Program Name

Identity and Access Management (IAM) Implementation

IAM Executive Sponsors

Jim Livingston

Stephen Hess

Project Scope

Project Description

The goal of this project is to implement an IAM solution to address the University of Utah, Healthcare and Clinics need to manage Identity and Access issues. This project could be implemented in three phases that span over 2 to 4 years. The following describes the three phases of the project. Based on project planning, part of these phases may overlap.

Phase 1 - Identity Provisioning and Administration: During this phase, the University will be implementing technology and modifying business processes to improve the management of identity proofing, provisioning/de-provisioning, and the enforcement of identity policies and procedures. By the end of this phase, the University of Utah, Healthcare and Clinics will have an enterprise-wide process for identity administration, as well as roles and groups management. A process will be created to ensure the mapping of one person to one identity. Finally, one of the goals of this phase is also to deploy a University wide service that provides current data about identities associated with the University. This service will be accessible by downstream systems used for access management and reporting.

Phase 2 – Enhance Access Management: The main goal of this phase is to manage and streamline the authentication, authorization, and identity federation processes across the entire University. An effective Access Management system will reduce the overhead and simplify the integration of new applications and services with these functions. By the end of this phase, the University will be able to streamline identities used to access University services, introduce some type of single or reduced logon service, and improve authentication assurance levels. The University will also simplify its ability to federate with internal and external service providers.

Phase 3 – Identity Business Intelligence and Auditing: The primary goal of this phase is to streamline, automate, and simplify the reporting on identity data. By the end of this phase, the University will have reduced the time and overhead in reporting and responding to audit requests and ensured compliance with regulatory requirements. Many of the auditing and reporting capabilities will be implemented during the first two phases of the project as part of the vended solution(s).

The following tenets provide a foundation for the IAM project implementation. These tenets definition should be reviewed and approved by IAM Governance Steering Committee -

- **Governance**: The IAM Governance structure provides a University wide oversight for the IAM policies and business practices. This includes vetting IAM policies, approving policies and standards exceptions, approving IAM solutions and design with respect to compliance, and conflict resolution for competing IAM strategies at the University of Utah, Healthcare and Clinics

- **Affiliation Management**: Affiliation Management is a University wide authoritative service to provide a list of all active University affiliations (students, employee, alumni, vendors, etc.) at any given moment, and provides a consistent interface to communicate changes to those affiliations. This service provide a foundation for any identity related project including

improved business process for providing University services to users, federation and collaboration with other Universities, access to cloud based services, user personalization, etc.

- **Identity Proofing**: Identity Proofing is the management and tracking of the assurance levels for identities associated with the University. An assurance level, in the context of proofing, specifies the degree to which the stored identity of an individual matches their actual identity. This service is not only critical to managing the risk of conducting electronic business, it is also a requirement for the Higher Education Opportunity and Access (HEOA) law for all Universities that offer distance learning.

- **Identity Provisioning**: Identity provisioning, for the purposes of this project, is the process of creating and maintaining digital or physical credentials (such as a network ID or university identification card) for university affiliates (employees, students, business partners, etc.) and also includes credential suspension, credential resumption, and de-provisioning of credentials. Having a University wide provisioning service for all Identities affiliated with the University will provide a great cost saving, improve users' experience, and most importantly pave the way for Federation/Collaboration between internal and external resources.

- **Identity Business Intelligence**: The Identity Business Intelligence is to provide real-time as well as historical reports with identity related information. The goal is provide answers to critical questions about who has access to what, improve the ability to respond to auditing inquiries, provide information regarding identity regulatory compliance, answer daily security operation questions, and provide other information regarding identities associated with the University.

- **Authentication**: Authentication or logon is the process by which users are challenged to prove their credentials to the system or application they are trying to access. This process can be as simple as providing a user ID and password, or by using multi-factor authentication such as using biometric as well as user ID and password. Authentication is often mentioned in conjunction with Single Sign-On. Single Sign-ON (SSO) is the process by which users are challenged to authenticate once and access multiple applications and systems without being challenged again during the same session. Authentication is important in order to establish trust. Confidence in the true identity of a person (or thing) is critical to most business operations, not to mention privacy laws and national security.

