



HARVARD UNIVERSITY
Information Technology

IAM Operations Transition CIO Council Review

January 23, 2016

Monday

Smith Center 561

2:30 pm - 3:30 pm

Agenda

- Closing Out The Plan
 - Overview of Program Deliverables and Accomplishments
 - Program Impact
- Future State Services
- Transition Strategy
 - Approach and Assumptions
 - Comparison to Peer Institutions
 - Resource Options and Recommendations
- Transition Plan
- Next Steps

Intended Objectives

The purpose of this overview is to identify how the completion of the IAM program impacts IAM operations.

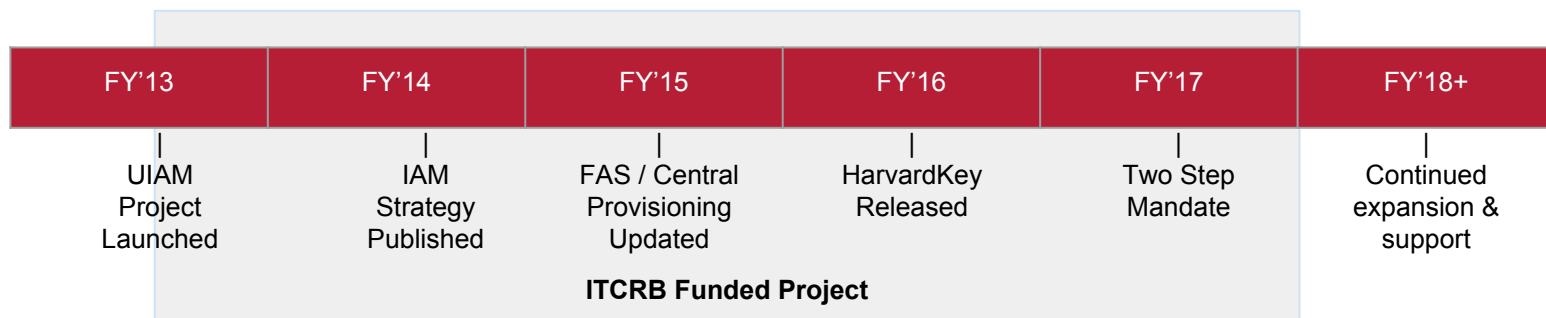
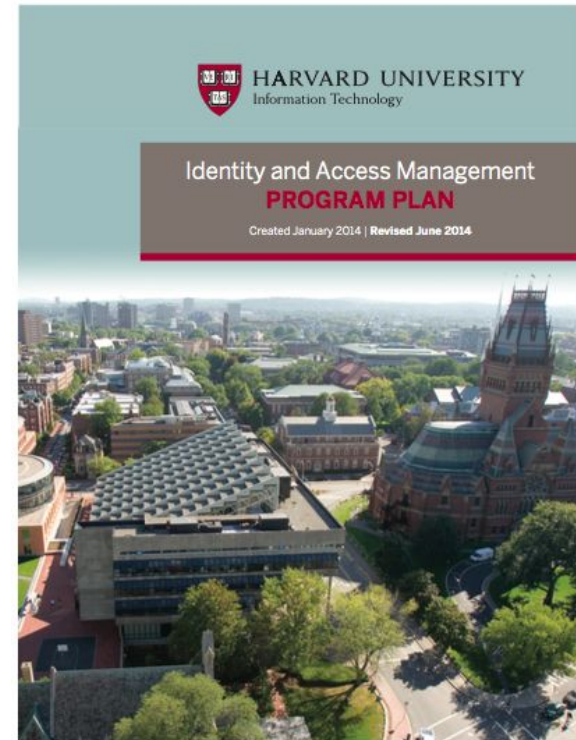
The intended objectives are to:

- achieve a common understanding of what the program has completed and the value it provides
- discuss how IAM's current program state maps to its future operational state
- discuss the future needs for ongoing IAM support

Identity and Access Management Program...

has completed what we set out to do.

