Bryant UNIVERSITY

Recommendation: Directory Services Architecture and Future IAM Governance Model

I. EXECUTIVE SUMMARY

Identity and access management (IAM) is a broad administrative function that identifies individuals in a system, and controls and facilitates their access to resources within that system by associating user rights and restrictions with the established identity. Most of the challenges associated with managing digital identities and access management are organizational rather than technical. The imminent solution is a well-planned institution-wide IAM framework. One that includes a formal IAM governing authority, a well-defined technology architecture, a risk assessment and assurance level model, and an overall directory services operations governance model.

The focus of this document is to outline a framework for the University to use in developing an IAM strategy and to address gaps in its current directory services architectural model such as: lack of ownership by a central body, lack of separation between operations and governance tasks, and an uneven information services governance maturity. University initiatives into future cloud solutions, managed services and application delivery models will benefit from our efforts here to plan and implement a well-designed, secure IAM infrastructure.

Goal: Establish IAM as a core information service, providing stable, reliable and reusable identity technologies and authoritative identity sources, supported by an expert and experienced identity delivery organization.

II. PROBLEM OPPORTUNITY STATEMENT

Secure and manageable access to information assets must be provided within an increasingly complex IT environment. Cloud solutions, managed service models, and packaged applications often have their own authentication and authorization systems, as well as management tools for creating and managing accounts that are separate from existing University directory stores. Separate directory stores frequently result in unconnected islands of digital identity information thereby increasing overall complexity.

Security, managed access and entitlement is also about effective operational processes. Poor management processes covering the accounts that represent faculty, students and staff results in increased operational and security risk.

III. IAM Benefits

Controlled and well-defined identity and access management allows organizations to extend access to their information systems without compromising security, reliability and stability. Organizations provide this extended access by precisely managing authentication and entitlements according to a standardized set of practices. Stakeholder agreement or direction on how subjects or identities are to be represented and what services they are entitled to is agreed upon, established, communicated, executed and documented.

Identity has become a focal point of many governmental and regulatory bodies. This emphasis is a result of the growing focus on privacy, as more personal information is stored on information systems. The Gramm-Leach-Bliley Financial Services Modernization Act is just one example applicable to the University environment. Controlling access to student and employee information is not just good business practice; an organization that fails in this area is open to significant financial and legal liability. Regulatory compliance ensures that the University meets applicable privacy, authentication, authorization, and auditing requirements mandated by any and all applicable regulations. A properly executed identity and access management infrastructure built on a solid identity and access management platform will help the University meet these regulatory requirements.

IV. IAM Framework Architecture

A well-planned institution-wide IAM framework which includes a formal IAM governing authority, a well-defined technology architecture, a risk assessment and assurance level model, and a directory services (e.g., Active Directory) operations governance model, puts the University on the path to establishing stable, reliable and reusable identity technologies and authoritative identity sources supported by a maturing and experienced identity delivery organization. See Figure 1.0.

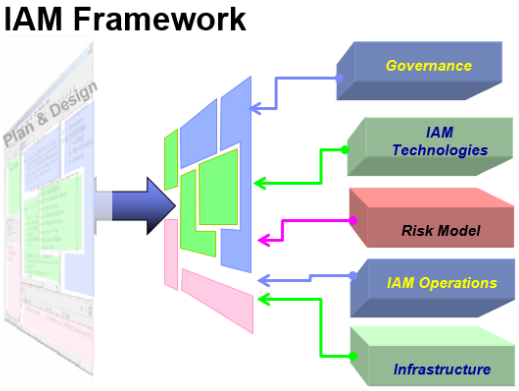

Figure 1.0

V. IAM GOVERNANCE

IAM governance is the establishment and management of policies (guidelines), processes and accountabilities for core IAM functions and is critical to the long-term success of any IAM deployment. The IAM governance committee's purpose is to take into consideration institution and regulatory drivers as it discusses, plans, and approves the implementation of changes and enhancements to IAM functions and components. In general, the committee takes into account stakeholder requirements, defines roles and responsibilities, and performs verification of compliance factors.

