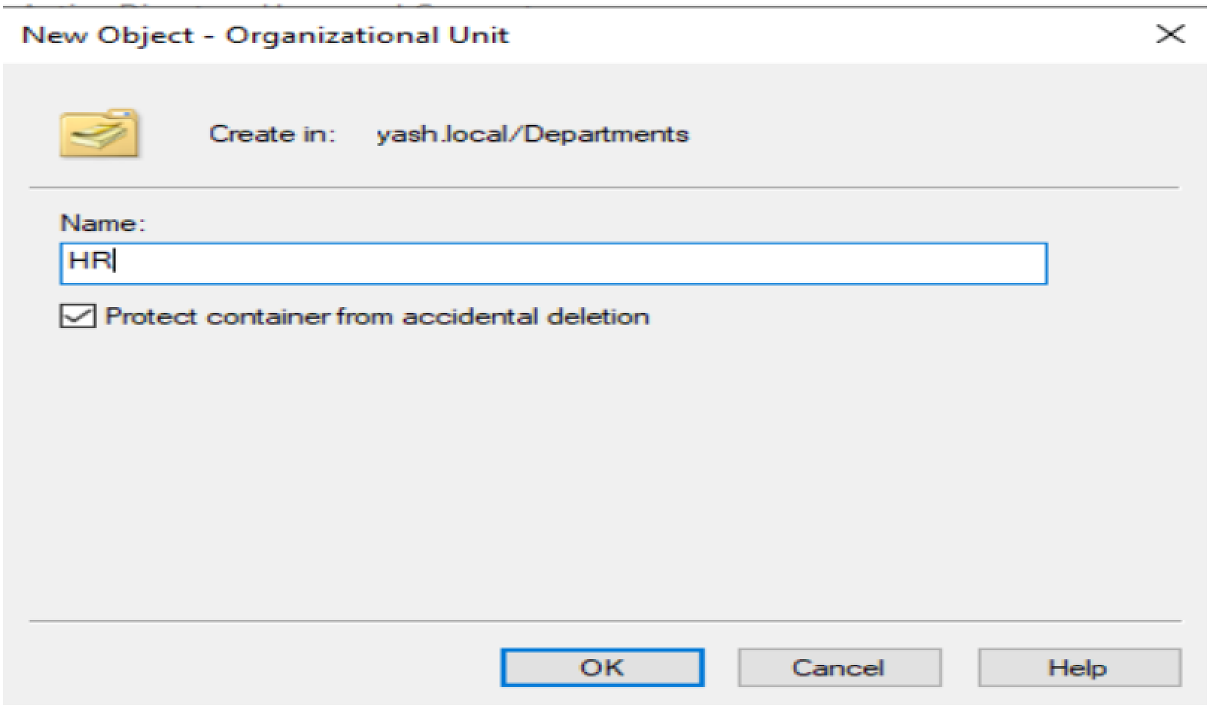
Create in: yash.local/Departments

Name:

IT

☑ Protect container from accidental deletion

(Created a OU-HR)



New Object - Organizational Unit

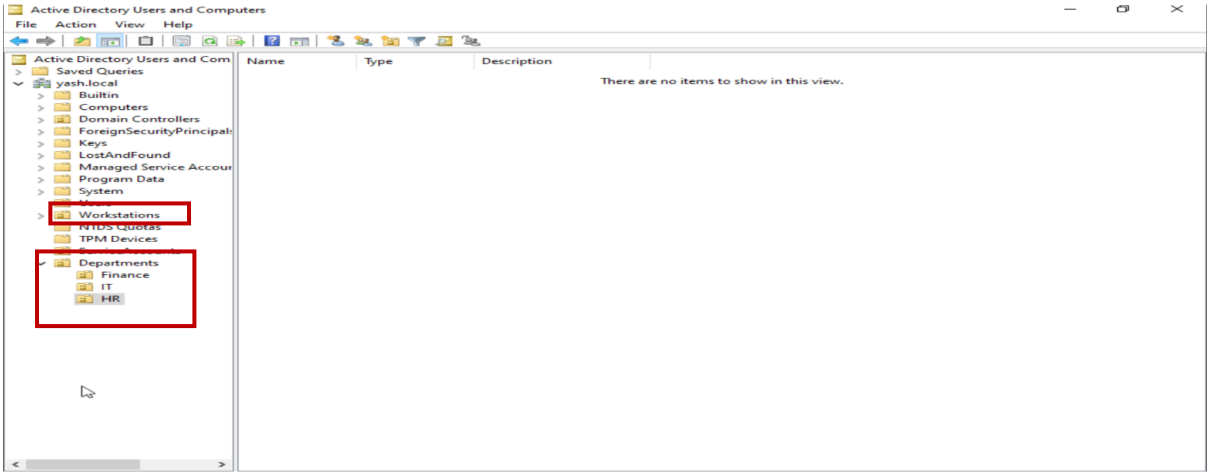
Create in: yash.local/Departments

Name:

HR

☑ Protect container from accidental deletion

(Visual proof of OUs confirms they exist and are ready for user and policy assignment.)



