HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

Identity and Access Management
IAM Lifecycle Committee

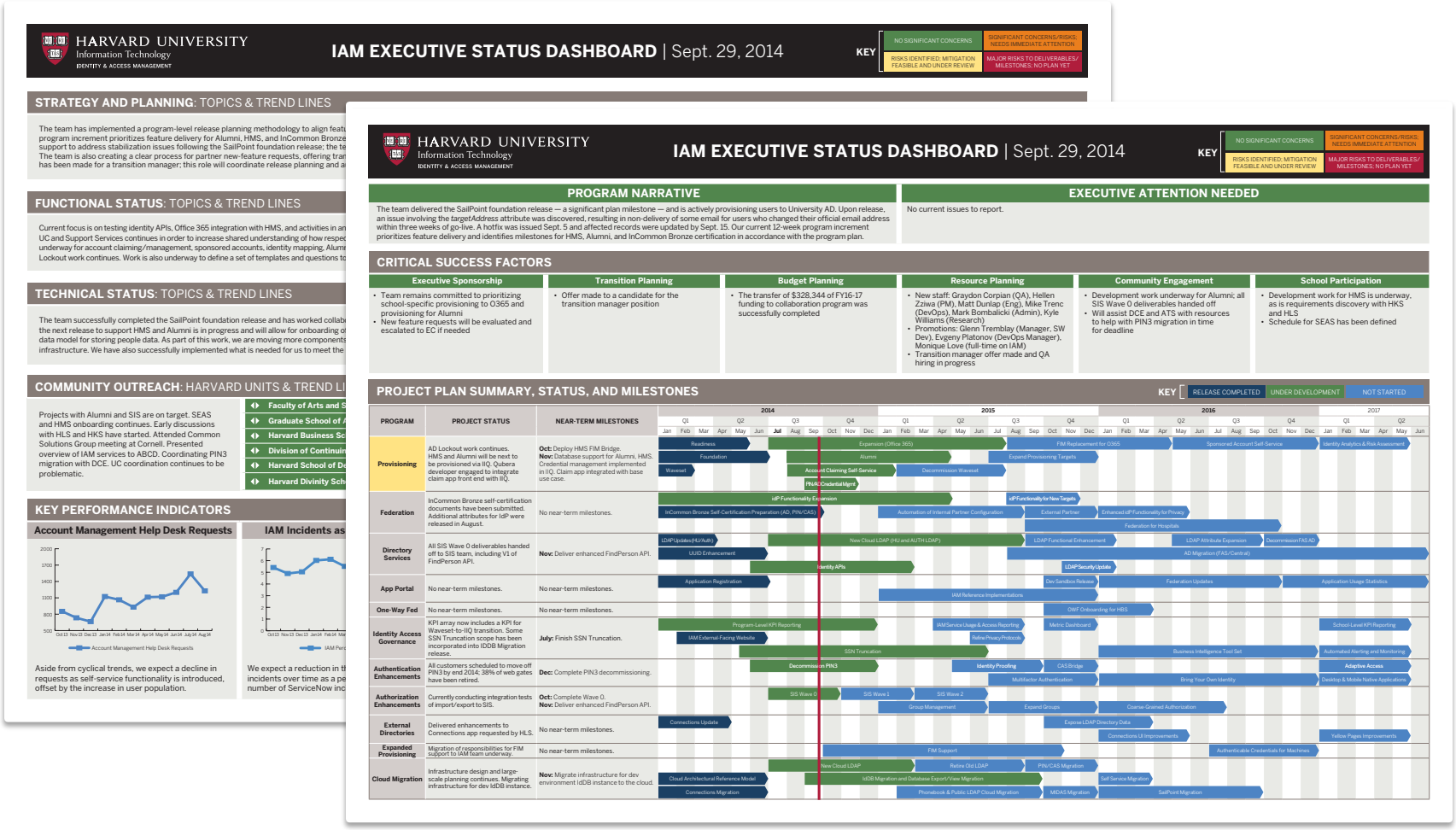
October 1, 2014	Wednesday	11 a.m. – 1 p.m.	6 Story Street

Agenda

- Summary: IAM Program News
- Quick Demo: Connections Feature To Be Added
- Discussion Topics:
  - Latest on Alumni
    - Data Model Overview
    - API instead of batch XML file
  - Review requirements Analysis Template for Onboarding Schools
  - Consolidating Users from the Schools into Identity Management

IAM Executive Status Dashboard

Please see the handout for the most recent version of the IAM Executive Status Dashboard.



HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

IAM EXECUTIVE STATUS DASHBOARD | Sept. 29, 2014

KEY: NO SIGNIFICANT CONCERNS | SIGNIFICANT CONCERNS/RISKS; NEEDS IMMEDIATE ATTENTION | RISKS IDENTIFIED; MITIGATION FEASIBLE AND UNDER REVIEW | MAJOR RISKS TO DELIVERABLES/ MILESTONES; NO PLAN YET

STRATEGY AND PLANNING: TOPICS & TREND LINES

The team has implemented a program-level release planning methodology to align featu
program increment prioritizes feature delivery for Alumni, HMS, and InCommon Bronze
support to address stabilization issues following the SailPoint foundation release; the te
The team is also creating a clear process for partner new-feature requests, offering trar
has been made for a transition manager; this role will coordinate release planning and a

FUNCTIONAL STATUS: TOPICS & TREND LINES

Current focus is on testing identity APIs, Office 365 integration with HMS, and activities in ar
UC and Support Services continues in order to increase shared understanding of how respec
underway for account claiming/management, sponsored accounts, identity mapping, Alumi
Lockout work continues. Work is also underway to define a set of templates and questions to

TECHNICAL STATUS: TOPICS & TREND LINES

The team successfully completed the SailPoint foundation release and has worked collab
the next release to support HMS and Alumni is in progress and will allow for onboarding o
data model for storing people data. As part of this work, we are moving more components
infrastructure. We have also successfully implemented what is needed for us to meet the

COMMUNITY OUTREACH: HARVARD UNITS & TREND LI

Projects with Alumni and SIS are on target. SEAS and HMS onboarding continues. Early discussions with HLS and HKS have started. Attended Common Solutions Group meeting at Cornell. Presented overview of IAM services to ABCD. Coordinating PIN3 migration with DCE. UC coordination continues to be problematic.

- Faculty of Arts and S
- Graduate School of A
- Harvard Business Sc
- Division of Continuin
- Harvard School of De
- Harvard Divinity Sch

KEY PERFORMANCE INDICATORS

Account Management Help Desk Requests

Aside from cyclical trends, we expect a decline in requests as self-service functionality is introduced, offset by the increase in user population.

IAM Incidents as

We expect a reduction in th
incidents over time as a pe
number of ServiceNow inc

HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

IAM EXECUTIVE STATUS DASHBOARD | Sept. 29, 2014

KEY: NO SIGNIFICANT CONCERNS | SIGNIFICANT CONCERNS/RISKS; NEEDS IMMEDIATE ATTENTION | RISKS IDENTIFIED; MITIGATION FEASIBLE AND UNDER REVIEW | MAJOR RISKS TO DELIVERABLES/ MILESTONES; NO PLAN YET

PROGRAM NARRATIVE

The team delivered the SailPoint foundation release — a significant plan milestone — and is actively provisioning users to University AD. Upon release, an issue involving the targetAddress attribute was discovered, resulting in non-delivery of some email for users who changed their official email address within three weeks of go-live. A hotfix was issued Sept. 5 and affected records were updated by Sept. 15. Our current 12-week program increment prioritizes feature delivery and identifies milestones for HMS, Alumni, and InCommon Bronze certification in accordance with the program plan.

EXECUTIVE ATTENTION NEEDED

No current issues to report.

CRITICAL SUCCESS FACTORS

Executive Sponsorship	Transition Planning	Budget Planning	Resource Planning	Community Engagement	School Participation
• Team remains committed to prioritizing school-specific provisioning to O365 and provisioning for Alumni • New feature requests will be evaluated and escalated to EC if needed	• Offer made to a candidate for the transition manager position	• The transfer of $328,344 of FY16-17 funding to collaboration program was successfully completed	• New staff: Graydon Corpian (QA), Hellen Zziwa (PM), Matt Dunlap (Eng), Mike Trenc (DevOps), Mark Bombalicki (Admin), Kyle Williams (Research) • Promotions: Glenn Tremblay (Manager, SW Dev.), Evgeny Platonov (DevOps Manager), Monique Love (full-time on IAM) • Transition manager offer made and QA hiring in progress	• Development work underway for Alumni; all SIS Wave 0 deliverables handed off • Will assist DCE and ATS with resources to help with PIN3 migration in time for deadline	• Development work for HMS is underway, as is requirements discovery with HKS and HLS • Schedule for SEAS has been defined

