TechCorp's IAM Platform Implementation Project Plan

Rohini Ravikumar
rohinizz96@gmail.com
https://www.linkedin.com/in/rrrohini/

agenda

1. Project Overview
2. Implementation Approach
3. Key Milestones & Timelines
4. Resource Requirements
5. Risk Management & Mitigation
6. Testing & Validation
7. Training & Change Management
8. Post-Implementation Support & Monitoring
9. Next Steps

Project Overview

Objective:

Implement an Identity and Access Management (IAM) platform that enhances **User Lifecycle Management** and **Access Control Mechanisms** to strengthen security, improve operational efficiency, and align with TechCorp's digital transformation strategy.

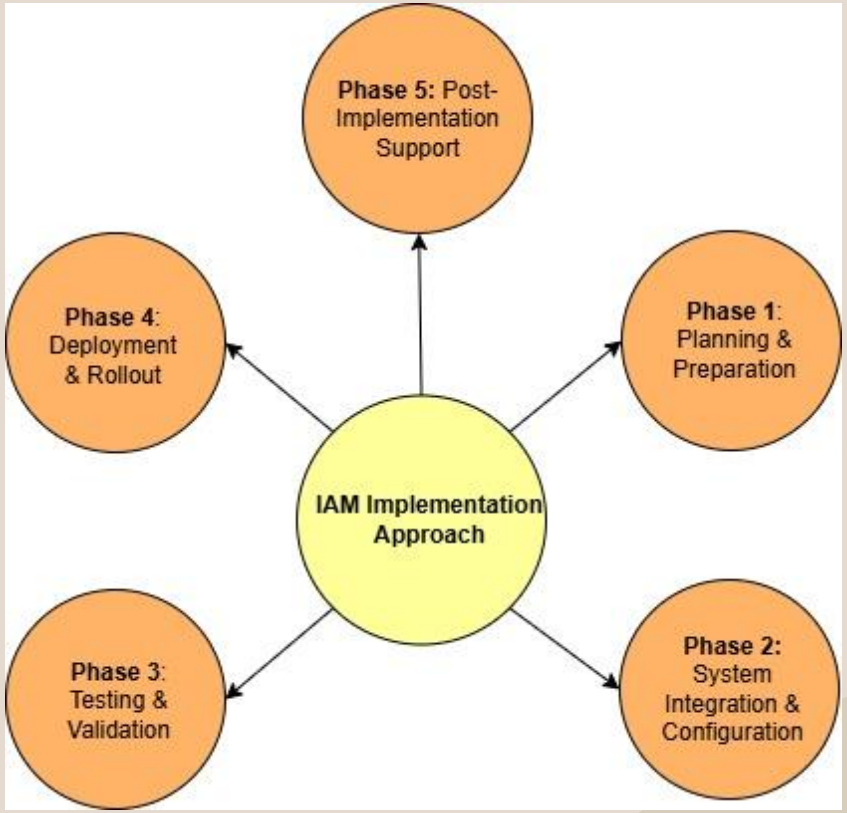
Scope:

- Automate user provisioning and de-provisioning
- Enforce multi-factor authentication (MFA)
- Strengthen privileged access management (PAM)
- Align IAM with compliance & governance

Success Criteria:

- Secure, seamless, and scalable IAM deployment
- Minimal disruption to TechCorp's daily operations

Implementation Approaches



A **structured, phased approach** ensures a seamless IAM platform deployment while minimizing disruptions to TechCorp's operations.

Phase 1: Planning & Preparation.

•Define **business & security requirements** for IAM integration
•Identify key **stakeholders** (IT, HR, Security, Compliance, Business Units)
•Assess **current infrastructure readiness** and integration points
•Develop a **project roadmap** with milestones, timelines, and dependencies

Phase 2: System Integration & Configuration.