- **Authorization**: Authorization is the process of ensuring that authenticated users have the right privileges (the minimum amount of access required to carry out their assigned duties) to access University resources. Systems and applications use roles, groups, user attributes (information), and direct grants to authorize users to access the various resources. Authorization is important because of business logic. Controlling access to things and auditing permissions is fundamental to most IT operations today.

Preliminary Understanding of Business Need

This project is not only critical for security reasons, improved efficiencies, and cost cutting; it is also critical for the following reasons (for more details on the items below, reference TOGAF Phase C templates):

- **Strategic IT Architecture**
- **Administrative Review & Restructuring (ARR)**
  - Cost Reduction/ Reduce portfolio size where possible
  - Positioning the University to Compete for Major Sponsored Projects
  - Improve Efficiency against Patient Management
- **One person; one identity**
- **Reducing complexity in the provisioning process**
- **Strict ownership of data**
- **User Convenience and Single-Sign on (SSO)**
- **Assurance levels present at several points:**
  - Proofing Assurance defines the confidence in the data in the Person Record.
  - Authentication Assurance defines the confidence in the success of a particular authentication operation.
- **Federation**
- **Compliance**
  - Family Educational Rights and Privacy Act (FERPA)
  - Health Insurance Portability Act (HIPAA)
  - Sarbanes-Oxley/Basel II
  - Red Flags Rule
  - Higher Education Opportunity and Access (HEOA) – Specifically with the new provisions for Distance Learning
  - InCommon
  - Government National Institute of Standards and Technology (NIST) standards
  - Payment Card Industry (PCI) Data Security Standards (DSS)
- **Keep the University Competitive**
- **Reduce Risk**

Project Deliverables and Objectives

Phase 1 - Identity Provisioning and Administration

- Deploy an enterprise wide service for administering person and non-person records and associated group memberships and roles
- Work with the Governance committee to build the business processes for proofing and assurance to implement in the system
- Design identity records in the new system based on business needs
- Implement request system to streamline requests for ID creation (i.e. Guests, etc.)
- Integrate the Identity service with PeopleSoft/EDW/uCard and other data sources to obtain the person data
- Implement vendor product enable IAM Platform to facilitate Identity Administration and Provisioning
    - **Access Request Management** – complete, highly functional user access request management and approval system for use by authorized users to request, modify, or terminate access across various applications.
    - **Access Fulfillment** – automated provisioning/de-provisioning processes for use by authorized users, or triggered from Access Request Manager or authoritative source, to be able to directly provision/de-provision users for a subset of applications
    - **Access Certification**– automated compliance processes for use in the review of current user access and the ability to revoke access no longer required
    - **Password Management** – automated password synchronization and reset self-service processes for user and support staff use
    - **Role Management** – automated enterprise role development processes for use with access fulfillment, and maintenance of enterprise roles defining user access levels for access fulfillment and access certification

Phase 2 - Access Management

- Review existing service(s) for an enterprise Authentication/Access management service
- Implement processes for single and/or reduced sign-on mechanism
- Deploy a coordinated infrastructure for the possibility of multifactor authentication service
- Deploy Web application agent architecture for accessing login service where applicable
- Implement a service for web applications to simplify access to Identity data, roles and group membership
- Implement access policy enforcement service
- Implement SAML based service to allow for identity federation
- Implement a user interface to manage the web logon service across the enterprise
- Create and deploy the business processes for requesting and administering the migration of applications and systems to the new Access Management service
- Implement Access Management Platform facilitate Authentication, Authorization, and Federation

Phase 3 - Identity Business Intelligence (BI) and Auditing

- Work with the Governance and policy group to define the specific reports
- Deploy OLAP, dashboard KPI's, and data mining service provide the needed reports for IAM
- Provide reports on identity provisioning, de-provisioning, and history
- Create real-time triggers for suspected identity theft and security breaches

