Identity and Access Management
IAM Lifecycle Committee

November 10, 2014  Monday  10:30 - 12  561 Smith Center
• Short Program Status Update

• User Name Policy Topics Coming to the Fore

• Discussion Topics:
  – User Names
  – POI Roles
  – Related Provisioning Process of Certain Access
  – Data Management Topics

• Closing/Questions or Concerns?
Provisioning stabilization releases completed last week

• Support for advanced features associated with “AD Lockout” use cases
• Ongoing stabilization work and data cleanup tasks
• HMS provisioning of 0365 using the FIM bridge is ready to go live

Current focus is delivery of Program Increment 1

• Preparation for next populations (Alumni, HMS) to be incorporated into the new account management / provisioning (SailPoint)
  – Account claiming proof of concept
• PeopleSoft Import
• New LDAP environment which will be used for Alumni
• Planning for start of Program Increment 2
• Also extensive planning around Office 365 implementation
Consolidation Challenges

• Merging schools into the central identity registry involves
  – Sharing data models
  – Developing processes that work across Harvard
• Consolidating user name space
  – Handling the case where there are two jhill@
• Local process change for the sake of the global Harvard user experience
• Surfaces Data Quality and Data Flow Issues
  – Example: Preferred Name at HMS is a good example of type of issue we may uncover
• When should a POI role be authorized?
• When should it definitely *not* be authorized?
• What are best ways to make the different clear?
• What can we learn from other distributed “identity intake” processes with regard to discouraging gaming the system to enable people to have access to Harvard resources?
Provisioning Process Questions

- In cases where limited access is requested early, how should those processes work so they are reasonable, and not subject to abuse?
- Are there specific cases related to student access between terms for which we need to prioritize solution development?
• Increased demand for distributing data to other systems at Harvard.
  – Do I have any volunteers to work with me on giving a sanity check on proposed criteria?
• Thoughts on how to motivate administrators to maintain phone and other directory data
• Concerns about deleting phone and office address data for employees after they terminate to avoid these data being assumed to still be accurate
  – What do you do in your own systems?
Thank you!
Supporting Materials
Appendix A: IAM Accomplishments to Date

Simplify the User Experience
• Selected and purchased an identity creation toolset that will lead to improved onboarding for all users.
• Implemented a new Central Authentication Service for faster, flexible deployment of applications across Harvard.
• Implemented one-way federation with the Harvard Medical School as proof of concept of credential self-selection by users in order to access services.
• Implemented provisioning improvements that set a foundation for expanded cloud services, support for Active Directory consolidation, and support for email migration.
• Integrated a new ID card application that enables large-scale replacement of expired cards.
• Implemented a new external-facing IAM website for regularly updated information on project purpose and status.
• Migrated University AD users to the SailPoint IdentityIQ provisioning solution.

Enable Research and Collaboration
• Joined the InCommon Federation, enabling authorized Harvard users to access protected material at HathiTrust.
• Enabled access to a planning tool used by Harvard researchers to assist with compliance of funding requirements specific to grants (e.g. NSF, NIH, Gordon and Betty Moore Foundation).

Protect University Resources
• Proposed a new University-wide password policy to the HUIT Security Organization in order to standardize password strength and expiration requirements.
• Drafted a cloud security architecture with the HUIT Security Organization to provide Level 4 security assurance for application deployments using Amazon Web Services.
• Refreshed the AUTH and HU LDAP software and infrastructure to current, supported versions.
• Certified as an InCommon Bronze Identity Provider.

Facilitate Technology Innovation
• Created a conceptual architecture for IAM services to be deployed within the Amazon’s offsite hosting facilities.
• Deployed the Connections directory to the AWS cloud.
The IAM program will be implemented according to the four strategic objectives, and work will be managed as a portfolio of 11 projects:

<table>
<thead>
<tr>
<th>Project</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning</td>
<td>Improves user account management processes by replacing outdated tools with a new, feature-rich solution that can be expanded for local use by interested Schools across the University.</td>
</tr>
<tr>
<td>Federation</td>
<td>Enables Harvard and non-Harvard users to collaborate and easily gain access to both internal and external applications and tools.</td>
</tr>
<tr>
<td>Directory Services</td>
<td>Reduces the number of user-information systems of record while expanding data model and user attributes stored in the central IAM identity repository — enabling quick, consistent, appropriate access across LDAP, AD, and web authentication protocols.</td>
</tr>
<tr>
<td>App Portal</td>
<td>Enables Harvard application owners to learn about and easily integrate applications and software services with central IAM services.</td>
</tr>
<tr>
<td>One-Way Federation</td>
<td>A series of authentication releases and school onboarding efforts that provide Harvard users the flexibility to access applications and services using the credential of their choice.</td>
</tr>
<tr>
<td>Identity &amp; Access Governance</td>
<td>Delivers visibility into IAM program metrics — including in time business intelligence capabilities such as advanced reporting and trend analysis — in support of security requirements.</td>
</tr>
<tr>
<td>Authentication Enhancements</td>
<td>Provides users with a simplified login experience, as well as enhanced security options for sensitive data and applications.</td>
</tr>
<tr>
<td>Authorization Enhancements</td>
<td>Provide application owners and administrators with the ability to manage users via access groups, as well as the ability to manage authorization rules for access to applications or software services.</td>
</tr>
<tr>
<td>External Directories</td>
<td>Securely exposes user identity information inside and outside of the University.</td>
</tr>
<tr>
<td>Expanded Provisioning</td>
<td>Enables identity creation and proofing for non-person users.</td>
</tr>
<tr>
<td>Cloud Migration</td>
<td>Provides the University with a cloud reference architecture for Harvard application deployments, including migrating IAM services from on-premise hosting to Amazon Web Services.</td>
</tr>
</tbody>
</table>