There are no items to show in this view.

3.2 User Organization by Department

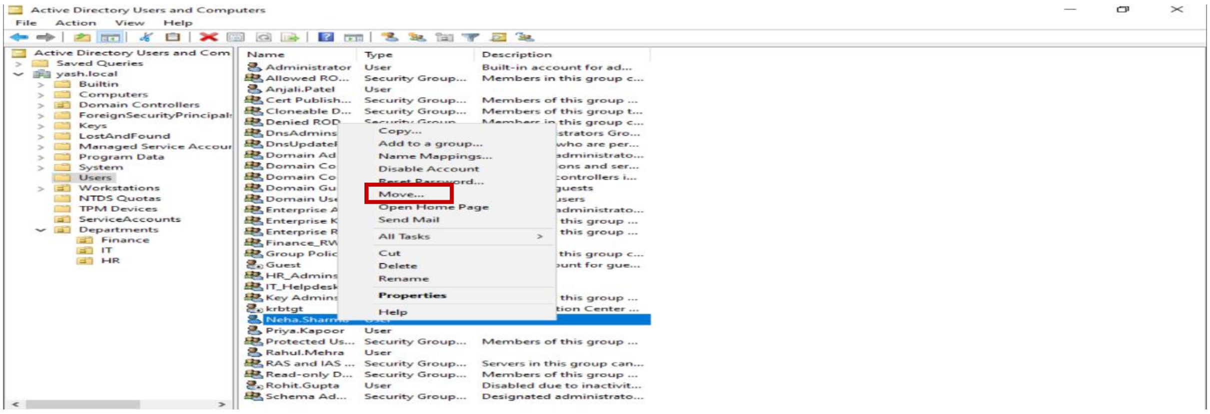
After setting up the OU structure, users were moved into the appropriate departments. This aligns AD structure with the actual organizational chart and ensures department-level policies affect only intended users.

- **Move Users into Appropriate Ous**

  Users were identified and moved into their respective OUs using the ADUC console. For example, finance staff accounts were placed under the Finance OU, ensuring clarity and correct policy inheritance. This ensures that department-specific GPOs apply only to relevant users and groups.

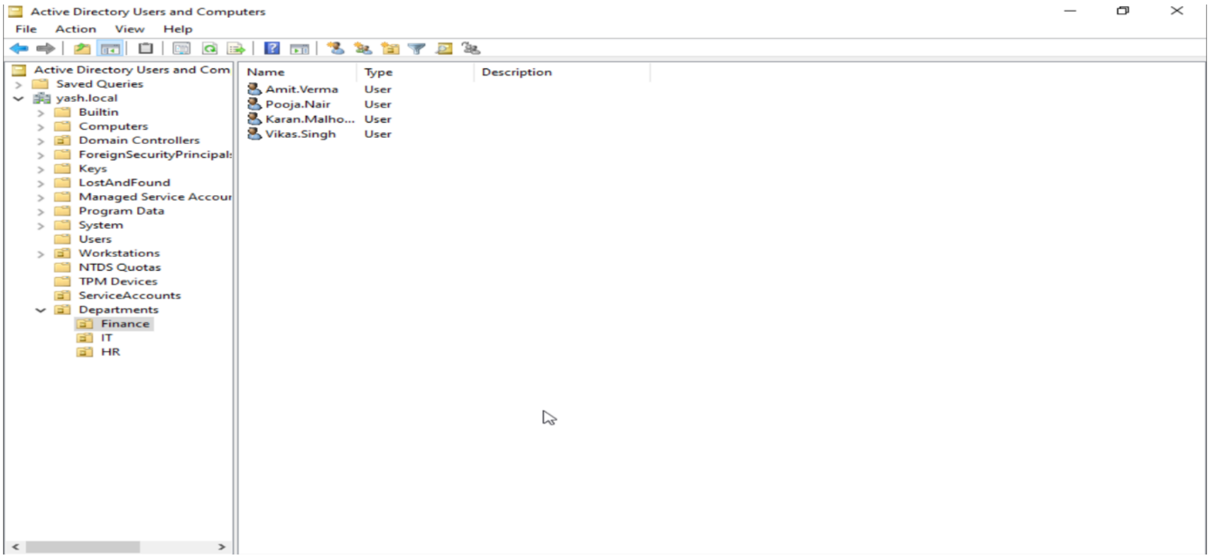
  To add users to group → Open ADUC → Expand domain → Click **Users** container → Right-click on a user → Move → Select target OU → OK

(Adding User Accounts in Departmental Ous.)