PROJECT PLAN SUMMARY, STATUS, AND MILESTONES

KEY: RELEASE COMPLETED | UNDER DEVELOPMENT | NOT STARTED

PROGRAM	PROJECT STATUS	NEAR-TERM MILESTONES
Provisioning	AD Lockout work continues. HMS and Alumni will be next to be provisioned via IIQ. Qubera developer engaged to integrate claim app front end with IIQ.	**Oct:** Deploy HMS FIM Bridge. **Nov:** Database support for Alumni, HMS. Credential management implemented in IIQ. Claim app integrated with base use case.
Federation	InCommon Bronze self-certification documents have been submitted. Additional attributes for IdP were released in August.	No near-term milestones.
Directory Services	All SIS Wave 0 deliverables handed off to SIS team, including V1 of FindPerson API.	**Nov:** Deliver enhanced FindPerson API.
App Portal	No near-term milestones.	No near-term milestones.
One-Way Fed	No near-term milestones.	No near-term milestones.
Identity Access Governance	KPI array now includes a KPI for Waveset-to-IIQ transition. Some SSN Truncation scope has been incorporated into IDDB Migration release.	**July:** Finish SSN Truncation.
Authentication Enhancements	All customers scheduled to move off PIN3 by end 2014; 38% of web gates have been retired.	**Dec:** Complete PIN3 decommissioning.
Authorization Enhancements	Currently conducting integration tests of import/export to SIS.	**Oct:** Complete Wave 0. **Nov:** Deliver enhanced FindPerson API.
External Directories	Delivered enhancements to Connections app requested by HLS.	No near-term milestones.
Expanded Provisioning	Migration of responsibilities for FIM support to IAM team underway.	No near-term milestones.
Cloud Migration	Infrastructure design and large-scale planning continues. Migrating infrastructure for dev IdDB instance.	**Nov:** Migrate infrastructure for dev environment idDB instance to the cloud.

Progress Against the Plan: Key Accomplishments

See below for key program accomplishments achieved since the July 2014 IAM Executive Committee meeting:

Project	Release	Description	Plan Date	Actual Date	Impact
Provisioning	SailPoint IIQ Foundation	University AD accounts now provisioned through SailPoint IIQ application	July 2014	Aug 2014	• 631,963 accounts moved off Waveset • HUIT organization, including Help Desk
Federation	InCommon Bronze Self-Certification	Submit Bronze self-certification document to InCommon	Sep 2014	Sep 2014	• InCommon Bronze self-certification complete
Authorization Enhancements	SIS Wave 0	Deploy the FindPerson Identity API to production	Oct 2014	**Sep 2014**	• Enables integration between IAM database and PeopleSoft SIS

SailPoint IIQ Foundation Release: Update and Status

The first production release of SailPoint IIQ was successfully completed August 17.

- University AD accounts for employees and students now managed in SailPoint instead of Waveset
- Successful Fall Start using new provisioning mechanisms, with no major incidents
- Handoff underway to Help Desk for ongoing support

Next steps:

- Support for advanced features associated with “AD Lockout” use cases
- Ongoing stabilization work and data cleanup tasks
- Preparation for next populations (Alumni, HMS) to flow through IIQ

Harvard University Directory Information

The compilation or redistribution of information from Harvard University directories is forbidden.

09/29/14, 07:02 PM

Gleason, Christopher

Email	
Phone	
Location	Harvard Univ Memorial Church Harvard Yard
Title	Counsellor, Denominational
Dept	CADM OPR MEM United Ministry

Gleason, Christopher Scott

Email	gleasonc@wit.edu
Phone	
Location	
Title	Contin Ed/Spec Prog Instructor
Dept	FAS FDCE Other Academic

Gleason, Emily Jean

Email	emily_gleason@hms.harvard.edu
Phone	
Location	Harvard Medical School Genetics, NRB 77 Avenue Louis Pasteur
Title	Research Fellow in Genetics
Dept	HMS Gene

No Image Available

Gleason, Jessica Ann

Email	jagleaso@bidmc.harvard.edu
Phone	
Location	Beth Israel Deaconess Medical Center Anesthesia One Deaconess Rd
Title	Clinical Fellow in Anaesthesia
Dept	HMS Anaesthesia-BIDMC

Gleason, Kelsey M

Email	kmg152@mail.harvard.edu
Phone	
Location	1539 Cambridge St Apt 1
Title	
Dept	

No Image Available

Gleason, Lauren Jan

Email	lgleason@bidmc.harvard.edu
Phone	
Location	Beth Israel Deaconess Medical Center Medicine/LMOB 1B 330 Brookline Ave
Title	Clinical Fellow in Medicine
Dept	HMS Medcn-BIDMC

No Image Available

Gleason, Mark

Email	mark@gleasonclan.com
Phone	

Gleason, Tim

Email	tgleason@camail.harvard.edu
Phone	617-495-5811

Alumni Data Model

- Review Data Model
- Discussion: Adding Alumni roles to MIDAS

Requirements for Onboarding Schools

- Preparing to migrate HMS to Sailpoint for User Management and Provisioning
- Discussion: Review the proposed requirements process

Requirements for Onboarding Schools

- System Landscape
  - Database
  - Input systems
  - Frequency of data flowing
  - Feeds to their target systems
  - Exports
  - All systems that connect
- Business context diagrams
- Stakeholders
  - Groups and how they interface with the data

Requirements for Onboarding Schools

- User Populations being managed
  - With HUIDS
  - Without HUIDS
  - Deeper dive on the people without Harvard IDs that are in their local IDM
    - Who are they
    - What level of detail do they have
    - Who owns the business processes
- Data Models for Populations
- Resource Management Matrix
  - Who gets what!