- Deploy **IAM platform** (Okta, Microsoft Entra ID, or SailPoint)
- Configure **Role-Based Access Control (RBAC)** and user identity policies
- Integrate IAM with **HRMS (Workday, SAP SuccessFactors), IT systems, and cloud environments**
- Implement **Multi-Factor Authentication (MFA)** and **Privileged Access Management (PAM)**

Phase 3: Testing & Validation

- Conduct **unit testing** for individual IAM components
- Perform **integration testing** with HR, IT, and cloud services
- Run **User Acceptance Testing (UAT)** to ensure seamless authentication and access management
- Validate **security & compliance** requirements, including access control policies and audit logging

Phase 4: Deployment & Rollout

- **Pilot Deployment:** Implement IAM for a small group of users to gather feedback

- **Phased Rollout:** Gradual expansion across business units to minimize risk

- **Full Deployment:** Organization-wide IAM adoption with monitoring and support

Phase 5: Post-Implementation Support & Monitoring

- Continuous **real-time monitoring** for anomalies and security threats
- Implement **incident response procedures** for IAM-related security events
- Conduct **regular access reviews & compliance audits**
- Optimize IAM policies based on **user feedback and evolving security needs**

Key Milestones & Timelines

Milestones	Timeline
IAM Project Kickoff	Week 1
Infrastructure Readiness Assessment	Weeks 2-3
IAM Platform Deployment & Configuration	Weeks 4-6
Role-Based Access Control (RBAC) Setup	Weeks 7-8
User Lifecycle Management Automation	Weeks 9-10
Testing & Security Validation	Weeks 11-12
Pilot Deployment	Weeks 13-14
Organization-Wide Rollout	Weeks 15-18
Post-Implementation Monitoring	Ongoing (Week 19+)

Resource Requirements

Personnel:

•IAM Specialists (Architects, Developers, Engineers)

•Security & Compliance Experts

•IT Operations & Support Team

•HR & Business Process Owners.

Technical Resources:

•IAM Solution (Okta, SailPoint, Microsoft Entra ID)

•Cloud Infrastructure & Integration Tools

•Logging & Monitoring Systems (Splunk, QRadar)

Budget Considerations:

•Licensing & Subscription Fees

•Hardware & Software Costs

•Training & Change Management Expenses

Risk Management & Mitigation

Potential Risks & Solutions:

- **Integration Challenges** → Conduct pre-implementation testing & phased rollout
- **User Resistance to Change** → Provide early communication & comprehensive training
- **Security Misconfigurations** → Implement rigorous testing & compliance validation
- **Downtime During Deployment** → Plan for off-peak deployment & rollback mechanisms

Testing & Validation

Testing Phases:

1.Unit Testing – Validate individual IAM components

2.Integration Testing – Ensure seamless connectivity with HRMS, IT, and cloud systems

3.User Acceptance Testing (UAT) – Conduct real-world testing with key user groups

4.Security & Compliance Testing – Validate MFA, PAM, and Zero Trust policies

Success Metrics:

•100% role-based access compliance

•No unauthorized access detected during penetration tests

•Seamless authentication & authorization experience

Training & Change Management

Training Approach:

- **End-User Training:** Self-service access management, MFA authentication
- **IT & Security Team Training:** IAM administration, incident response
- **Leadership Awareness Sessions:** Strategic IAM benefits & compliance impact

Communication Strategy:

- Stakeholder briefings & Q&A sessions
- Internal knowledge base & help desk support
- Feedback collection & iterative improvements

Post-Implementation Support & Monitoring

Continuous Performance Monitoring:

•Use SIEM tools (Splunk, IBM QRadar) for security event monitoring
•Real-time alerts on authentication failures & access anomalies

Incident Response & Troubleshooting:

•Define escalation procedures for IAM-related incidents
•Conduct post-implementation audits & fine-tune policies

Ongoing Enhancements:

•Regularly update IAM policies based on business changes
•Integrate new security features as IAM technologies evolve

Next Steps

- Finalize stakeholder approvals & project kick-off.
- Conduct initial infrastructure assessment
- Establish implementation roadmap & assign resources
- Initiate first phase (IAM platform configuration & integration)
- Set up governance & monitoring framework for sustained security

thank you

Rohini Ravikumar

- rohinizz96@gmail.com
- https://www.linkedin.com/in/rrrohini/