- Simplify the User Experience
- Enable Research and Collaboration
- Protect University Resources
- Facilitate Technology Innovation



Achieved Goals and Impact

| IAM Strategic Objectives | Impact |
|--|---|
| Simplify the User Experience | Less passwords to remember... <ul style="list-style-type: none">● One login for life has replaced an average of over 6 logins per user across Harvard |
| Enable Research and Collaboration | Improved access to university resources... <ul style="list-style-type: none">● All schools across Harvard are integrated with common user identities that enable University email, HarvardPhone, and over 2,000 other applications |
| Protect University Resources | Better security... <ul style="list-style-type: none">● University-wide adoption of standardized and improved passwords with associated two factor authentication dramatically increases security |
| Facilitate Technology Innovation | Improved participation in higher education community... <ul style="list-style-type: none">● Improved sponsored guest accounts and external federation allow external researchers and university staff to collaborate quickly |

Before IAM - The bad old days

“Onboarding” happened after you were already here



- You didn't know your ID number or how to get an account
- Then you had to get your PIN in order to get your desktop login
- But first, we needed to give you your email, so you could get the PIN

You had too many accounts, and never knew which one to use



- PIN, Desktop, Email, MeetingMaker, Sharepoint, Google

You logged into accounts with different usernames & passwords



- The passwords had different rules and expired on different timeframes
- You had to call the SupportDesk in tears because you couldn't make a password with the PIN system that worked.
- And while you were guessing what your password was, you locked yourself out.

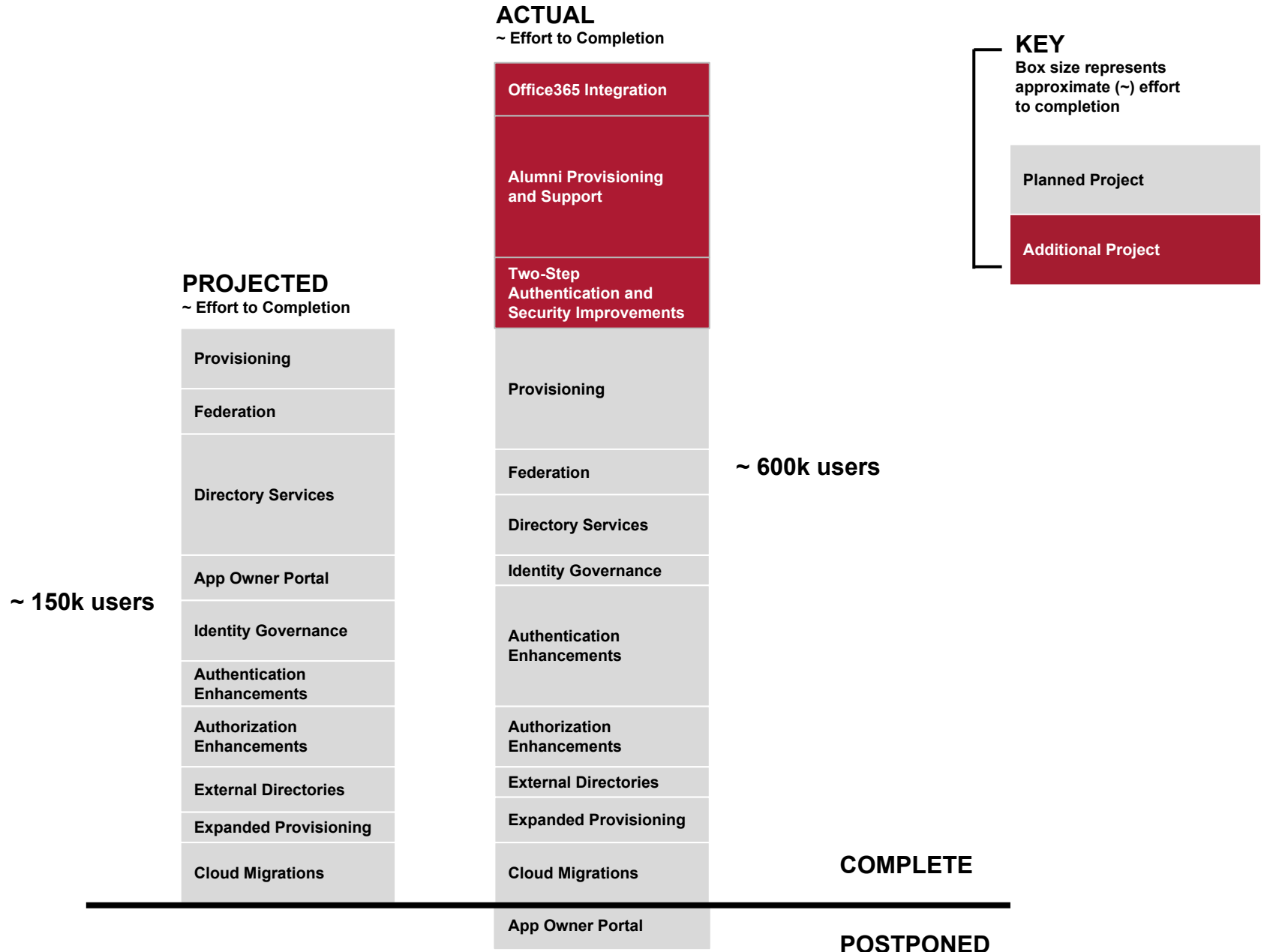
And as you walked off the stage with your hard-earned diploma, Harvard asked you to register for a new account.