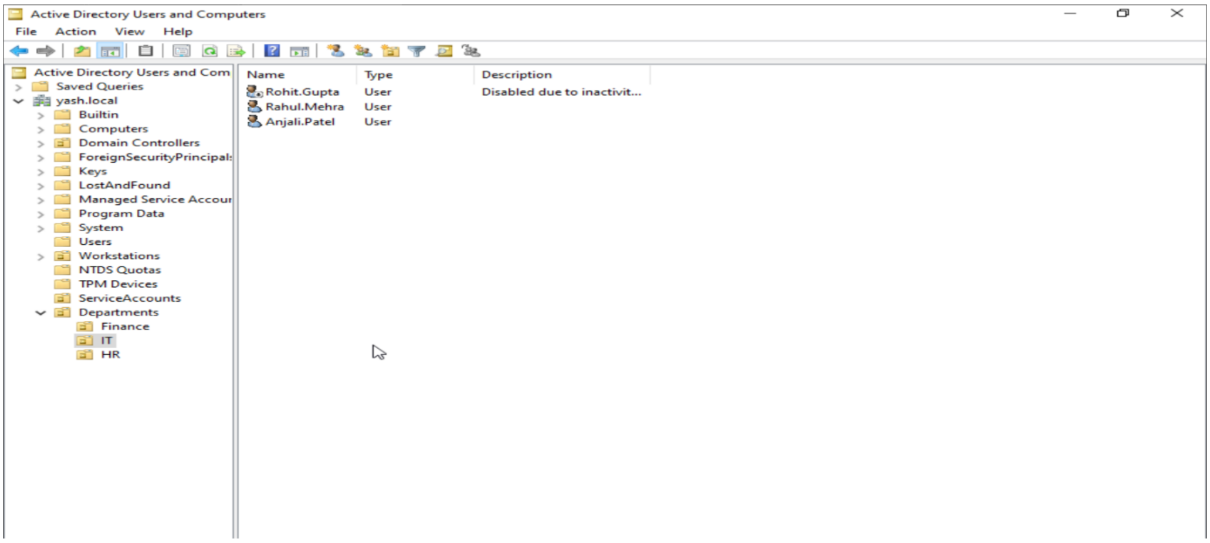
Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Anjali.Patel	User	
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD	Security Group	Members in this group c...
DnsAdmins		strators Gro...
DnsUpdateP		who are per...
Domain Ad		administrato...
Domain Co		ons and ser...
Domain Co		controllers i...
Domain Gu		guests
Domain Use		users
Enterprise A		administrato...
Enterprise K		this group ...
Enterprise R		this group ...
Finance_RW		
Group Polic		this group c...
Guest		ount for gue...
HR_Admins		
IT_Helpdesk		
Key Admins		this group ...
krbtgt		tion Center ...
Neha.Sharma	User	
Priya.Kapoor	User	
Protected Us...	Security Group...	Members of this group ...
Rahul.Mehra	User	
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Rohit.Gupta	User	Disabled due to inactivit...
Schema Ad...	Security Group...	Designated administrato...

(Users moved in Finance OU)



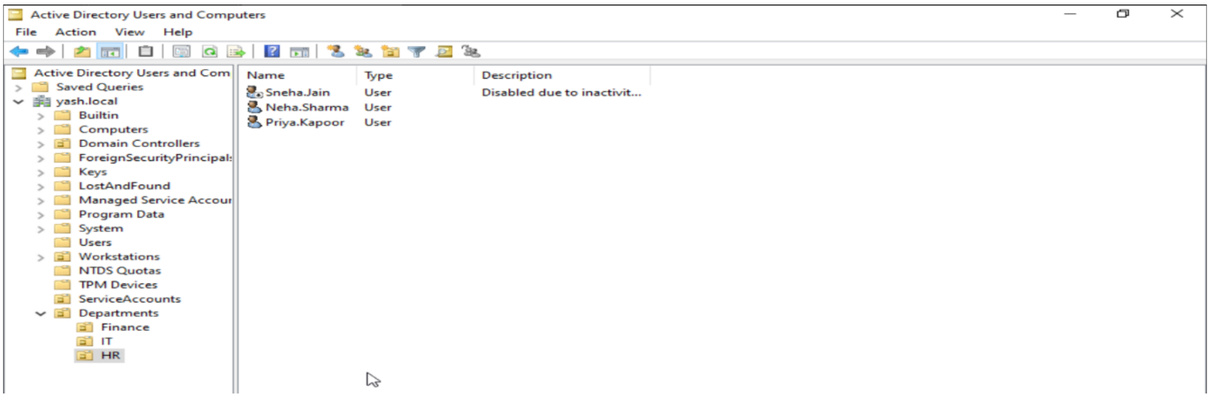
Name	Type	Description
Amit.Verma	User	
Pooja.Nair	User	
Karan.Malho...	User	
Vikas.Singh	User	