Requirements for Onboarding Schools

- Sponsored Account Requests
  - People
  - Non-People (Service)
    - Types of services
- Self-Registered Accounts
- Device Management
- Historical use of the Central POI processes
  - POI
  - Library
- Inventory: Existing Onboarding/Request Process Flows for various populations
  - End User Account Requests
  - Account claiming
  - Requesting resources for users
    - Self Service
    - Manager based

Requirements for Onboarding Schools

- Targets Needing Provisioned Data
  - Need schema for any targets
  - If they have any meta data information
- Password related information
  - Password policies and rules
- Username policies
  - Naming conventions (anything you are fussy about)
- School-specific
  - Access Management approaches
  - Use of ‘groups’ to authorize access
  - VIP Exception processes
  - Discuss overlapping credentials for populations
    - Duplicate identities, multiple credentials, etc.

Requirements for Onboarding Schools

- Implementation and Rollout
- Support Services Models
- Communication
  - Stakeholders
  - Channels they typically use
  - Key Contact for developing a plan

- Discussion: Are there major dimensions of this analysis missing from this list?

Consolidation Challenges

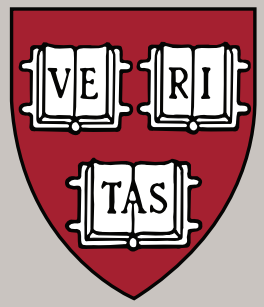
- Merging schools into the central identity registry involves
  - Sharing data models
  - Developing processes that work across Harvard
- Consolidating user name space
  - Handling the case where there are two jhill@
- Local process change for the sake of the global Harvard user experience
- Surfaces Data Quality and Data Flow Issues
  - Example: Preferred Name at HMS is a good example of type of issue we may uncover

Use Case: Preferred Name

- **Background/Issue**: Individuals may optionally use, and display, a different name other than their official name within Harvard systems. This attribute is known as the preferred name, listing name, or display name, depending on the system. The issue is that for HMS, some downstream systems and directories are not displaying an individual's most current preferred name.
- **User Scenario:** An HMS faculty or staff person gets married and submits the paperwork to HR to change both their Official and Preferred name. Once the change is made in PeopleSoft for both name types, the HMS-AD, HMS White Pages and MARS reports display the changed name, but downstream systems such as Canvas do not display the name change. In addition, once the HMS user is migrated from HMS-AD to O365 their display name may revert back to their maiden name.
- **Root Cause:** Although the preferred name attribute value in PeopleSoft is populated out to the HMS Data warehouse, the HMS IDM and eventually out to the HMS-AD, white pages and MARS, the attribute does not auto-populate to the HUIT IDdb or University-AD. Any downstream systems relying on the HUIT IDdb for preferred/listing/display name will therefore, not reflect the change made in PeopleSoft.
- **Mitigation:** An individual's preferred name can be updated manually in the HUIT IDdb via the MIDAS interface accessible by directory services personnel or a departmental directory contact.
- **Solution in Progress:** HUIT IAM is in the process of testing a solution to auto-populate the HUIT IDdb "listing_name" attribute from the PeopleSoft "preferred_name" attribute.
- **Compounding Issue:** While it seems this issue might only affect individuals who choose to use a preferred name in PeopleSoft, it appears that data conversions in the past may have auto-populated the "listing_name" in the HUIT IDdb to be equal to the "official_name". The result is that even individuals who just use their official_name in PeopleSoft may not see their name changes in downstream systems that use the HUIT IDdb "listing_name" attribute over the official_name attribute.

HARVARD

INFORMATION TECHNOLOGY



IDENTITY & ACCESS MANAGEMENT

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.

Appendix B: Project Description Summary

The IAM program will be implemented according to the four strategic objectives, and work will be managed as a portfolio of 11 projects:

Project	Description
Provisioning	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.
Federation	Enables Harvard and non- Harvard users to collaborate and easily gain access to both internal and external applications and tools.
Directory Services	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.
App Portal	Enables Harvard application owners to learn about and easily integrate applications and software services with central IAM services.
One-Way Federation	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.
Identity & Access Governance	Delivers visibility into IAM program metrics — including in time business intelligence capabilities such as advanced reporting and trend analysis — in support of security requirements.
Authentication Enhancements	Provides users with a simplified login experience, as well as enhanced security options for sensitive data and applications.
Authorization Enhancements	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.
External Directories	Securely exposes user identity information inside and outside of the University.
Expanded Provisioning	Enables identity creation and proofing for non-person users.
Cloud Migration	Provides the University with a cloud reference architecture for Harvard application deployments, including migrating IAM services from on-premise hosting to Amazon Web Services.