“Imagine If...”

At the onset of the IAM project, we imagined a list of key ideas that represented an ideal state for our stakeholder groups. This is how we did:

| Stakeholder | Imagine If... | Outcome | Solution Implemented |
|--------------------------|---|-----------------|--|
| Faculty and Staff | <ul style="list-style-type: none"> • Faculty and staff could access information and perform research across schools and with other institutions without having to use several sets of credentials. • Faculty and staff could manage their own accounts and sponsor others through a centralized web applications. | COMPLETE | <ul style="list-style-type: none"> • Harvard has Federated with InCommon to allow for resource access across other Higher Ed institutions using Harvard credentials • Sponsored Account process automated and distributed across the University to allow for self-service management of Harvard partners |
| Students | <ul style="list-style-type: none"> • Students could choose to use their home school credentials to login into applications across the University. • Students could keep using the same set of credentials after they graduate. | COMPLETE | <ul style="list-style-type: none"> • HarvardKey credentials aligned to University affiliations with ability to choose login name • One HarvardKey for life for all Harvard affiliates including Students / Alumni |
| Technical Staff | <ul style="list-style-type: none"> • Automated provisioning could reduce the burden on IT staff and increases the security posture of the University. • Application teams could easily integrate Harvard users with internal and external applications. | COMPLETE | <ul style="list-style-type: none"> • Automatic provisioning of access based on users' University affiliations • Over 2000 applications integrated with HarvardKey |
| External Users | <ul style="list-style-type: none"> • External users could access Harvard applications using credentials native to their home institution. | COMPLETE | <ul style="list-style-type: none"> • External access to Harvard resources based with either federated login or sponsored accounts |

