**IAM Framework and Scope for Redback Operations.**

Introduction

An Identity and Access Management (IAM) framework establishes a standardized approach to managing user identities, access controls, and authorization within an organization. This report outlines the scope of an IAM framework for Redback Operations. Defining the scope ensures the framework identifies and addresses critical security needs while remaining implementable and scalable.

The Businesses Constraints and Considerations

The IAM framework should address the following business needs:

* Must mitigate the risk of unauthorized access to sensitive data and resources by implementing strong authentication and authorization controls.
* Must ensure compliance to relevant industry regulations and data privacy laws (e.g., GDPR, PCI-DSS).
* Should streamline user provisioning, access requests, and permission management processes.
* Should accommodate growth in users, applications, and data while maintaining security and control.
* Must provide a centralised platform for managing identities and access across the organization.

Framework Scope

The IAM framework will encompass the following core elements:

1. Identity Management:

* User registration and provisioning processes.
* User lifecycle management (e.g., activation, deactivation, deletion).
* User attributes and group memberships.
* Directory services integration (e.g., Active Directory, LDAP).

1. Access Control:

* Role-Based Access Control (RBAC) model for assigning permissions based on user roles.
* Attribute-Based Access Control (ABAC) for granular access control based on specific user attributes and resource characteristics.
* Least Privilege principle: Granting users the minimum access required to perform their jobs.
* Authentication:
* Multi-factor Authentication (MFA) for strong user verification beyond passwords.
* Single Sign-On (SSO) for seamless access to multiple applications with a single login.

1. Authorization:

* Defining access policies that determine user permissions to access resources (e.g., applications, data).
* Continuously monitoring and auditing user activity to identify suspicious behavior.
* Governance:
* Establishing clear ownership and accountability for IAM processes.
* Defining approval workflows for access requests and permission changes.
* Regularly reviewing and updating the IAM framework to address evolving security threats.

Framework Exclusions

The following elements are currently excluded from the IAM framework scope:

* Physical Access Control: Managing physical access to facilities and equipment (may be integrated in the future).
* Device Management: Securing and managing employee-owned devices (may be integrated in the future).
* Data Loss Prevention (DLP): Preventing unauthorized data exfiltration (may be integrated as a complementary security measure).
* These exclusions can be revisited and incorporated into the framework at a later stage based on evolving security requirements.

Implementation Considerations

The successful implementation of the IAM framework requires careful consideration of the following factors:

* Existing Infrastructure: Leveraging existing systems for the use of on premises solutions.
* Scalability: Choosing an IAM solution that can scale to accommodate future growth.
* User Adoption: Developing a comprehensive training program to educate users on the new IAM processes.
* Integration: Ensuring seamless integration of the IAM framework with existing applications and systems.
* Cost: Balancing the cost of implementing and maintaining the IAM framework with the security benefits it provides.

Conclusion

This report has outlined the scope of an IAM framework for Redback Operations. By implementing a comprehensive IAM framework, the organization can significantly enhance security, improve compliance, and streamline user access management. The defined scope provides a roadmap for successful implementation, considering business needs, technical considerations, and ongoing governance. Regular review and updates will ensure the IAM framework remains effective in protecting the organization's critical assets in the ever-evolving threat landscape.

References

National Institute of Standards and Technology (NIST). (2018, August). Special Publication 800-63B: Digital Identity Guidelines. <https://pages.nist.gov/800-63-3/sp800-63b.html>

Cloud Security Alliance (CSA). (2020). Cloud Controls Matrix (CCM) v4.0. <https://cloudsecurityalliance.org/research/cloud-controls-matrix>

Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Systems (2nd ed.). Wiley.