PERFORMANCE AND TESTING

Date	1 November 2025
Team ID	NM2025TMID07110
Project Name	Optimising user,group, and role management with access control and workflows
Maximum Marks	2 marks

Problem

The problem of Optimizing user, group, and role management with access control and workflows can be summarized as the challenge of balancing security, compliance, and operational efficiency in complex, multi-system IT environments. When not optimized, this area creates significant risk and administrative strain for the organization.

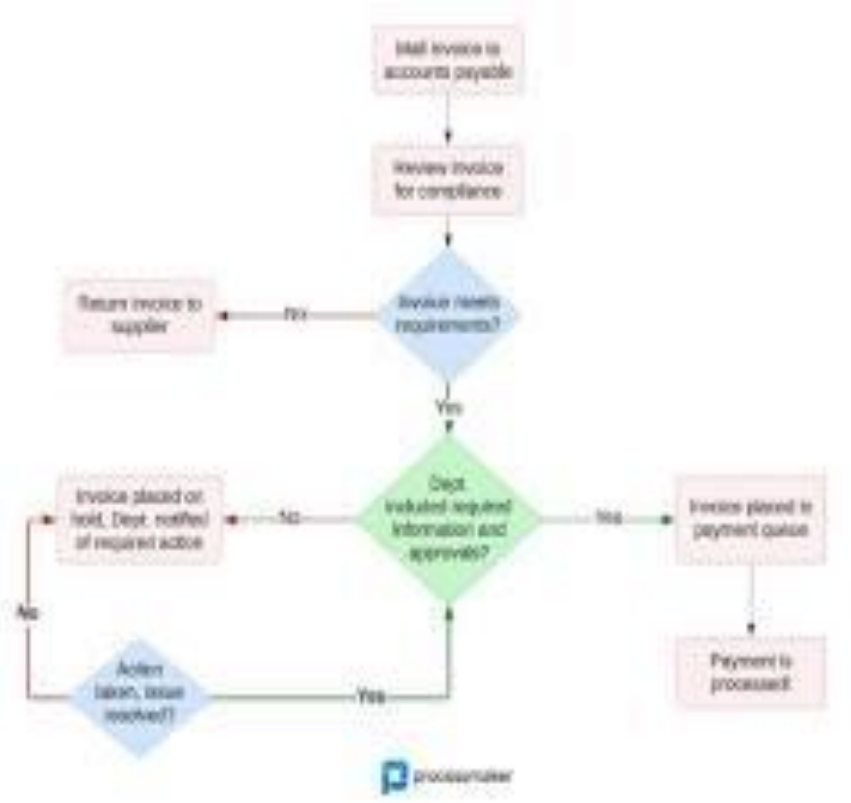
The primary pain point is the inability to consistently enforce the Principle of Least Privilege and maintain a verifiable audit trail. In unoptimized systems, access rights are often granted manually on a per-user, per-application basis, leading to “access sprawl” or “privilege creep.” This means employees retain access long after they need it, especially after changing roles, creating security vulnerabilities that can be exploited by malicious actors or lead to accidental data exposure.

Purpose

- **Enhance Security Posture**: To strictly enforce the Principle of Least Privilege, ensuring that every user (human and non-human) possesses only the minimum access rights absolutely necessary to perform their job function. This minimizes the organizational attack surface, mitigates the risk of insider threats, and prevents lateral movement by attackers exploiting excessive or stale permissions.
- **Ensure Regulatory Compliance:** To build an always-on, auditable system that can demonstrate “who has access to what, when, and why.” By automating access changes and maintaining comprehensive audit trails via defined workflows, the organization can easily satisfy stringent regulatory and audit requirements (like SOX, HIPAA, and GDPR), avoiding costly fines and reputational damage.
- **Drive Operational Efficiency and Scalability:** To eliminate manual, repetitive tasks associated with the user lifecycle—Joiner, Mover, Leaver (JML). By implementing automated provisioning and de-provisioning workflows, IT

administrators are freed from reactive access granting, speeding up employee onboarding, reducing troubleshooting time, and allowing the Identity and Access Management (IAM) infrastructure to scale seamlessly with business growth.

Template :


Mail invoice to accounts payable
Review invoice for compliance
Invoice meets requirements?
No
Return invoice to supplier
Yes
Dept. included required information and approvals?
No
Invoice placed on hold, Dept. notified of required action
Yes
Invoice placed in payment queue
Payment is processed
No
Action taken, issue resolved?
Yes
processmaker