Evolving Program Focus



Business Value Achieved

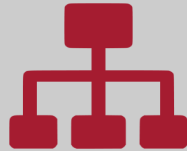
Please refer to the handout

| IAM PROGRAM | 2014 | | | | | | | | | | | | 2015 | | | | | | | | | | | | 2016 | | | | | | | | | | | | 2017 | | | | | |
|-----------------------------|---|-----|-----|-----|-----|-----|---|-----|-----|-----|-----|-----|--|-----|-----|-----|-----|-----|--|-----|-----|-----|-----|-----|--|-----|-----|-----|-----|-----|---|-----|-----|-----|-----|-----|------|-----|-----|-----|-----|-----|
| | Q1 | | | Q2 | | | Q3 | | | Q4 | | | Q1 | | | Q2 | | | Q3 | | | Q4 | | | Q1 | | Q2 | | | | | | | | | | | | | | | |
| | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun |
| SailPoint | Simplify Account Management: Users will be able to change passwords on multiple key target systems (PIN, Exchange, Google Apps) via a single operation. ✓ | | | | | | Reduce Manual Processes for Guest Sponsorship: Shift manual creation of a sponsored guest from administrators of identities to end-users; allow sponsors to directly manage guest's identity and access. ✓ | | | | | | Simplify Role Transitions: Resources that have transitioned from one role (e.g. contractor) to another (e.g. employee) will retain key accounts and access to resources without requiring complex migration. ✓ | | | | | | Expand Access to Resources (Resource Catalog): Using SailPoint, users will be able to see what applications they have access to and which applications they can request access to. ✗ | | | | | | Expand Access to Resources (Email): Users will be able to find contact and calendar (e.g. free/busy) information for users across all participating Harvard Schools. ✓ | | | | | | Increase Self Service: Users will be able to make account management updates and request access to resources directly via a portal, rather than going through the help desk. ✓ | | | | | | | | | | | |
| | Simplify User Access Management: Simplify the process for requesting access for users. ✓ | | | | | | Quickly Revoke User Access: Remove end-user access across resources in a streamlined fashion; reduce administrative touchpoints to removing user access. ✓ | | | | | | Reduce Local Administrative Overhead: Enable provisioning of users to local applications, enabling easier management of access privileges to Harvard resources. ✓ | | | | | | Reduce Number of User Management Toolsets: Enable a person administrator to provide users access across directory stores via a single tool. ✓ | | | | | | | | | | | | | | | | | | | | | | | |
| Federation | | | | | | | | | | | | | Expand Access to Resources: Users will be able to access an increasing number of internal resources via InCommon and IAM relationships with Harvard communities. ✓ | | | | | | Expand Access to Resources: Users will be able to access an increasing number of internal resources via InCommon and IAM relationships with Harvard communities. ✓ | | | | | | | | | | | | | | | | | | | | | | | |
| Directory Services | Match Identities Across Domains: Expand the number of attributes — including adding a unique identifier — to correlate identities across federated systems. ✓ | | | | | | Improve Security Posture of IAM Services: Retire end-of-life applications that do not provide the needed provisioning and authentication services. ✓ | | | | | | | | | | | | Incorporate Discoverability: Incorporate the use of researcher identities into directory services to enable global tracking of authorship of published resources. ✗ | | | | | | | | | | | | | | | | | | | | | | | |
| App Portal | Simplify Application Setup: Provide application owners with an online portal that will lead them through the process of integrating their application with IAM services. ✓ | | | | | | Reduce Security Development Burden: Provide standard authentication libraries to application owners to reduce the likelihood of errors resulting in duplicate development efforts. ✓ | | | | | | Reduce Complexity of IAM Integration for Cloud and Third Party: Define a standard set, based upon InCommon, of identifiers and attributes about Harvard users. ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| One-Way Federation | Expand Access to Resources (Central): Users will be able to access PIN-authenticated central applications using local school credentials instead of HUD. ✓ | | | | | | Improve Collaboration Across School Boundaries: Allow use of local school credential to access data and applications across the University. ✓ | | | | | | Allow Choice of Credentials: Users will be able to use a single preferred login and password to access an increasing number of applications both internal and external to the University. ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Identity Access Governance | | | | | | | | | | | | | | | | | | | Improve Situational Awareness: Perform automated alerting and take actions to remediate harmful activity without requiring human intervention. ✓ | | | | | | Improve Visibility into Application Access: Offer guidance and libraries to provide advanced auditing and logging functionality including the capability to track user activities within applications. ✗ | | | | | | Limit Unauthorized Access to User Data: Introduce alerting of unusual access patterns and other security events to limit unauthorized access to user data. ✓ | | | | | | | | | | | |
| Authentication Enhancements | | | | | | | | | | | | | Reduce Number of Logins: Users will see fewer requests to log in after accessing an application, and then another application. ✓ | | | | | | Reduce Risk of Identity and Account Compromise: Implement multifactor authentication to provide additional security assurance. ✓ | | | | | | Enable Choice of Identity: Allow users to use their personal identities from social media to access Harvard resources. ✗ | | | | | | Reduce Administrative Overhead and Development Time: Mobile app owners will be able to integrate with Harvard credentials using CAS/PIN. ✓ | | | | | | | | | | | |
| Authorization Enhancements | | | | | | | | | | | | | Simplify Administration of Groups of Users: Allow admin changes to affect a set of users rather than forcing separate operations and updates for each user. ✓ | | | | | | Simplify Application Administration: Provide a central IAM authorization service to manage coarse-grained access control, and expose an enhanced set of attributes to determine appropriate access control. ✓ | | | | | | Expand Integration with Desktop: Streamline user login experience to workstation and desktop applications. ✗ | | | | | | | | | | | | | | | | | |
| External Directories | | | | | | | | | | | | | Improve Security of Information: Leverage identity assurance attributes for increased confidence in a user's identity. ✓ | | | | | | | | | | | | Expose Departmental Information: Create a new Web application that provides an advanced internal directory of departmental information. ✗ | | | | | | | | | | | | | | | | | |
| Expanded Provisioning | | | | | | | | | | | | | | | | | | | | | | | | | Improve Security of Machine-to-Machine Communication: Validate that nonstandard users (e.g. user community), resources (e.g. microscopes) and protocols receive proper authentication credentials when acting as initiating machines. ✗ | | | | | | | | | | | | | | | | | |
| Cloud Migration | Provide Best Practices: Provide guidance, best practices, and lessons learned to future implementers of Amazon Web Services cloud application hosting at Harvard. ✓ | | | | | | Reduce Development Costs: Reduce the costs associated with infrastructure deployment by taking advantage of the cloud's economies of scale. ✓ | | | | | | Improve Reliability of IAM Services: Leverage Amazon Web Services to provide hosting for IAM Services, increasing the agility of service enhancements and improving uptime for application authentication services. ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

