Project Charter

Identity & Access Management Strategy

Executive Summary

The Identity and Access Management (IAM) Strategy project will provide a roadmap for implementing a comprehensive and full-featured set of IAM services to encourage collaboration, facilitate stakeholder engagement, and support online interactions with a variety of users, while maintaining the security and integrity of the university's digital assets. To develop this roadmap, the project team will identify key campus IAM business requirements and drivers, research IAM solutions and best practices, and map out the desired future state for IAM at the university.

Business Need and Background

Identity and Access Management (IAM) is the broad set of policies, processes, and technology used to manage digital identity information and to provide these identities with access to approved electronic resources when they need that access. IAM includes:

- Both person and non-person identities (such as organizations and applications/systems)
- The data maintained about these identities and how access to that data is controlled
- The issuance of credentials that can be used to authenticate the identity holder
- The level of confidence the university has in the identity of an identity holder
- Identification of the services an identity is entitled to use and the mechanisms that allow them to securely access those services

The university is faced with the challenge of simultaneously providing greater security for its digital assets and computer systems, while providing a greater and more varied range of online services. The bulk of the university's current IAM services were designed and implemented in the late 1990s and early 2000s. Although this infrastructure has been enhanced over time, these improvements have been implemented in a piecemeal and sometimes uncoordinated manner. As a result, the university's current IAM infrastructure is increasingly unable to keep up with evolving campus requirements (for example, the need for flexible and easy-to-use IAM services for returning populations such as former students as well as loosely affiliated populations such as applicants, seamless integration with externally hosted and "cloud" applications, and robust support for research collaborations using federated identities). The

university needs to establish an overall strategy designed to address campus IAM needs using a coordinated, holistic approach.

Project Description

The Identity and Access Management (IAM) Strategy project will provide a roadmap for implementing a comprehensive and full-featured set of IAM services to encourage collaboration, facilitate stakeholder engagement, and support online interactions with a variety of users, while maintaining the security and integrity of the university's digital assets.

Project Goals

The goals of the IAM Strategy project are as follows:

- Identify key high-level IAM business requirements and drivers
- Research IAM solutions and best practices for meeting business requirements, including benchmarking with peer institutions
- Define the IAM Strategy, which will include:
    - Map of the desired future state for IAM at UT Austin
    - Sequence of solution implementation, addressing priorities and interdependencies
    - Guidelines for solution selection
- Define a long-term IAM governance structure for UT Austin

Schedule and Milestones

Milestone/Deliverable	Target Date
Project Charter	June 2012
Project Plan	July 2012
Project Communication Plan	August 2012
Key High-Level IAM Business Requirements	November 2012
IAM Solutions Research	January 2013
IAM Strategy	May 2013
IAM Governance Charter	May 2013

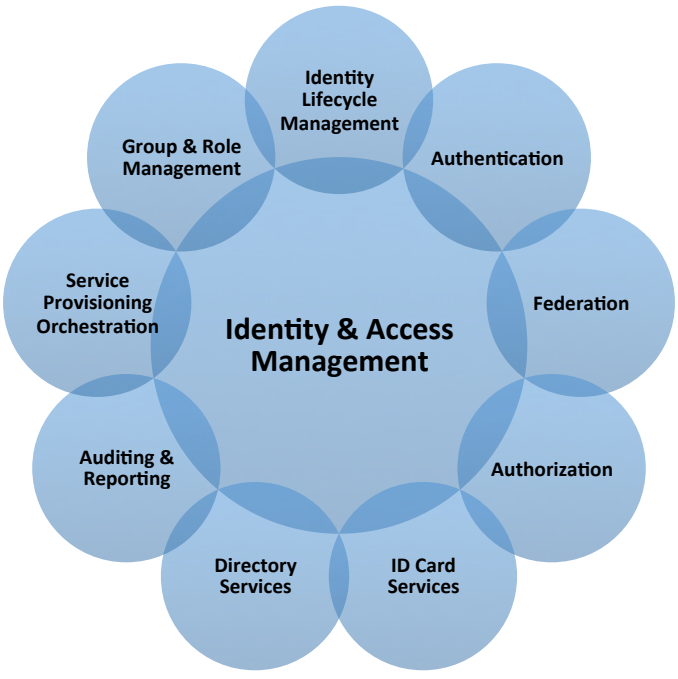
Scope

In Scope

This project will establish high-level business requirements, investigate solutions and best practices for meeting those requirements, and define a strategic roadmap that address the following IAM topic areas:

