Identity and Access Management (IAM) Workflows

- **Objective**: Develop structured workflows for identity lifecycle management (Joiners, Movers, Leavers) and access control processes to ensure secure, efficient, and compliant identity management.

Onboarding Process and Security Guidelines

- Initiate Onboarding:

Provide an overview of the employee's scope of work and security guidelines they must follow.

Safety Training:

Phishing awareness

Preventing tailgating at turnstiles

Badge security (avoiding badge switching)

Access control procedures

Best practices for handling company data and passwords

- Knowledge Session:

Employees must complete a knowledge session with a minimum qualification requirement to proceed in the onboarding process.

- Role Assignment and Workflow Integration:

Hiring manager collaborates with department managers (the provisioner) to assign employees to specific workflows.

IT team (system owner) updates the employee database and assigns necessary equipment from the inventory.

Department managers guide employees through: Account and profile creation, Single sign-on (SSO) usage, Passkey management within the company’s domain

- Access Control:

  Manager assigns roles based on job functions.

  Compliance officer reviews and approves role assignments for alignment with security policies.

- Data Encryption & Password Management:

  Compliance officer ensures that all personal data is fully encrypted.

  Provide employees with a secure password manager for creating, managing, storing, and sharing passwords.

  Admins have visibility into employee password practices for enforcing strong password creation and management.

- Role-Based Access Control (RBAC):

  Enforce RBAC to comply with the principle of least privilege.

  Ensure employees have access only to the resources required for their job functions.

- GDPR Compliance:

  Align with GDPR laws to ensure employee data rights are protected.

  Retain personal data only as long as necessary for its intended purpose.

Transfers and Promotions

- Employee Role Change:

  During transfers within the organization, an employee changes their role based on the scope of work.

- Provisioner Responsibility:

  The manager (provisioner) needs to pass on the information and update the IT department about this change.

- System Owner Duties:
    - The IT department (system owner) must:

      Deactivate any access the employee has to their former workflow.

      Reassign the employee's credentials to the new team (OWinfreyATL, 2024).

- Hiring Manager Notification:

  The hiring manager needs to be kept in the loop regarding all the changes.

- Role Reprovisioning and Auditing:

  Role reprovisioning and logging changes must be audited.

  Logs should be updated and documented for compliance and future reviews.

- Automation:

Offboarding Process

- Manager Responsibilities:

  Remove all access the employee has.

  Promptly replace the employee in any ongoing or upcoming projects.

- IT Department Duties:

  Permanently revoke permissions and delete or archive accounts after a specified period of time.

  Inform HR about the offboarding process.

Payroll Update:

Ensure payroll is updated to reflect the employee’s departure.

- Equipment Handover:

    On the last working day, the employee must:

    Return all equipment provided by the organization.

    Ensure that necessary data, email IDs, or files are transferred to the appropriate managers.

    Update returned equipment into the inventory system.

- Security Clearance:

    Verify and sanction the employee's security clearance before completion of offboarding.

- Compliance Auditor Duties:

    Verify that all access has been revoked.

    Document information about the employee’s roles and access privileges for future reviews.

IAM Entitlement Reviews and Approvals

- Audit Frequency:

    Companies should conduct an audit on a specified timeline, such as every quarter, to verify that security standards and protocols comply with company policies.

- Manager Responsibilities:

    Review employee access to identify outdated or excessive permissions.

    Automatically generate a list of current user permissions for review.

- Identifying Anomalies:

    If any anomalies are found, submit requests to the auditor for further action.

- Auditor and IT Department Duties:

  The auditor collaborates with the IT department to modify or remove unnecessary permissions.

- Documentation:

  Document details of all user accounts, including information about their roles and access privileges, for compliance and future reviews (User Access Reviews: Process & Best Practices Checklist, n.d.).