IAM by the Numbers



160,000+
HarvardKeys
claimed



Over 2700
applications
protected by
HarvardKey



28k tickets
processed
by IAM
in 2016

Reduction by 75% of
compromised accounts
due to Two-Step



31k Office365
mailboxes enabled
by HarvardKey



80,000 unique users
login per month



IAM Services / Organization

Future State Services and Offerings

| Current Service | # offerings |
|---|-------------|
| End User Computing | |
| Collaboration Services | 3 offerings |
| Email and Calendars | 6 offerings |
| Field Support Services | |
| Network Services | |
| Phone Services | |
| IT Provider Services | |
| Cloud Services | |
| HUIT Support Tools and Systems | |
| Identity and Access Services | 4 offerings |
| Network Services | |
| Phone Services | |
| Server Administration | |
| Web Hosting | |
| IT Security | |
| Information Security Education and Consulting | |
| Information Security Operations and Engineering | |

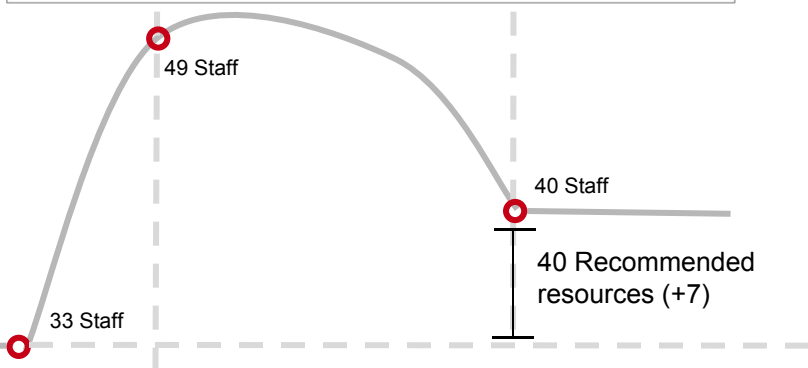
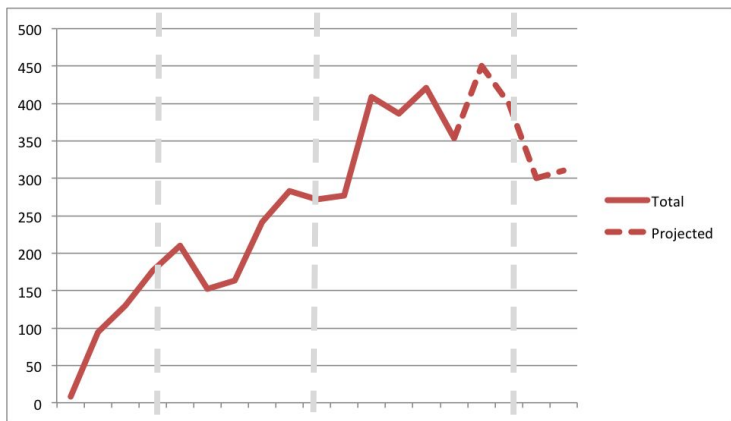
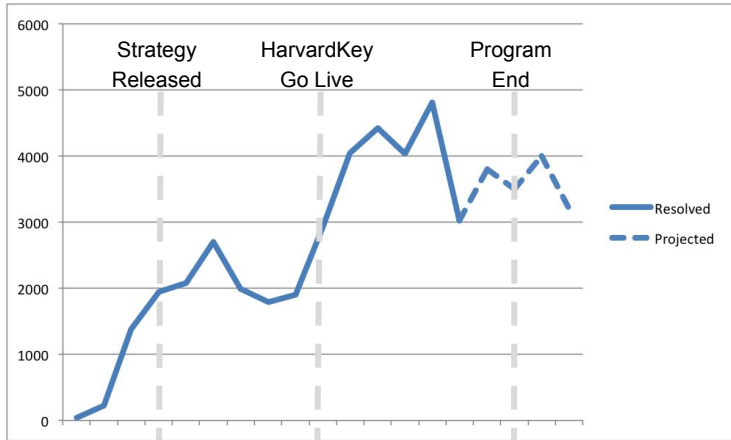
| Future Service | # offerings |
|---|-------------|
| End User Computing | |
| Collaboration Services | 3 offerings |
| Field Support Services | |
| Network Services | |
| Phone Services | |
| IT Provider Services | |
| Cloud Services | |
| HUIT Support Tools and Systems | |
| Identity and Integration Services | 3 offerings |
| Network Services | |
| Phone Services | |
| Server Administration | |
| Web Hosting | |
| IT Security | |
| Information Security Education and Consulting | |
| Information Security Operations and Engineering | |

