**TechCORP Enterprise IAM Strategy Assessment**

SUMMARY

TechCORP Enterprise operates in the Information Technology and Services industry with a global reach of 100 plus countries in the world. It employs over 150,000 people across the globe. As an enterprise operating internationally, TechCORP has a plethora of digital assets that need to be secured and available for their daily operations.One of the primary controls for protecting these assets is Identity and Access Management (IAM). However, before an IAM solution is implemented it is necessary to assess TechCORP’s current IAM strategy and their challenges and aspirations regarding the control. Following checklist is produced for assessing the IAM readiness of the organization.

CHALLENGES AND ASPIRATIONS of TechCORP

* Security concerns: With TechCORP’s expanding digital footprint, data breaches are an extreme concern.
* User experience: TechCORP aims to provide a seamless and secure experience for employees, partners and customers accessing its digital platforms.
* Operational efficiency: Streamlining access management and minimizing manual processes are key aspirations to TechCORP.
* IAM strategy: TechCORP already has an existing strategy in place, but it needs a thorough assessment to ensure it aligns with the organization's evolving needs.

IAM Strategy Assessment Checklist for TechCorp

User lifecycle management:

* Evaluate the process of onboarding and offboarding users.
* Ensure efficient management of user roles and privileges.
* Verify the handling of user account changes and updates.

Access control mechanisms:

* Review access control policies and procedures.
* Assess the effectiveness of authentication methods.
* Check for access controls that prevent unauthorized access.

Compliance and governance:

* Ensure compliance with industry regulations and data protection laws.
* Verify the existence of governance policies and procedures.
* Evaluate the process for auditing and reporting access activities.

Integration with existing systems:

* Assess the integration of IAM systems with TechCorp's legacy systems.
* Check for seamless synchronization of user data across systems.
* Verify the compatibility of IAM solutions with existing IT infrastructure.

Cloud services integration:

* Review the integration of IAM with cloud services used by TechCorp.
* Ensure that IAM solutions extend to cloud environments securely.
* Verify access controls for cloud-based applications and data.

Enhanced user experience:

* Evaluate user interfaces for ease of use and accessibility.
* Check for self-service capabilities for password resets and access requests.
* Ensure a balance between security and user convenience.

RESULT

After a thorough assessment it was found that TechCORP requires enhanced user life cycle management and strong access control mechanisms. Based on this result a customized IAM solution is designed.

**User Lifecycle Management**

Objective: To streamline user onboarding, access modification, and offboarding processes.

Solution: Implement an automated user provisioning system integrated with TechCORP's HR database. This system will ensure that user access permissions are updated in real-time based on employment status changes. Additionally, a self-service portal will allow employees to request access changes with manager approval workflows.

Technology: Utilize identity management software like SailPoint to automate user provisioning and de-provisioning. Integrate this software with HR systems using API connectors.

**Access Control Mechanisms**

Objective: To strengthen access controls and reduce the risk of unauthorized access.

Solution: Implement a role-based access control (RBAC) system. Define roles based on job responsibilities and grant permissions accordingly. Conduct regular access reviews and certifications to ensure alignment with roles.

Technology: Implement a leading RBAC solution such as Oracle Identity Manager. Configure the system to assign permissions based on user roles and integrate it with TechCORP's Active Directory.