(Users moved in IT OU)



Name	Type	Description
Rohit.Gupta	User	Disabled due to inactivit...
Rahul.Mehra	User	
Anjali.Patel	User	

(Users moved in HR OU)



Name	Type	Description
Sneha.Jain	User	Disabled due to inactivit...
Neha.Sharma	User	
Priya.Kapoor	User	

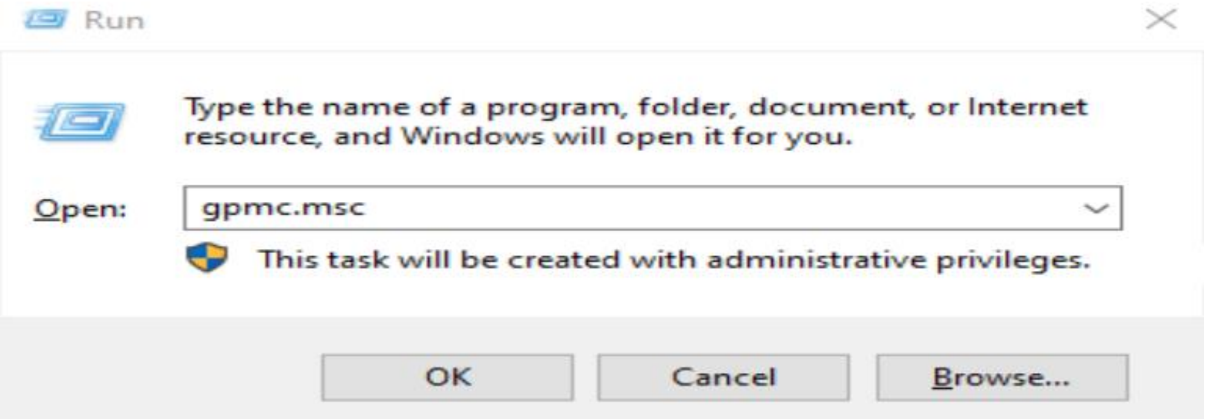
3.3 Apply and Configure GPO

With users placed in OUs, the next step was to apply a department-specific Group Policy. For this task, the Finance department required tighter security by disabling USB storage devices.

- **Apply GPO to Disable USB Storage for Finance OU**

  A new GPO was created using the Group Policy Management Console (GPMC). Under Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access, USB storage was disabled. The GPO was then linked to the Finance OU, restricting USB use on systems within that OU.

(Open Group Policy Management Console)



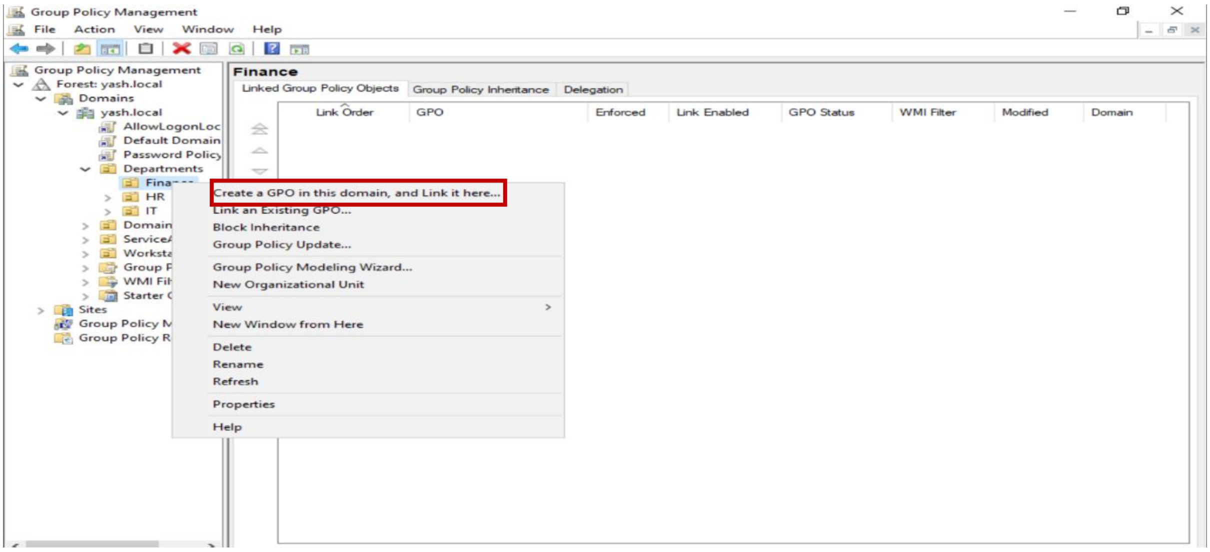
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

