IT Architecture and Infrastructure Committee
9:00-10:30am, February 10, 2017, FAC 228D

I. 9:00-9:30 Printing (Eric Hepburn)

II. 9:30-10:00 IAM Modernization Program – Update (CW Belcher, Rosa Harris, Madia McCarthy)

III. 10:00-10:20 Urgent Update (David Pavkovic)

IV. 10:20-10:30 UT Cloud Services Subcommittee – Discussion (Charles Soto)
IAM Modernization Program (IAMMP)/SailPoint Implementation

IT Architecture & Infrastructure Committee
Friday, February 10, 2017

CW Belcher, Associate Director
Joel Guajardo, Senior Business Analyst
Agenda

- IAMMP Background and Approach
- Interface and Data Overview
- Group and Role Management Overview
- Next Steps
- Q&A
IAMMP Background

• The Identity and Access Management (IAM) Strategic Roadmap prioritized the implementation of new enabling technologies to address several functional gaps in IAM services.

• Functional gaps in current IAM services include manual processes, delays in onboarding and poor visibility regarding who has access to what.

• SailPoint IdentityIQ (IIQ) was selected as the software to address those gaps and modernize our IAM services across the University.
IAM Enabling Technologies

Identity Repository
Central directories and repositories of identity information

Authentication
Authentication services for enterprise and cloud applications

Identity Administration
Digital identity management, password management, and identity data provisioning

IAM Services

Authorization and Access Governance
Role-, rule-, and attribute-based authorization management
IAM Enabling Technologies

Identity Repository
TED, AD, etc.
Central directories and repositories of identity information

Identity Administration
SailPoint IIQ
Digital identity management, password management, and identity data provisioning

IAM Services

Authentication
UTLogin/Shib
Authentication services for enterprise and cloud applications

Authorization and Access Governance
SailPoint IIQ
Role-, rule-, and attribute-based authorization management
IAMMP Implementation Approach

The IAMMP work has been organized into three phases based on campus stakeholder input and technical dependencies:

**Phase 1**
2016 – Summer 2017
- Technical Architecture and Environments
- Interface and Data Transition Strategy and Implementation
- Group and Role Management Foundation

**Phase 2**
Fall 2017 – Fall 2018
- Identity Administration and Provisioning
- Password and Credential Management
- Risk-Based Security Controls and Assurance Level Management
- Group and Role Management Expansion

**Phase 3**
2019
- Access Request and Approval Management
- Access Recertification
- Enterprise Authorization Reporting
- Group and Role Management Expansion (continued)
IAMMP Phase 1 Progress

Technical Architecture and Systems Environments
- Built eight environments
- Automated and executed test scripts

Phase 1 Interface and Data Implementation
- Designed Identity Hub components and integrations
- Building Identity Hub components and integrations
- Executing initial testing between SailPoint and Workday

Group and Role Management
- Confirmed early adopters and roles
- Finalized use cases and requirements for basic Group and Role Management functionality
- Designing Group and Role Management functionality and integrations
- Defining the role governance model/process
IT Architecture & Infrastructure Committee

INTERFACE AND DATA OVERVIEW
Phase 1 Identity Hub with Workday

- **TIM Web Apps**
- **Mainframe Authoritative Sources**
- **TIM**
- **Existing Downstream Systems (incl. TED & Austin AD)**
- **Onboarded Disconnected Systems**
- **Onboarded Connected Systems**
- **SailPoint IdentityIQ**
- **Workday**
GROUP AND ROLE MANAGEMENT
OVERVIEW
Group and Role Management Scope

- **Establish**
  - Establish **basic functionality and role governance** model and process

- **Implement**
  - Implement **early adopter roles**

- **Develop**
  - Develop a **role adoption plan** to guide next steps

- **Integrate**
  - Integrate **early adopter applications**

IAMMP – IT Architecture & Infrastructure Committee
IAM Standard Model

The objective of the IAM standard model is to onboard applications and role functionality in a consistent manner, promoting University wide standard policies and procedures for account and access management.
Role Management Use Cases by Phase

Phase 1
- Joiner
- Mover
- Leaver
- Access Request
- Role Maintenance
- Reporting

Phase 2
- Joiner
- Mover
- Leaver
- Access Request
- Role Maintenance
- Reconciliation
- Reporting
- Certification

Phase 3
- Joiner
- Mover
- Leaver
- Access Request
- Role Maintenance
- Certification

Legend
- Initial Limited Functionality
- Full Functionality
Levels of Engagement

Benefits

- Automated provisioning and access control
- Reduced time, effort and errors across access requests, approvals and certifications
- Structured Segregation of Duties with preventative and corrective actions
- Simplified and predictable access control model
- Simplification of responsibilities for an administrator
- Scalable access control
- Accurate reporting of who has access to what

How?

Level 1
- Reporting
- Reconciliation
- Email Notifications

Level 2
- Group Management
- Indirect Provisioning
- Automated Group Assignment

Level 3
- Role Modeling
- Direct Provisioning
- Access Requests
- Certifications
- Direct Connection to SailPoint IIQ via OOTB Connector
- Query TED or AD for Group Membership
- Read-Only Connection to SailPoint IIQ
# Early Adopter Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Organization</th>
<th>Application Type</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>TED</td>
<td>Identity and Access Management</td>
<td>Connected (Direct Connector)</td>
<td>Foundational Application</td>
</tr>
<tr>
<td>Active Directory</td>
<td>ITS Systems</td>
<td>Connected (Direct Connector)</td>
<td>Foundational Application</td>
</tr>
<tr>
<td>MS Office365</td>
<td>ITS Systems</td>
<td>Connected (AD)</td>
<td>Significant impact on manual processes; Birthright for Employees</td>
</tr>
<tr>
<td>TSC Tools</td>
<td>ITS Networking</td>
<td>Connected (TED)</td>
<td>Identified by ITS Networking as in need of a centrally managed authorization system.</td>
</tr>
<tr>
<td>Usher Web Apps</td>
<td>College of Communication</td>
<td>Connected (TED &amp; AD)</td>
<td>Birthright for College of Communication</td>
</tr>
<tr>
<td>ServiceNow</td>
<td>ITS Customer Support Services</td>
<td>Disconnected (Direct Connector)</td>
<td>Strategic Application</td>
</tr>
<tr>
<td>Spectra</td>
<td>UT Athletics</td>
<td>Disconnected (Flat File)</td>
<td>Audit issues with separations</td>
</tr>
<tr>
<td>Wikis</td>
<td>Web &amp; Contract Services</td>
<td>Disconnected (JDBC)</td>
<td>Helps address pain point for separations</td>
</tr>
</tbody>
</table>

2/10/2017

IAMMP – IT Architecture & Infrastructure Committee
Joiner Example

Applies to all Staff Joiners across the University

- BR – All – Current Staff
  - Inherits
- BR – UT Austin – Current Employee
  - Required
- ITR – 0365 – Mailbox Access
  - Assigns
- AD Group - O365 Mailbox

Applies to all Staff Joiners for School of Journalism

- ITR – USHER – JOU Staff
  - Assigns
- AD Group - USHER JOU Staff
  - By virtue of Required IT Role
- TED Group - USHER JOU Staff

By request of TSC Manager for School of Journalism and logging into Wikis

- TED Group - TSC Manager in School of Journalism
  - Wikis - Users Group
NEXT STEPS
Next Steps

• **April** – Group and Role Management Adoption Plan

• **June** – Group and Role Management Go Live for Early Adopters
Questions?
Contact Us

Email:
iammp@utlists.utexas.edu

Web:
https://iamservices.utexas.edu/projects/iammp