13 Services Offerings → 6 Services Offerings

| FUTURE OFFERINGS | |
|--|---|
| Collaboration Services <ul style="list-style-type: none"> Account and HarvardKey Services Email and Calendar Groups and Guests | Identity and Access Integration Services <ul style="list-style-type: none"> Identity Data and Provisioning Identity Repositories Authorization Services |

See Appendix A: Service Taxonomy for more details

Capacity Analysis



Operational

- IAM serves as a critical path function for thousands of applications and every user at the University
- Assumption: Consistent Operational demand in FY'18 due to widespread adoption and continual growth due to Alumni, new University affiliates, security enhancements, and group services

Development

- New feature development has greatly increased during the program
- IAM has a backlog of development work required to meet University demand

Staffing Recommendation

- Reduce 16 Project Staff by 65% and convert 7 existing project staff
- Split IAM into two teams aligned to service structure: User facing and Integration (backend)

Development Roadmap

| FY 2018 | | | | FY 2019 | | | | FY 2020 | | | |
|--|----|--|----|---------------|----|--|----|--|----|-----------------------|----|
| Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| Provision HKS | | Provision HMS InCommon federation with hospitals | | | | HarvardKey Self Service Improvements - XID | | Migrate legacy AuthProxy and PIN customers to CAS or IDP | | | |
| Decommission remaining on-premise servers | | | | Replace Midas | | Group Services Expansion | | Self Service Sponsored Guests | | HU-LDAP Consolidation | |
| Replace and modernize IAM Import/Exports with APIs | | | | | | | | | | | |

FY'18 - 20 Development Priorities

Security

- Continued implementation of University Security policies and practices

Complete Cloud Migrations

- Migrate remaining on-prem servers to the cloud to meet University goals and significantly reduce \$70k monthly server spend

Modernization

- Upgrade IAM tools and features to meet growing University needs (e.g. PeopleSoft upgrade, University data integration, APIs)