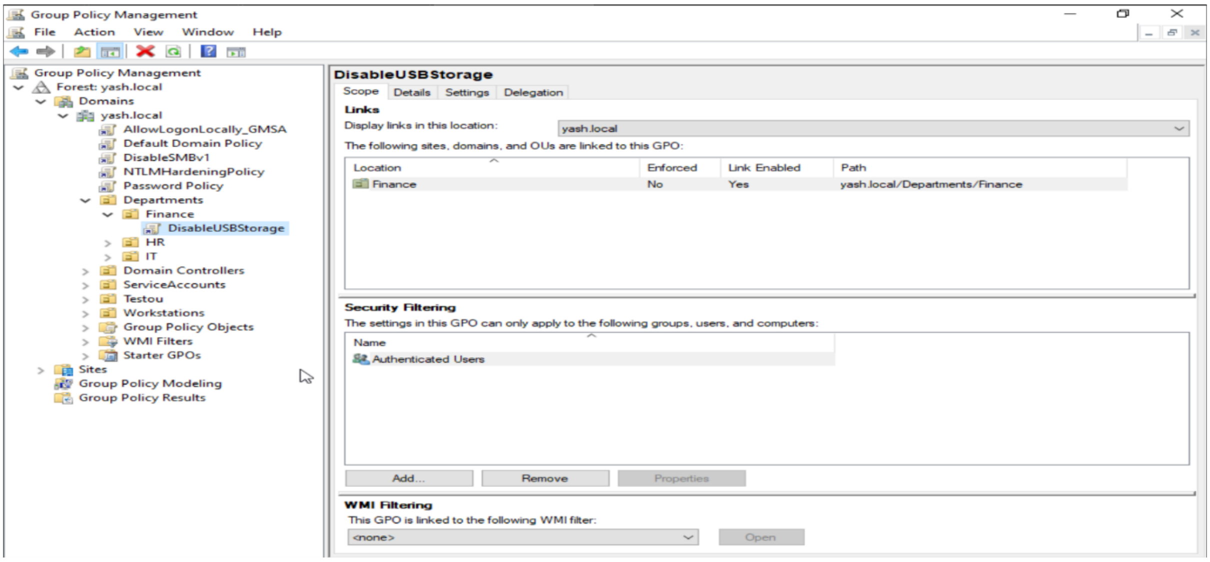
Open: gpmc.msc

This task will be created with administrative privileges.

(Creating a new GPO.)



(Created, named -   DisableUSBStorage.)



DisableUSBStorage

Links

Display links in this location: yash.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Finance	No	Yes	yash.local/Departments/Finance

