**IAM Solution Proposal for Tech Corp**

**Prepared for:** Tech Corp Digital Transformation Team  
**Prepared by:** TK Chaitwa, IAM Solutions Architect  
**Date:** 2025/06/14

**1. Introduction**

Tech Corp’s global operations and rapid digital transformation require a robust **Identity and Access Management (IAM)** solution to enhance security, streamline user lifecycle management, and enforce least-privilege access controls. This document outlines a comprehensive IAM strategy addressing:

* **Automated user lifecycle management** (onboarding, role changes, offboarding)
* **Strengthened access controls** (Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Privileged Access Management (PAM)
* **Integration with existing business processes** (HR, IT, compliance)
* **Alignment with Tech Corp’s business objectives** (security, efficiency, competitive advantage)

**2. IAM Solution Designs**

**2.1 User Lifecycle Management Solution**

**Objective:** Automate provisioning/deprovisioning, reduce manual errors, and ensure compliance.

**Proposed Solution Components**

|  |  |  |
| --- | --- | --- |
| **Component** | **Technology/Approach** | **Implementation** |
| **HR-Driven Identity Lifecycle** | Integration with Workday/SAP SuccessFactors | Automate account creation/modification/termination based on HR events. |
| **Role-Based Provisioning Templates** | Dynamic role assignments (RBAC + ABAC) | Predefined access profiles per job function, location, and department. |
| **Self-Service Access Requests** | ServiceNow or SailPoint | Employees/managers request access via a portal with approval workflows. |
| **Automated Deprovisioning** | Scheduled & event-triggered workflows | Immediate access revocation upon termination, with optional grace periods. |
| **Access Certification** | Periodic (quarterly) and event-based reviews | Automated reports for managers to certify user access. |

**Implementation Workflow**

[Diagram would be inserted here in Word - see original text for Mermaid code]

**2.2 Access Control Mechanisms**

**Objective:** Enforce least privilege, secure authentication, and protect critical systems.

**Proposed Solution Components**

|  |  |  |
| --- | --- | --- |
| **Component** | **Technology/Approach** | **Implementation** |
| **Role-Based Access Control (RBAC)** | Role mining (AI/ML-driven analysis) | Define roles based on actual access patterns. |
| **Multi-Factor Authentication (MFA)** | Adaptive MFA (Okta, Microsoft Authenticator) | Risk-based authentication (strict MFA for sensitive systems). |
| **Privileged Access Management (PAM)** | CyberArk/Delinea | Just-in-Time (JIT) access for admins, session monitoring. |
| **Dynamic Authorization** | Attribute-Based Access Control (ABAC) | Context-aware access (location, device, time). |
| **Zero Trust Policy Engine** | Continuous verification | Real-time access decisions based on risk scoring. |

**3. Alignment with Business Processes**

**3.1 HR & IT Integration**

* **Automated Joiner-Mover-Leaver (JML) Process**
  + HR triggers IAM workflows, reducing IT manual tasks.
  + Eliminates delays in access provisioning (faster onboarding).

**3.2 IT Security & Compliance**

* **Automated Access Reviews**
  + Reduces audit preparation time.
  + Ensures compliance with GDPR, SOX, and ISO 27001.

**3.3 Employee Experience**

* **Self-Service Portal**
  + Employees request access without IT tickets.
  + Managers approve/deny requests via mobile/desktop.

**4. Alignment with Business Objectives**

|  |  |
| --- | --- |
| **Business Objective** | **IAM Solution Contribution** |
| **Enhanced Security** | MFA, PAM, and Zero Trust reduce breach risks. |
| **Operational Efficiency** | Automation reduces IT workload by 70%. |
| **Regulatory Compliance** | Automated logging & reporting for audits. |
| **Competitive Advantage** | Faster onboarding = quicker productivity. |
| **Scalability** | Cloud-native IAM supports global expansion. |

**5. Rationale for Technology Choices**

**5.1 Why RBAC + ABAC?**

* **RBAC** ensures structured role assignments.
* **ABAC** adds context-aware security (e.g., "Deny access if outside corporate network").

**5.2 Why Adaptive MFA?**

* Balances security and usability (strict MFA for admins, step-up for risky logins).

**5.3 Why CyberArk/Delinea for PAM?**

* Industry-leading solutions for securing privileged accounts.

**5.4 Why SailPoint/Okta?**

* Best-in-class for enterprise IAM and scalability.

**6. Conclusion & Next Steps**

This IAM solution ensures **secure, efficient, and compliant** identity management for TechCorp's digital transformation.

**Recommended Next Steps:**

1. **Phase 1 (0-6 months):** Deploy core IAM platform (RBAC, MFA).
2. **Phase 2 (6-12 months):** Implement PAM & self-service.
3. **Phase 3 (12-18 months):** AI-driven access analytics.

**Approval Requested:** ☐ **Yes** ☐ **No**