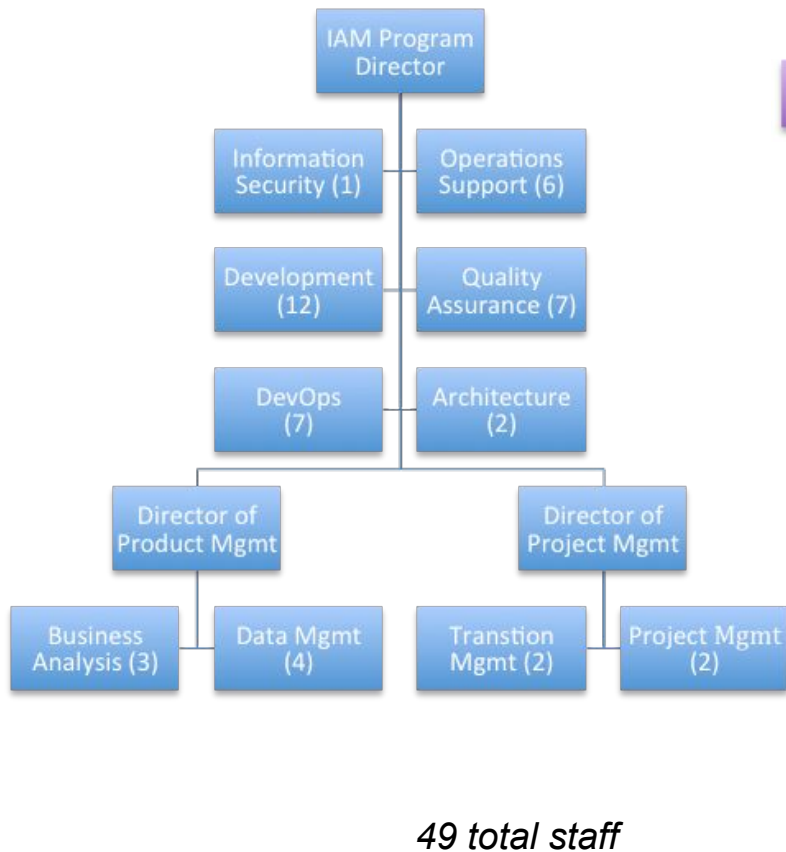
School Adoptions

- Continue IAM expansion to additional schools such as HKS, HLS, and HMS

See Appendix B: Service Roadmap for more details; and Appendix C for other ITCRB projects that may impact roadmap

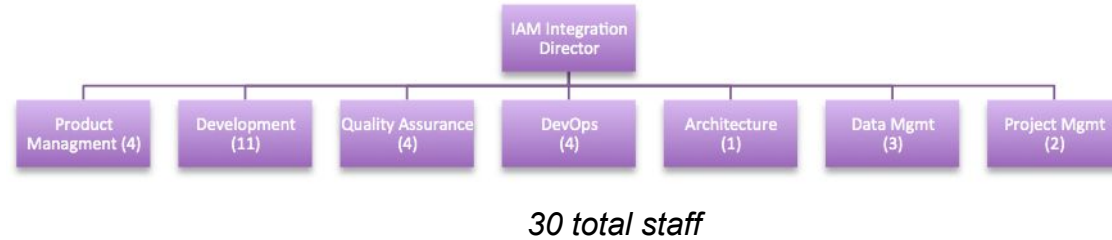
Proposed Organizational Transition

Current State

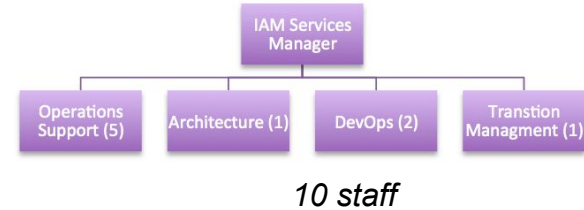


Operational State

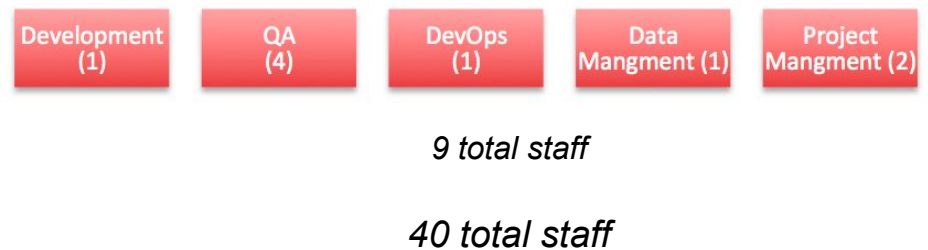
Identity and Integration Services



Collaboration Services



Expired Positions



Transition Plan

- 1. Simplify Service Definitions (through March 2017)**
 - a. Communicate transition to customers and IAM partners
 - b. Partner with ITSM to adjust service catalog for IAM services