In Scope

- IAM Platform's (Vendor product) installation and integration with authoritative systems (e.g. PeopleSoft, uCard, Datawarehouse etc)
    - Document criteria used for defining authoritative systems
- Onboarding Process and identity lifecycle management
- Termination Process
- Password management including a central password service (central password policy) and password synchronization across the main password stores at the University of Utah, Healthcare and Clinics :
    - Enterprise LDAP (CAS)
    - Campus Active Directory
    - SRVER Active Directory Domain
    - CSBS Active Directory Domain
    - Standalone PCI Active Directory
- Design a process for managing Non-system affiliates. This will include:
    - The management of identities that are not in an authoritative system, such as for guest accounts, Intensive English Institute, OLLI Scholars, etc.
    - A streamlined repository for storing all identities at the University of Utah, Healthcare and Clinics
    - A process for associating identities with specific affiliation types
    - A process for requesting the addition of new identity types
    - A process for easily requesting access for non-system affiliates
    - An automated process for provisioning identities similar to traditional identities
- Replacement of existing Identity Provisioning/De-Provisioning processes that includes:
    - Identity creation and registration
    - User id creation and access provisioning/de-provisioning
    - ID claiming process
    - Profile registration
    - Access Request System

- Provisioning to University and Campus-wide systems such as:
    - University directories (i.e. Enterprise LDAP, Campus Active Directory etc)
    - Additional provisioning to be included for Email/Exchange, Lync, Epic, Cerner, Citrix
- Identity change processes including changes to Identity affiliation and attributes. This includes changes such as roles, departments, identity information, etc
- Access auditing and compliance control - automated compliance processes for use in the review of current user access and the ability to revoke access no longer required
- Role mining and role management workflows - automated enterprise role development processes for use with access fulfillment, and maintenance of enterprise roles defining user access levels for access fulfillment and access certification
- Review the process for authentication (logon) and managing access to the University systems. This process will include:
    - Review of University-wide authentication infrastructure based on CAS/Shib
    - Implementing a process for requesting and adding new applications to the new authentication system
    - Deploying a single web page where all users are authenticated to use University systems
    - Implementing a process for managing Federation with the University, to be integrated with Shib as the identity provider. The federation implementation will comply with NIST and InCommon
    - Providing the needed training to both system admins and end users to help improve the adoption rate of the new systems
- The provisioning and de-provisioning of Primary Accounts are in-scope
- Implementing Integrated Windows Authentication (IWA) for supported hardware or applications where applicable and allowed by policy

Out of Scope

- Integration with systems other than those listed as in scope for provisioning and de-provisioning of identities
- The provisioning and de-provisioning of administrative/service accounts
- Changing the format of the University ID Number (UNID).
- The decommissioning of University systems whose functionality will be replaced. Such systems may include:
    - Decommissioning Enterprise (EAS) LDAP
    - Collapsing campus Active Directories
    - Decommissioning of SRVER domain
    - Decommissioning of Account Requestor System
    - Decommissioning of Password Program, uNID Retrieval Tool
- Implementing Integrated Windows Authentication (IWA) for non-supported hardware or applications