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

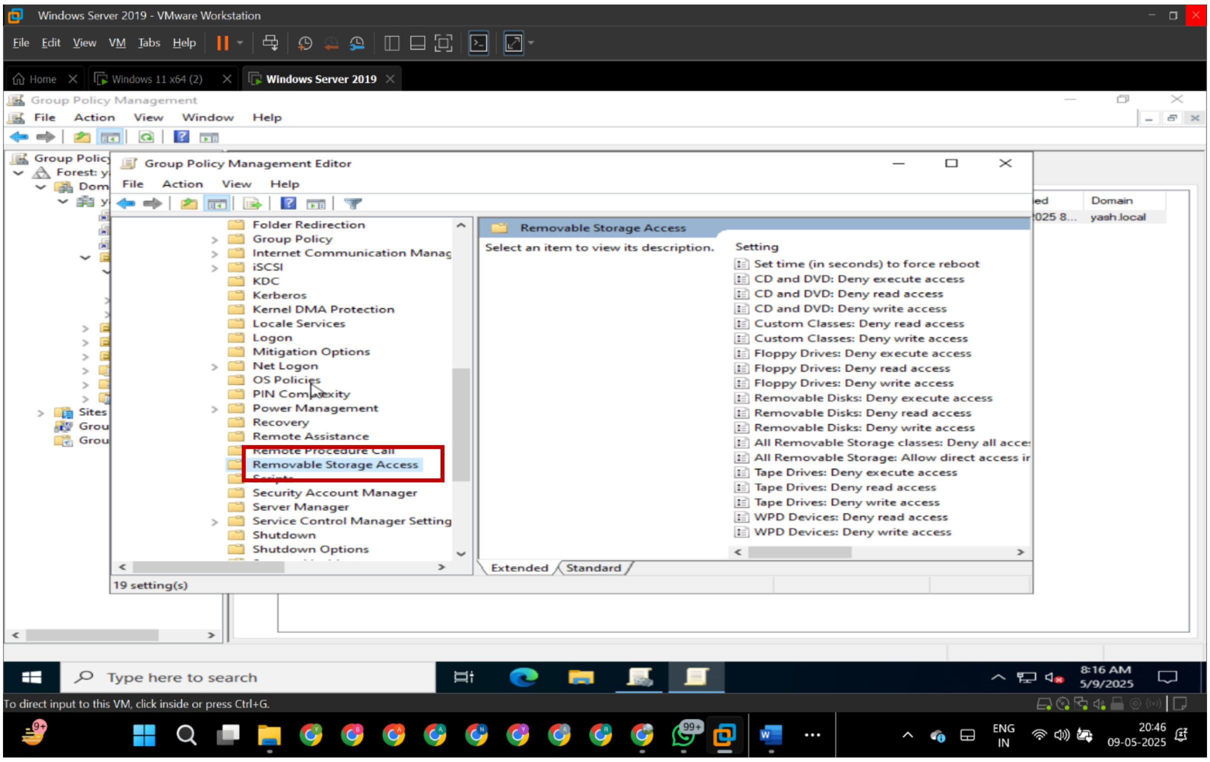
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access



Removable Storage Access

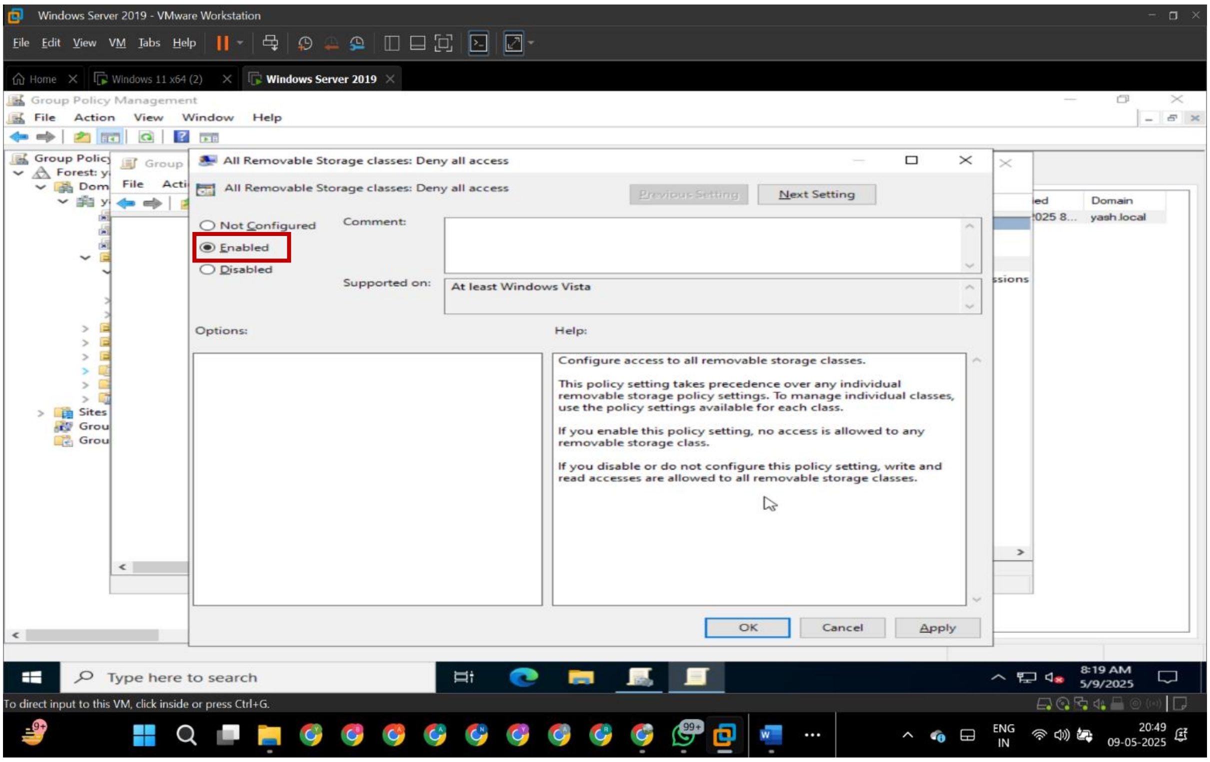
Select an item to view its description.