- 2. Align Organization (through June 2017)**
 - a. Transition to the service based structure
(Collaboration Services and Identity and Integration Services)
 - b. Adjust budgets to align with organizational structures

- 3. Growing T-Shaped Professionals (through FY'18)**
 - a. Transition IAM teams from CTO Office to operating organizations
 - b. Realign positions where necessary to address gaps
 - c. Distribute specialized functionalities across team: DevOps/Support, Project Management, Product Management

Next Steps

- Integrate operational approach and financial plan
- Communicate approach to teams and customers
- Define separate Duo operational funding model with Security
- Realign organization and services to match vision
- Adjust budgets to align with new organizational structure
- Refine job descriptions where necessary to address gaps and future needs
- Execute organizational transition plan

Thank You / Questions

Appendix

Appendix A: Service Taxonomy

| Services | Service Offerings | Offering Components |
|--|---------------------------------|---|
| Collaboration Services | Account and HarvardKey Services | <ul style="list-style-type: none"> • HarvardKey self service • User identity and accounts • Service and resource accounts • Two step verification |
| | Email and Calendar | <ul style="list-style-type: none"> • Office365 email and calendar • Google apps for Harvard • Mailing lists • Active directory |
| | Groups and Guests | <ul style="list-style-type: none"> • Web conferencing • Document and file sharing • Group and list services • Sponsored affiliates and guests |
| Identity and Integration Services | Identity data and provisioning | <ul style="list-style-type: none"> • Account provisioning / deprovisioning • Identity data and registry • Identity data integration |
| | Identity Repositories | <ul style="list-style-type: none"> • Identity targets (LDAP) • Connections and white pages |
| | Authorization Services | <ul style="list-style-type: none"> • Application authorization • Federation • Backend group creation and maintenance |

Appendix B: Service Roadmap

In Scope

- Group Services Expansion
- Registry Data Services
 - CDPL replaced with APIs
 - Replace Midas
 - Replace existing Import processes
 - Replace existing Export processes
 - Decommission remaining on-premise servers
- Directory Consolidation: HU-LDAP
- HarvardKey Self Service Improvements
- HMS Provisioning to AD
- InCommon federation with hospitals if requested
- Migrate AuthProxy and PIN customers to CAS or IDP
- Replace XID functions with Self Service Sponsored Guest request process

Out of Scope

- FAS AD Consolidation
- Modernize the Identity Registry to an Entity Registry for non-people based accounts (ITCRB)
- FAS LDAP Modernization
- Replace Alias Manager
- Decommission FIM
- Replace Public LDAP
- Replace Dionysus
- Provisioning users to additional targets
- OpenID Connect
- End user self-managed groups for personal use
- Application owner self service
- Resource/service account self service
- Metrics dashboard
- IAM Analytics
- Privileged Account Management

Note: There will be customer impact and costs when customers are asked to migrate from decommissioned and consolidated services

Appendix C: Outstanding ITCRB Requests

IAM has partnered with several other initiatives to support ITCRB requests for FY'18 and beyond that would impact the proposed Service Roadmap.

| FY18 Request | Value to University | Impact on Roadmap |
|---|---|---|
| <p>University Data Services: <i>Entity Registry</i></p> | <ul style="list-style-type: none"> • Simplified integration with IAM data to enable service delivery • Faster time to delivery for projects • Improved security through expanded identity tracking | <ul style="list-style-type: none"> • Ability to expand scope of managed accounts to non-people resources • Retire outdated legacy applications |
| <p>Broadcast Communications: <i>Group/List Integration</i></p> | <ul style="list-style-type: none"> • Consistent data for communication • Increase reach of emergency communication • Alignment with policy and improved compliance | <ul style="list-style-type: none"> • Integrated communication tools with group service • Expand HarvardKey self-service to transition to opt-out model for emergency comm's |
| <p>Security Initiatives: <i>Active Directory</i></p> | <ul style="list-style-type: none"> • Close security gaps that put Harvard and individual users at risk | <ul style="list-style-type: none"> • Enhanced Active Directory (AD) security and new procedures |