# Access Control

## 1. Introduction

Access control ensures that only authorized users can view, modify, or approve network requests. This phase focuses on leveraging ServiceNow’s Access Control Rules (ACLs) and dynamic approval assignment using Flow Designer.

## 2. Access Control Rules (ACLs)

***Objective***

To restrict read and write access to sensitive records based on user roles.

***Implementation***

- When the custom table (**u_network_database**) was created, default ACLs were automatically generated.
- Default ACLs were used to control:
  - Read access
  - Write access
  - Create access
  - Delete access
- Role-based restrictions were applied where necessary.

## 3. Dynamic Approver Assignment via Flow Designer

***Objective***

To dynamically determine approvers based on request conditions.

***Approval Logic***

Approvers are selected based on:

- Requester’s department
- Request approval state

***Configuration Steps***

- Create or update flow in **Flow Designer**.
- Add **Ask for Approval** action.
- Configure approver as:
    - Manager
    - Network group
- Use **Flow Logic → If condition** to validate approval state.
- Proceed only if approval is **Approved**.

## 4. Security Benefits

- Prevents unauthorized access
- Ensures compliance with approval policies
- Maintains audit trails

## 5. Conclusion

Access control mechanisms ensure secure handling of network requests by enforcing role-based access and dynamic approval routing, thereby strengthening governance and compliance.