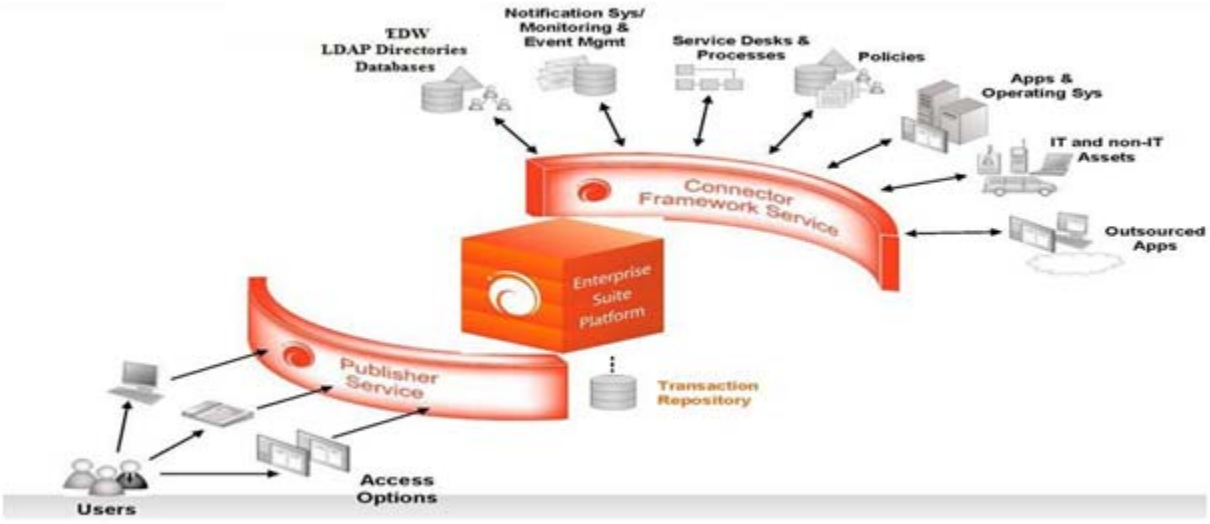
Work and Project Process Description

Preliminary Description of Work

A new system will be implemented during this project. These systems include:

1. IAM Platform - the solution should include the following components:

    - Access Compliance Manager (ACM)
    - Data Access Governance (DAG)
    - Access Request (ARM)
    - Role Manager (BRM)
    - Access Fulfillment Express (AFX) (Provisioning Module)



2. Access Management Platform solution includes the following features:

    - Advanced authentication schemes
    - User entitlement and authorization functionality
    - Single Sign-On
    - Access Federation
    - Access auditing

Project Processes

- A project website has been created for providing project updates
- Documentation will be stored on the website and in SharePoint
- A high level Project plan will be maintained in Clarity so everyone can see the current status
- Resource time will also be tracked in Clarity under the appropriate task
- Once the governance structure has been finalized, determinations will be made on frequency of meetings
- Actions can be taken without meetings and by coordination via email
- Agenda and meeting materials will be provided prior to the meetings at a frequency to be determined
- Issues that arise during the project that require immediate attention can be sent out via email and may require a timely response. If the team feels a meeting is necessary to discuss the issue, a meeting will be scheduled by the project manager
- Action Items, Risks, and Issues will be tracked via an Excel Spreadsheet and reviewed at project meetings

Change Management

Once the project charter is approved and the project planning is underway, all changes to project scope and any significant changes to project budget and schedule must go through the project managers, documented and discussed with the project team. The exact Change Management process will be further defined and shared.

Known Risks

Risk	**Risk Description**	**Impact (How would this risk impact schedule, budget or scope)**	**Likelihood of Occurrence (What is the chance or this risk situation occurring on this project: High/Medium/Low)**	**Mitigation and Contingency Plan (What steps would be taken to avoid the risk? What would be done if it happened?)**
Maturity of solution (e.g., are similar solutions in place elsewhere; specify # of sites and how long the solution has been in use)		Schedule: High / **Medium** / Low Budget: High / **Medium** / Low Scope: High / **Medium** / Low	High / **Medium** / Low	
Institutional commitment and consensus (e.g., management buy-in)	This project has a university wide impact and will require consensus	Schedule: High / **Medium** / Low Budget: High / Medium / **Low** Scope: High / **Medium** / Low	High / **Medium** / Low	Council of CIOs need to meet with all IT departments, Medical Office, Academic Affairs etc.
Aggressiveness of Project Schedule (e.g., how does schedule compare to other installs)		Schedule: High / **Medium** / Low Budget: High / Medium / **Low** Scope: High / **Medium** / Low	High / **Medium** / Low	The UIT/ITS and the Leadership teams in the various departments have to elevate the priority of this project.
Adequate Budget (e.g., budget benchmarked, contingency available)	N/A	Schedule: High / **Medium** / Low Budget: High / **Medium** / Low Scope: High / **Medium** / Low	High / **Medium** / Low	

Complexity (e.g., scale, degree of change required, number of parties involved)	The scope of this analysis project includes multiple components of the infrastructure and will impact large number of departments at the University.	Schedule: High / **Medium** / Low Budget: High / Medium / **Low** Scope: High / **Medium** / Low	High / **Medium** / Low	The scope and requirements have been thoroughly reviewed and vetted. A phased approach with benefits and risks has been documented in section.

