**Governance Workflows in IGA**

Governance workflows automate user lifecycle events like onboarding, role changes, and offboarding, ensuring compliance and efficiency.

1. **Why Governance Workflows?**

* Consistency: Automates repetitive tasks like provisioning access.
* Security: ensures access is revoked promptly when users leave.
* Compliance: Tracks every action for audits.

1. **Key Life Cycle Events**:
2. Joiner (Onboarding)
   * Triggered when a new employee joins.
   * Tasks:
     + Create user account
     + Assign default roles and permissions
     + Notify stakeholders (managers, IT)
3. Mover (Role/Department Change)
   * Triggered when an employee changes roles.
   * Tasks:
     + Revoke old role permissions
     + Assign new role permissions
     + Update attributes (e.g., department, manager)
4. Leaver (Offboarding):
   * Triggered when an employee resigns or is terminated
   * Tasks:
     + Disable user account
     + Remove all access
     + Archive account data for audits
5. Example Workflow

Imagine onboarding a Software Developer:  
1. Trigger:

* + HR enters the new hire into Workday.
  + Saviynt detects this and starts the Joiner workflow.

2. Automated Actions:

* Provision accounts in AD and Git.
* Assign “Developer” role (access to code repositories, testing tools).

3. Notifications:  
 Notify the manager and IT team of successful onboarding.

4. Auditing:

* Log the actions for compliance purposes.

**Activity 5: Designing a Governance Workflow**

Design a workflow for the following scenario:

Joiner: A new HR manager joins the company.

1. What triggers the workflow?
2. What automated tasks would be performed?
3. Who should be notified?

***Joiner Workflow for an HR Manager:***

1. **Trigger**

* Onboarding/Joiner event triggers the workflow.
* Details:
  + HR enters the new hire into the HR systems (e.g. Workday).
  + A feed from Workday to Saviynt detects the new hire and initiates the workflow.

1. **Tasks performed**

* Create User Account
  + Provision an account in:
    - Active Directory (AD) for basic authentication
    - HR system (e.g., SAP SuccessFactors) for operational tasks.
* Assign Default Roles and Permissions:
  + Grant the HR Manager Role, which includes
    - Access to payroll systems
    - Access to employee data for reporting and analysis.
  + Apply additional ABAc rules
* Additional tasks (optional enhancements)
* Notify stakeholders
  + Stakeholders
  + Reporting manager
  + IT support for device allocation

1. **Notifications**

* Send notifications to
  + HR manager’s manager
    - Summary of granted permissions and tasks to complete (e.g., device setup).
  + IT team
    - Notify IT to provide a laptop, phone, and access card
  + Compliance Team
    - Inform for audit purposes if needed.

