Agenda

• Program Status Update

• Discussion Topics:
  – Overview of Sponsored Affiliations
  – New Deceased Status at Person Level
  – SIS-Related Topics

• Questions and Close
Program Status Update

• Program Increment 2 completed – PI-3 starts this week
• In consultation with FAS, decision was made to align HarvardKey rollout strategy closely with the Security campaign launching this fall
  – Provides context for many of the features
• By end of PI-3, features for Alumni rollout will be ready:
  – Alumni registration for HarvardKey via web application
  – Provisioning of Alumni to the new Harvard LDAP instance
  – Authentication for Alumni using HarvardKey
• Continued focus on migrating applications to the cloud
• Database rationalization and migration to the cloud, including SailPoint IIQ
**PI-2 Business Objectives**

Teams accomplished the following objectives:

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Demonstration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement data migration method for Alumni data</td>
<td>• Import Alumni data into Identity Registry (IdDB) using Identity API</td>
</tr>
</tbody>
</table>
| Allow migrated users (Alumni) to claim and manage their HarvardKey credentials | • Self-service Alumni registration for a new HarvardKey  
• Provision accounts and passwords to credential repository (H-LDAP) |
| Support Alumni authentication with HarvardKey | • Authenticate Alumni using HarvardKey |
## PI-2 Business Objectives

Teams accomplished the following objectives:

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Demonstration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace FAS account management and provisioning so that we can decommission Oracle Waveset</td>
<td>Self-Service&lt;br&gt;• Password change&lt;br&gt;• Password reset&lt;br&gt;• Update password recovery email</td>
</tr>
<tr>
<td>Retire technical debt to speed future development</td>
<td>• PIN/CAS to the Cloud?</td>
</tr>
</tbody>
</table>
## PI-2 Business Objectives

### Teams met these additional commitments:

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Accomplishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade SHA algorithm to remain compliant with InCommon Bronze standards</td>
<td>• Upgrade to SHA-2 without any customer application interruption</td>
</tr>
<tr>
<td>Migrate off Oracle Access Manager (PIN3)</td>
<td>• Decommissioned servers in order to save $100K</td>
</tr>
<tr>
<td>Implement new Google API before new students onboard</td>
<td>• Deployed Waveset changes for new Google API design</td>
</tr>
<tr>
<td>Capture HMS functional and technical requirements to facilitate further</td>
<td>• Extensive work from Marlena Erdos</td>
</tr>
<tr>
<td>planning of their migration to SailPoint IIQ</td>
<td></td>
</tr>
</tbody>
</table>
Discussion Topic: POI Creation Follow-Up

Sub-Topic: Sponsored Affiliations

A means to manage information and control access for individuals with affiliations to Harvard other than — or in addition to — their affiliations as students, employees, alumni or library borrowers.
POI Creation Follow-Up: Affiliation Classifications

In this context, an affiliation specifies a person's relationship(s) to Harvard.

HUIT’s broad affiliation classifications include:

• Student
• Employee
• Alumni
• Library Borrower
• Person of Interest (POI)
POI Creation Follow-Up: Roles = Affiliations

*Roles* are the means by which we define an individual’s affiliations with Harvard.

- A person may have multiple roles (e.g. student and employee)
- Role *types* are generic (e.g. student), but a person’s instance of that role relates to a specific school/organization (e.g. FAS Student)
- Access to a School or organization’s resources are based on the type of role plus the faculty code
POI Creation Follow-Up: HarvardKey

A unified credential that enables access to applications and services spanning the entire Harvard Community.

- Includes an individual’s identity information and **roles**
- An individual has one HarvardKey for life
- Evolves over time in tandem with his or her relationship with Harvard
POI Creation Follow-Up: Who is a POI?

Includes all affiliations which are \textit{not} classified as student, employee, library borrower or alumni (e.g. visitor).

- Has the most variation of uses
- Potential for misunderstanding and misuse
- Important to understand the reason, know the person, and control their access
- Most require a sponsor
POI Creation Follow-Up: Sponsored Affiliations

Sponsored affiliations allow Harvard faculty and staff to give individuals outside of their School or organization — or outside of Harvard itself — temporary access to resources within their organization.

- Sponsored affiliations = sponsored POI role types
- Roles must have a sponsor and be renewed
- Sponsors may be held accountable
- May delegate administration to a Sponsor Administrator
- Requires full date of birth or existing HUID
POI Creation Follow-Up: POI Role Types

Current (14)

• Consultant, Contractor, Vendor, Security, Family Member, Tenant, SAO Employee, HMC Employee, Overseer, Retiree, Spouse of Retiree, Retired Hospital Affiliate, Spouse of Retired Hospital Affiliate, and Other

Proposed (9)

• Incoming Employee/Transfer, Collaborator, Visitor, Volunteer, Inter-school Affiliated, Academic Advisor, Field Education Supervisor, Hospital Employee, Course Auditor

*Italic = non-sponsored affiliations*
POI Creation Follow-Up: FAS Sponsored Accounts

Approximately 1,000 FAS sponsored identity accounts are located in Waveset, outside of the HUIT Identity Registry.

• Are all of these sponsored affiliations?
• Map to the sponsored role types: Incoming Employee/Transfer, Collaborator or Visitor
• Administered by the HUIT Accounts Team
• Need DOB and sponsor validations
• To be migrated to the HUIT Identity Registries and provisioned through SailPoint IIQ in 2015
Discussion Topic: New Person Status of ‘Deceased’

• Addition of a deceased flag at person level effective December 2014
• PeopleSoft is the first system to modify its import to set this flag
• Alumni system will update it as well

Discussion: What are the IAM lifecycle ramifications?
Discussion Topic: New Person Status of ‘Deceased’

Issues we have today:

1. Overlaying the identity of a deceased employee with an image of that person’s spouse results in:
   - Untenable confusion for physical access systems
   - Confusing for MIDAS users who see “mismatched” gender and photo

2. Now in conflict with the deceased flag at the person level
   - If we receive an update that a person is deceased, we should not keep the identity going to enable a spouse to have access?

3. Why are we doing it this way?
Discussion Topic: SIS-Related Topics

• New SIS system (Campus Solutions) going live in June
• SIS is the source of student role information for Identity and Access Management
  – Many downstream internal service providers rely on this information to automate access to resources

Tom Mayhew has some discussion topics:

1. Impact of SIS not sending data updates for students who have not been active for the last 90 days … will this uniform approach work?
2. SIS concerned about address object – specifically address Line 3
3. More …?
Thank you!