Organizational Readiness (e.g., functional staffing, employee attitudes)		Schedule: High / **Medium** / Low Budget: High / Medium / **Low** Scope: High / Medium / **Low**	High / **Medium** / Low	Detailed requirements have been identified in section C and appendix 3
Benefits realization (e.g., will savings materialize and be captured)		Schedule: High / Medium / **Low** Budget: High / Medium / **Low** Scope: High / Medium / **Low**	High / Medium / **Low**	This is an analysis project. The savings will be realized at later stages of the project.
Application Performance (e.g., will system scale to meet demand)	N/A	Schedule: High / Medium / Low Budget: High / Medium / Low Scope: High / Medium / Low	High / Medium / Low	
Other Risk (please specify)		Schedule: High / Medium / Low Budget: High / Medium / Low Scope: High / Medium / Low	High / Medium / Low	

Impact and Dependencies

Impacts:

- Business processes for generating and administering identities for the University.
- CAS / Federation Systems
- ETL based services provided by USS, DW etc
- Active Directory
- Central LDAP
- Epic
- Cerner

Dependencies:

- Active Directory for storing identities
- Business processes for creating and tracking affiliations
- Decisions being made regarding changing or developing business processes

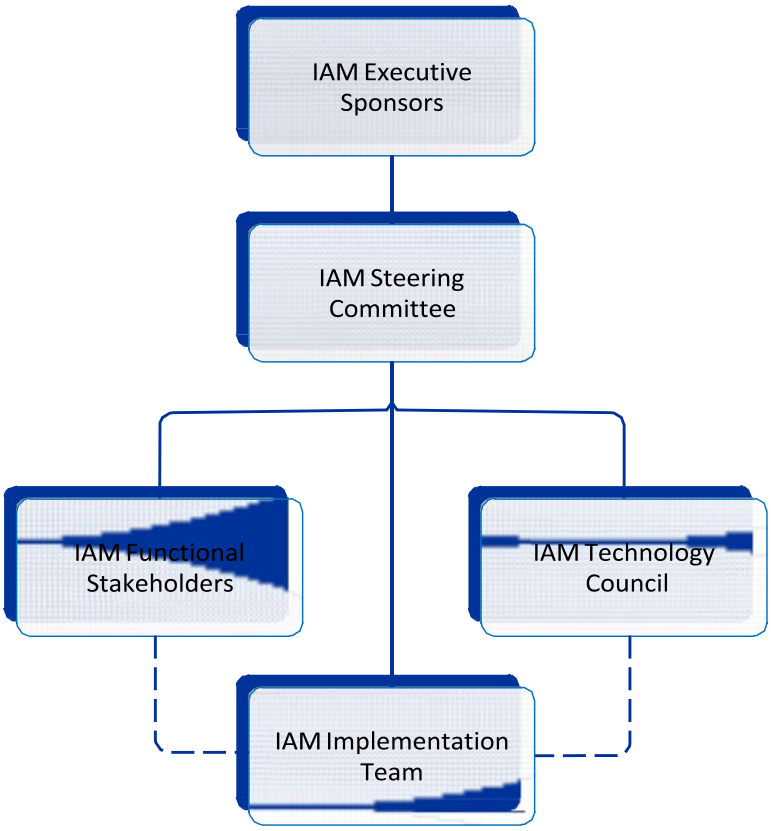
Assumptions

- Resources will be available from all units necessary
- Governance will be in place for making business process decisions
- Business processes will need to change
- ETL based services provided by USS, DW feeds will be replaced with proper architecture
- Not all identity issues will be resolved 100%
- If users change their password in a system other than IAM platform, it will be overwritten.

Initial Project Team

The Full details of the IAM project governance structure are documented in on the following web site: <TBD>

The high level of the project governance structure is depicted in following diagram:



Preliminary Estimate of Project Size

Budget FY 16 is being drafted and would be model against the definition of this charter

Preliminary Cost Benefit Analysis

Tangible benefits to be realized include:

- Manual identity provisioning, de provisioning and proofing
- Establishing streamline processes for Onboarding, Termination, Password Management, Audit enterprise-wide
- Consolidation of the IAM infrastructure and support (including Rebus, Nid Tools etc)
- Address Risk and Compliance on-time needs