Setting
- Set time (in seconds) to force reboot
- CD and DVD: Deny execute access
- CD and DVD: Deny read access
- CD and DVD: Deny write access
- Custom Classes: Deny read access
- Custom Classes: Deny write access
- Floppy Drives: Deny execute access
- Floppy Drives: Deny read access
- Floppy Drives: Deny write access
- Removable Disks: Deny execute access
- Removable Disks: Deny read access
- Removable Disks: Deny write access
- All Removable Storage classes: Deny all acce
- All Removable Storage: Allow direct access ir
- Tape Drives: Deny execute access
- Tape Drives: Deny read access
- Tape Drives: Deny write access
- WPD Devices: Deny read access
- WPD Devices: Deny write access

19 setting(s)

To direct input to this VM, click inside or press Ctrl+G.

(Enabled the policy -All Removable Storage classes: Deny all access)



All Removable Storage classes: Deny all access

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

Configure access to all removable storage classes.

This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

If you enable this policy setting, no access is allowed to any removable storage class.

If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.

To direct input to this VM, click inside or press Ctrl+G.

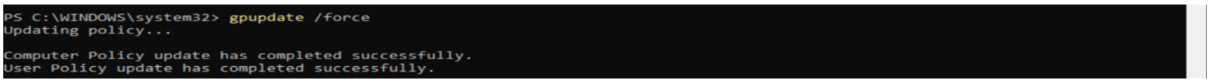
3.4 Policy Enforcement and Validation

The final phase involved validating that the GPO was correctly applied to the Finance OU users. This ensures that policy settings are not only configured but also enforced on target systems.

- **Verify GPO Application Using gpresult**

  Logged in as a user from the Finance OU in windows-domain joined machine, the gpresult /r command was run from the Command Prompt. This tool lists all applied GPOs, confirming whether the USB restriction policy took effect. The result showed the GPO was linked and enforced, meaning the configuration was successful.

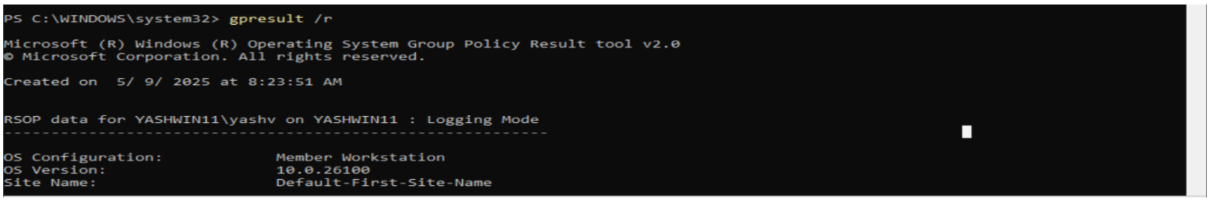
  (Forces a re-application of all Group Policy settings.)



```
PS C:\WINDOWS\system32> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Displays the summary of which policies were applied.



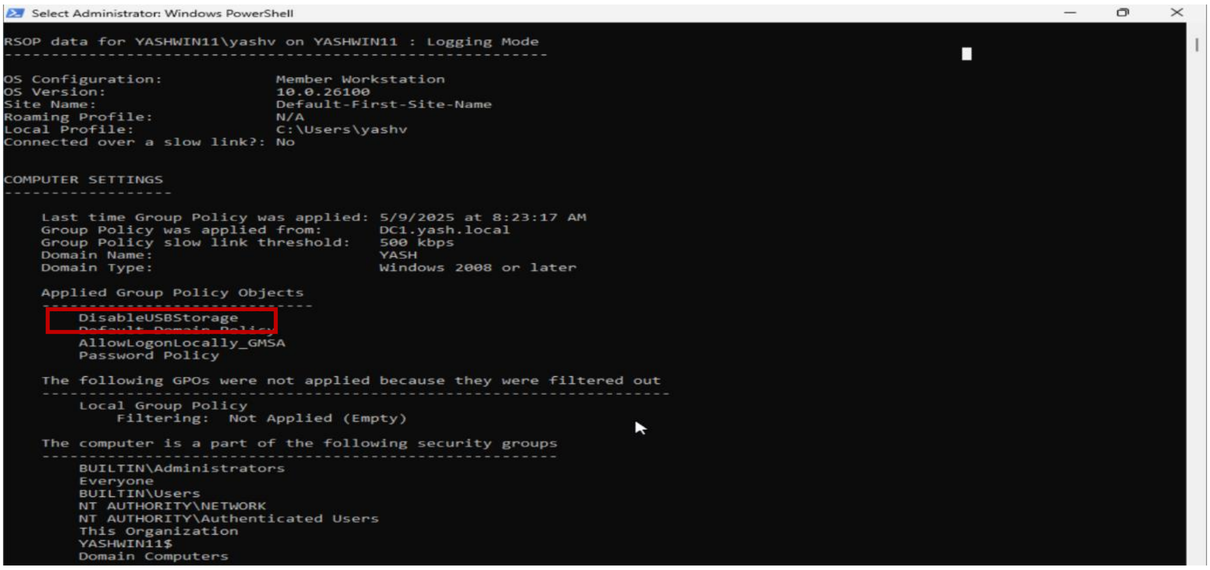
```
PS C:\WINDOWS\system32> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  5/ 9/ 2025 at 8:23:51 AM

