1. Introduction

TechCorp Enterprises has undertaken a strategic initiative to strengthen its digital identity management to support its ongoing digital transformation. Based on our readiness assessment, we propose the following IAM solution designs focused on enhancing **User Lifecycle Management (ULM)** and **Access Control Mechanisms (ACM)**.

---

2. IAM Solution Designs

A. User Lifecycle Management (ULM)

Solution Outline

Implement a centralized Identity Governance and Administration (IGA) platform that automates identity provisioning, de-provisioning, role assignment, and access reviews.

Key Components

- **Identity Repository**: A master directory (e.g., Microsoft Active Directory + LDAP integration)
- **Automated Provisioning/De-provisioning**: Using tools like **SailPoint**, **Okta Lifecycle Management**, or **Microsoft Entra ID**
- **Role-Based Access Control (RBAC)**: Predefined access roles for departments/functions
- **Joiner-Mover-Leaver (JML) Automation**:
  - *Joiner*: Auto-provision roles, email, tools on Day 1
  - *Mover*: Adjust permissions with role change
  - *Leaver*: Revoke access immediately and archive data
- **Periodic Access Review System**: Integrated with HRMS and audit trail logging

Implementation Plan

1. Integrate HR system with IAM tool (e.g., SAP SuccessFactors + Okta)
2. Define user personas and map roles

3. Automate workflows for onboarding and offboarding
4. Set review policies and automatic expiry of temporary access
5. Train admins and conduct UAT before rollout

B. Access Control Mechanisms (ACM)

Solution Outline

Strengthen identity verification and access control by implementing a Zero Trust model using fine-grained access controls and continuous authentication.

Key Components

- **Multi-Factor Authentication (MFA)**: Biometric + device-based MFA using **Duo Security** or **Microsoft Authenticator**
- **Single Sign-On (SSO)**: Federated login for internal & cloud apps using **SAML/OpenID Connect**
- **Privileged Access Management (PAM)**: Solutions like **CyberArk** or **BeyondTrust** to manage high-level access
- **Least Privilege Enforcement**: Role-based entitlements with just-in-time (JIT) access for sensitive systems
- **Access Request Portal**: Self-service access request platform with approval workflow
- **Real-time Session Monitoring** and **Anomaly Detection**: Using **SIEM tools** (Splunk, Elastic, Azure Sentinel)

Implementation Plan

1. Enforce MFA for all users
2. Set up SSO integrations for enterprise and SaaS tools
3. Identify and secure privileged accounts
4. Deploy policy-based access and Just-In-Time access control
5. Monitor logs and review anomalies weekly

3. Alignment with Business Processes

IAM Element	Business Process Integration
JML automation	Connects directly to HR workflows, automating onboarding/offboarding
Role-based access	Aligns with departmental roles for efficient provisioning
SSO & MFA	Simplifies authentication across business units, improving productivity
PAM	Protects systems used by developers, system admins, and cloud engineers
Access reviews	Embedded into audit/compliance team routines

4. Alignment with Business Objectives

Business Objective	IAM Contribution
Enhance security	Immediate access revocation, MFA, session monitoring
Improve UX	SSO + seamless onboarding
Operational efficiency	Workflow automation, reduced helpdesk load
Digital transformation	Supports secure scaling of digital tools and cloud adoption
Competitive edge	Modern, agile, and secure IAM aligned with innovation

5. Rationale Behind Choices

- **SailPoint / Okta**: Industry-standard IAM tools with cloud-native support and HR integration
- **SSO + MFA**: Balance between user convenience and robust security
- **Zero Trust**: Modern standard for securing a distributed workforce
- **Privileged Access Control**: Addresses growing insider threat risks

- **Automated Access Reviews**: Ensure regulatory compliance with minimal manual effort

6. Conclusion

These IAM solution designs are crafted to meet TechCorp’s security goals and support their operational agility in a fast-paced tech environment. By automating identity management and enforcing strong access controls, TechCorp will be positioned to reduce risk, enhance user experience, and lead confidently through its digital transformation journey.