# Detailed IAM Process Flows

## User Onboarding and Provisioning Flow

Initiation: HR system flags new hire. Data Collected: Personal details, job title, department.  
Role Assignment: Based on job description, cross-reference with role matrix specifying access rights per role. Security Checks: Verify minimum necessary access.  
Account Creation: Tools used - IAM systems like Microsoft Azure AD, scripts for batch account creation. Verification by IT for proper setup.  
Access Provisioning: Automated where possible, manual steps are documented and audited. Exception Handling for additional access requests.  
Notification: Automated emails via IAM system. New employee must acknowledge receipt and understanding.  
Verification: Audit trail of all activities related to account setup. Compliance checks for internal and regulatory requirements.

## Access Request and Approval Flow

Request Submission: Via self-service portal, requiring specific access details and justification. Managerial Approval needed with logging.  
IT Review: IT reviews for security implications and compliance verification against standards like SOX, GDPR.  
Provisioning: Automated through provisioning engines, with manual oversight logged. Audit Logging using tools like Splunk.  
Notification: Automated upon successful provisioning, with all steps and approvals logged for audit purposes.

## Regular Access Review and Recertification Flow

Review Initiation: Scheduled quarterly, with pre-review reports generated. Stakeholder Notification through automated alerts.  
Data Collection: Using IAM tools to extract current access rights, cross-checked against job functions.  
Stakeholder Review: Discussions in meetings, decisions documented. Adjustments and revocation of access as needed, documented for compliance.  
Documentation: Updated in real-time, stored for audit purposes, ensuring compliance with all policies.

## De-provisioning and Offboarding Flow

Offboarding Initiation: Triggered by HR notification of employee termination. System Notification automated to IT and security.  
Access Revocation: Immediate revocation, verified across all systems. Account Deletion/Disabling as per data retention policies.  
Final Audit: Comprehensive check to ensure no residual access or data remains, with confirmation required from both IT and HR.