**TechCorp Enterprises: Proposed Identity & Access Management (IAM) Solutions**

**Prepared for:** TechCorp Executive Leadership & IT Governance Board

**Prepared by:** Ikwuka Okoye – Cybersecurity IAM Consultant (TCS Virtual Experience Program)

**Date:** 2nd December, 2025

**Executive Summary**

TechCorp Enterprises operates in a highly competitive technology sector where rapid innovation must be balanced with robust security and regulatory compliance. Following the recently completed IAM readiness assessment, this document presents a comprehensive, business-aligned IAM solution design that directly addresses the two priority areas identified:

1. Enhancing User Lifecycle Management
2. Strengthening Access Control Mechanisms

The proposed solutions leverage modern, cloud-native, and standards-based technologies to deliver measurable improvements in security posture, operational efficiency, employee/contractor experience, and overall competitive advantage.

**1. IAM Solution Design Overview**

| Focus Area | Core Platform | Key Supporting Technologies | Deployment Model |
|---|---|---|---|
| User Lifecycle Management | SailPoint IdentityNow (primary) + Okta Workforce Identity Cloud (secondary/hybrid) | Workday (HRIS integration), ServiceNow (ITSM), Microsoft Entra ID (Azure AD) | Cloud-first (SaaS) |
| Access Control Mechanisms | Saviynt Enterprise Identity Cloud + BeyondCorp-style Zero Trust (Google | OAuth 2.0 / OIDC, FIDO2/WebAuthn, AWS | Cloud-native + on-prem gateways where |

| | |
|---|---|
| BeyondCorp Enterprise) | Verified Permissions (policy required engine), Prisma Access (ZTNA) |

**Rationale for Technology Choices**

- **SailPoint IdentityNow** and **Saviynt** are Gartner Magic Quadrant leaders in 2025 for both Identity Governance & Administration (IGA) and Privileged Access Management (PAM).
- **Okta** provides best-in-class SSO and lifecycle automation with native Workday integration (TechCorp's HR system).
- Zero-Trust principles are enforced using **Google BeyondCorp Enterprise** and **Palo Alto Prisma Access**—both proven at global scale in tech companies similar to TechCorp.

**2. Detailed Solution: Enhancing User Lifecycle Management**

**2.1 Automated Joiner-Mover-Leaver (JML) Processes**

- **Joiners**: New hire record created in **Workday** → automatic provisioning of accounts (Entra ID, Google Workspace, Salesforce, GitHub, AWS, ServiceNow, etc.) within <3 minutes.
- **Movers**: Department or role change in Workday triggers birthright role re-evaluation and automatic access adjustment using AI-driven identity analytics (SailPoint AI Access Modeling).
- **Leavers**: Immediate de-provisioning upon HR termination event; 100% off-boarding within 15 minutes, including revocation of VPN, physical badge, and cloud accounts.

**2.2 Self-Service Access Request Portal (ServiceNow + SailPoint)**

- Low-risk applications available via shopping-cart-style catalog.
- AI-driven recommendation engine suggests appropriate roles based on peer analysis ("people like you have these apps").

**Efficiency Gains**

- 85% reduction in manual IT tickets for access provisioning (industry benchmark achieved by similar deployments).
- Average new-hire productivity ramp-up reduced from 5 days to <4 hours.

**3. Detailed Solution: Strengthening Access Control Mechanisms**

**3.1 Role-Based + Attribute-Based Access Control (RBAC + ABAC Hybrid)**

- Birthright roles for baseline access (e.g., “All Employees”, “Engineering”).
- Dynamic ABAC policies using attributes such as device compliance, location, time, and risk score (e.g., “Engineers can push to production only from corporate-managed devices inside trusted geographies”).

**3.2 Continuous Zero-Trust Verification**

- Implementation of **Google BeyondCorp Enterprise**: every request is authenticated, authorized, and encrypted—regardless of source IP.
- Integration with **CrowdStrike Falcon Identity Protection** for real-time risk scoring.

**3.3 Passwordless & Phishing-Resistant Authentication**

- Enterprise-wide rollout of FIDO2 hardware keys (YubiKey 5) and passkeys for privileged users.
- All other users migrated to WebAuthn/passkeys by Q4 2026.

**3.4 Just-in-Time (JIT) Privileged Access**

- Privileged accounts have zero standing permissions.
- Elevation requests via **Saviynt** → temporary access granted for 1–8 hours with full session recording.

**Security Impact**

- Eliminates credential theft as an effective attack vector.
- Reduces lateral movement risk by >90% (aligned with MITRE ATT&CK framework coverage).

**4. Alignment with TechCorp's Existing Business Processes**

| Business Process | Current Pain Point | How the IAM Solution Resolves It |
|---|---|---|
| New hire onboarding | 3–5 days to full productivity | Fully automated provisioning (<4 hours) |
| Mergers & Acquisitions | Manual access reconciliation takes weeks | Automated identity ingestion & rapid de-provisioning |
| Agile development cycles | Frequent role changes cause access lag | Real-time attribute sync + AI role recommendations |
| Remote/hybrid workforce | VPN-based access is slow and insecure | Zero-Trust model removes VPN dependency |
| Regulatory audits (SOC 2, ISO 27001, GDPR) | Manual evidence collection | Automated certification campaigns & continuous compliance reporting |

**5. Alignment with TechCorp's Broader Business Objectives**

| Business Objective | Contribution of Proposed IAM Solution |
|---|---|
| Maintain market leadership in innovation | Faster onboarding & secure collaboration enable engineers to focus on building instead of waiting for access |
| Zero major security breaches | Phishing-resistant MFA + continuous Zero Trust verification drastically reduces breach probability |
| Exceptional customer & employee experience | Passwordless login and self-service access requests deliver seamless, modern digital experience |
| Scalability for global expansion | Cloud-native SaaS platforms support instant rollout to new regions with zero additional hardware |
| Cost efficiency | 60–80% reduction in helpdesk tickets + elimination of legacy on-prem IAM systems |

**6. Summary of Key Benefits**

| Metric | Current State (Est.) | Target State (12 months post-implementation) |
|---|---|---|
| Time to provision new user | 3–5 days | <4 hours |
| % of access requests self-service | ~15% | >90% |
| MFA coverage (phishing-resistant) | 8% | 100% (privileged) + 85% (all users) |
| Mean time to revoke leaver access | 24–48 hours | <15 minutes |
| Annual IAM-related helpdesk tickets | ~18,000 | <4,000 |

**Conclusion & Recommendation**

The proposed IAM architecture—centered on **SailPoint IdentityNow**, **Saviynt**, **Okta**, and a **Zero-Trust** access fabric—directly addresses TechCorp's maturity gaps while delivering immediate business value. It transforms identity from a cost center into a strategic enabler of secure innovation, employee productivity, and customer trust.

I recommend proceeding with a 10-week proof-of-concept focusing on the Engineering and Finance business units, followed by enterprise-wide rollout in 2026.

Ikwuka Okoye

Cybersecurity IAM Consultant

Tata Consultancy Services (TCS) Virtual Experience Program