The IAM governance committee should include a variety of stakeholders from across the University that make use of identity and access management services. Similar to the Banner Data Standards Committee, the IAM Committee's charge should be:

- Link IAM governance to IT, information security and risk governance;
- Remove barriers to the IAM program's success;
- Provide effective IAM program oversight;
- Drive IAM governance across the University;
- Guide and participate in the promotion of the business benefits of IAM services;
- Define the composition, roles and responsibilities, and authority for a governing body for the campus IAM service;
- Allow in-depth stakeholder participation in specific areas of interest;
- Enact IAM governance decisions.

The accountable party for accepting, rejecting, and enforcing proposals from the committee should be the Office of the CIO.

VI. IAM TECHNOLOGIES

Current IAM frameworks in the University space include a typical set of enabling technologies (all may not be immediately applicable to Bryant):

- Identity Administration & Provisioning - Flexible and reliable tools for identity and account creation, update, and removal, and connector-based provisioning integration with downstream systems. Both person and non-person identities (e.g., resources, services/applications, devices) are included;
- Group & Role Management - Federated management of static and dynamic groups and roles;

- Authorization Workflows and Repository - Access request/approval and renewal/recertification workflows and tracking, plus a repository to store authorization and privilege data extracted from key campus systems to provide a single source for knowing "who has access to what" across the university;
- Authentication - Enhancements to existing campus Login authentication services to enable lightweight (and "bring your own identity") authentication for low-risk transactions and strong multi-factor authentication for high-risk activities, as well as federated authentication;
- Logging & Auditing - Collection and storage of transactions across the above IAM functional areas, and the mechanisms to analyze and report on those transactions.

Directory services is the foundation of the identity and access management technologies. It provides a single source of authoritative digital identity information. Such information includes security information such as passwords, as well as user profile information in the form of user attributes that include addresses, telephone numbers, office space, titles, and department names. A consistent and effective identity and access management strategy requires a sound understanding of the approaches and technologies used to address proliferating digital identities. The identity data should ultimately be made available for this purpose through an identity data service supported by an enterprise directory.

The primary identity directory used by the University is Microsoft Active Directory. There are several other database, directory service, and application-specific identity stores proliferating within the University. An effective identity and access management strategy would consolidate these into the minimum number of identity stores that collectively would become the standard trusted identity service for the University. A central identity integration service can help create an aggregate view of the information from multiple identity stores.

The extent to which IAM technologies listed above are applicable to the Bryant environment and the extent to which existing technologies can be leveraged, should be a recommendation made by the governance committee after careful exploration. It is highly recommended that the committee seek input from an IAM strategy consultant.

VII. IAM RISK MODEL

An IAM risk model is an important component in the overall framework. It will help ensure that resources and services are appropriately governed, they are compliant and processes are in place to mitigate risks. As an organization we seek to administer, secure, and access our information resources. It's important we go beyond merely managing the allocation of access and authorizations by including a risk-based model that will allow us to uncover critical security gaps and thus help prevent any form of misuse.

VIII. IAM OPERATIONS GOVERNANCE

IAM operational management should be performed by an IAM operations team consisting of members of the various IT technical groups. The day-to-day operational duties consisting of acquisition, hosting, configuration, administration, monitoring, debugging, support, disaster recovery, etc., on the set of IAM core services should be performed in accordance with IAM governance decisions.

IX. INFRASTRUCTURE

IAM technologies should leverage existing underlying core infrastructure resources wherever possible to minimize costs. However, University decision makers should make the determination whether or not to enlist new resources (premise or cloud based) that will aid in the development and implementation of the IAM solution.

X. SUMMARY

This document represents a high-level overview of an IAM roadmap for the University to consider. The actual planning and implementation of any selected technology solution described within this document requires a separate set of follow-on projects in order to develop and implement a practical and achievable IAM plan. The University cannot expect to achieve an IAM framework overnight, but rather, we should start with a subset of IAM governance practices and put a plan in place (with assistance from an IAM strategy consultant) to build a complete solution, one fitting the University's risk profile.