- **Identity Lifecycle Management** – The management of identity creation, identifier assignment, attribute profiles, identity reconciliation, and authenticators (e.g., passwords, digital certificates).

- **Group & Role Management** – The management of collections of identities that represent groups and roles. Identities can be assigned to groups and roles based on identity attributes, business rules, or on an ad hoc basis.
- **Authentication** – The process of proving that a user or non-person entity (such as a device or application) is who they claim to be, using a password, certificate, or other authenticator. Includes single sign-on, authentication for non-web applications, and multi-factor authentication.
- **Federation** – The implementation of trusted connections to allow UT Austin constituents to use their local identifier (e.g., UT EID) to access resources provided by other institutions and organizations, and to allow authorized users from outside UT Austin to access UT Austin resources using their local identifiers.
- **Authorization** – The process of determining if an individual should have access to a system or function. Includes role-based authorization.
- **Service Provisioning Orchestration** – The coordination of processes that create accounts and grant system access for individuals affiliated with the university, and the revocation of that access when no longer required or appropriate.
- **Directory Services** – Directory services provide a repository of information about identities for use by campus users, services/applications, and the public.
- **ID Card Services** – The provisioning and management of physical UT ID cards, which are used to verify the cardholder's status as a member of the university community and to control physical access to campus facilities (e.g., via BACS – Building Access Control System).
- **Auditing & Reporting** – The collection and storage of IAM-related transactions, and the mechanisms used to analyze and report on those transactions.



Out of Scope

This project will not:

- Develop detailed technical requirements for IAM topic areas
- Develop Request for Proposals for IAM solutions
- Select vendors and/or products for IAM solutions

Project Management and Governance

The project will be sponsored by the Architecture & Infrastructure Committee (AIC). A Customer Steering Committee will be created to provide direct oversight of the project. Membership of the steering committee will be vetted by the AIC and Business Services Committee (BSC).

Role	Names
Executive Sponsor(s)	Ryan Baldwin, AIC chair Brad Englert, CIO
Customer Steering Committee	Cam Beasley, Information Security Office David Burns, McCombs School of Business John Chambers, Computer Science Cesar de la Garza, Development Office Karen DeRouen, Student Accounts Receivable Paul Grotevant, Undergraduate Studies Ladd Hanson, UT Libraries Jimmy Harper, Payroll Services Nathaniel Mendoza, TACC Juan Ortiz, Financial Information Systems Chris Palacios, Procurement & Payment Services Roy Ruiz, TRECS Steve Rung, Office of Admissions Charles Soto, College of Communication Tim Tashjian, Office of the Registrar Greg Baker, ITS Systems Aaron Reiser, ITS User Services
Project Manager	CW Belcher
Project Team	TBD

Assumptions

- Selection and implementation of IAM solutions will be addressed in later phases.
- The Centralized Authentication System Implementation (CASI) project will continue as planned during the development of the IAM Strategy.

Risks

- IAM business requirements may change too quickly for a roadmap to be useful.
- A complete set of requirements may be difficult to develop in a reasonable time period given the diverse and decentralized nature of the university.

- Emerging IAM requirements from the ASMP business area road-mapping process and the development of the Open Systems Technical Environment may require rework of the IAM roadmap.
- Project resources with required skills may not be available or may be diverted to other projects or activities.

Revision History

Version	Date	Description
v1.0	11 Jun 2012	Initial version
v1.1	17 Aug 2012	CSC membership & schedule revisions
v1.2	30 Aug 2012	CSC membership & schedule revisions