RSOP data for YASHWIN11\yashv on YASHWIN11 : Logging Mode
-----------------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.26100
Site Name:                   Default-First-Site-Name
```



Select Administrator: Windows PowerShell

```
RSOP data for YASHWIN11\yashv on YASHWIN11 : Logging Mode
-----------------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.26100
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\yashv
Connected over a slow link?: No

COMPUTER SETTINGS
------------------

    Last time Group Policy was applied: 5/9/2025 at 8:23:17 AM
    Group Policy was applied from:      DC1.yash.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        YASH
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        DisableUSBStorage
        Default Domain Policy
        AllowLogonLocally_GMSA
        Password Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The computer is a part of the following security groups
    -------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Users
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        This Organization
        YASHWIN11$
        Domain Computers
```

4. Results and Findings

This section outlines the outcomes observed after implementing the Organizational Unit (OU) structure and applying the USB restriction policy. Each step of the process—from OU creation to GPO verification—was carefully tested to ensure accuracy and effectiveness. The findings confirm that the intended security configurations were applied as designed and behaved consistently across user systems.

- **OU Creation Successful**
  All four Organizational Units—Finance, HR, IT, and ServiceAccounts—were created under the domain root, providing a clear departmental structure for user organization and GPO targeting.

- **Users Correctly Organized**

Users were accurately moved into their respective OUs based on department. This ensures proper GPO application and simplifies future user management.

- **GPO Created and Linked Properly**
  The "Disable USB Storage" GPO was successfully created and linked specifically to the Finance OU, allowing targeted enforcement without affecting other departments.

- **GPO Verified Using gpresult**
  Running gpresult /r on a Finance user account confirmed that the USB restriction policy was applied and active, demonstrating successful policy propagation.

- **USB Access Blocked in Finance OU**
  Testing confirmed that USB storage devices were blocked on systems within the Finance OU, proving that the GPO was functioning as intended.

5. Recommendations

Based on the successful implementation and results, several recommendations are proposed to further enhance Active Directory management and security. These suggestions aim to improve policy precision, support long-term scalability, and ensure the environment remains secure and easy to administer. Following these recommendations can help maintain a robust and well-organized domain structure.

- **Use Sub-OUs for Granularity**
  Implement sub-OUs within major departments (e.g., Finance → Auditing, Payroll) for more refined control over group policies and delegated permissions.

- **Apply Additional GPOs**
  Consider applying GPOs for password complexity, login time restrictions, or application control to strengthen security policies across the network.

- **Schedule Policy Reviews**
  Regularly audit and test existing GPOs to ensure they remain effective, relevant, and aligned with current organizational security standards.

- **Enable GPO Logging**
  Enable GPO processing and event logging on client systems to monitor policy application issues or delays in real-time.

- **Train Admins on OU Management**
  Provide training for IT staff on OU and GPO management to ensure consistent policy deployment and reduce configuration errors.

6. Conclusion

This task successfully demonstrated the structured use of Organizational Units (OUs) and Group Policy Objects (GPOs) within an Active Directory environment to improve organization, security, and manageability. The creation of departmental OUs and the movement of users into their correct units enabled targeted policy deployment. Specifically, applying a GPO to disable USB storage access for the Finance department showed how security controls can be effectively enforced without impacting unrelated departments.

Through this implementation, the environment is now better prepared for future scaling, role-based access control, and enhanced departmental autonomy. The approach followed a systematic methodology that ensured accuracy, relevance, and verifiability at each step.