A CASE OF IDENTITY

Building Solutions to Assist

HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

WHAT IS IDENTITY & ACCESS MANAGEMENT?

Identity and access management (IAM) technologies and services enable the right individuals to access the right resources at the right times for the right reasons.

We all use IAM solutions many times a day:

- Logging in to websites, servers, and other resources
- Accessing research materials at Harvard and beyond
- Checking a colleague’s calendar for a meeting
- Adding, removing, or changing employee records

At Harvard, the IAM program exists to streamline these interactions and make it easier for you to do your day-to-day tasks.

WHAT IS IDENTITY & ACCESS MANAGEMENT?

Our vision: Provide users, application owners, and IT administrative staff with secure, easy access to applications; solutions that require fewer login credentials; the ability to collaborate across and beyond Harvard; and improved security and auditing.

Objectives

Simplify User Experience

Simplify and improve access to applications and information inside and outside of the University

Enable Research & Collaboration

Make it easier for faculty, staff, and students to research and collaborate within the University and with other institutions

Protect University Resources

Improve the security stature of the University via a standard approach

Facilitate Technology Innovation

Establish a strong foundation for IAM to enable user access regardless of new and/or disruptive technologies

Guiding Principles

Harvard Community needs will drive our technology

Tactical project planning will remain aligned with the program's strategic objectives

Solution design should allow for other Schools to use foundational services to communicate with the IAM system in a consistent, federated fashion

Communication and socialization are critical to our success

Key Performance Indicators

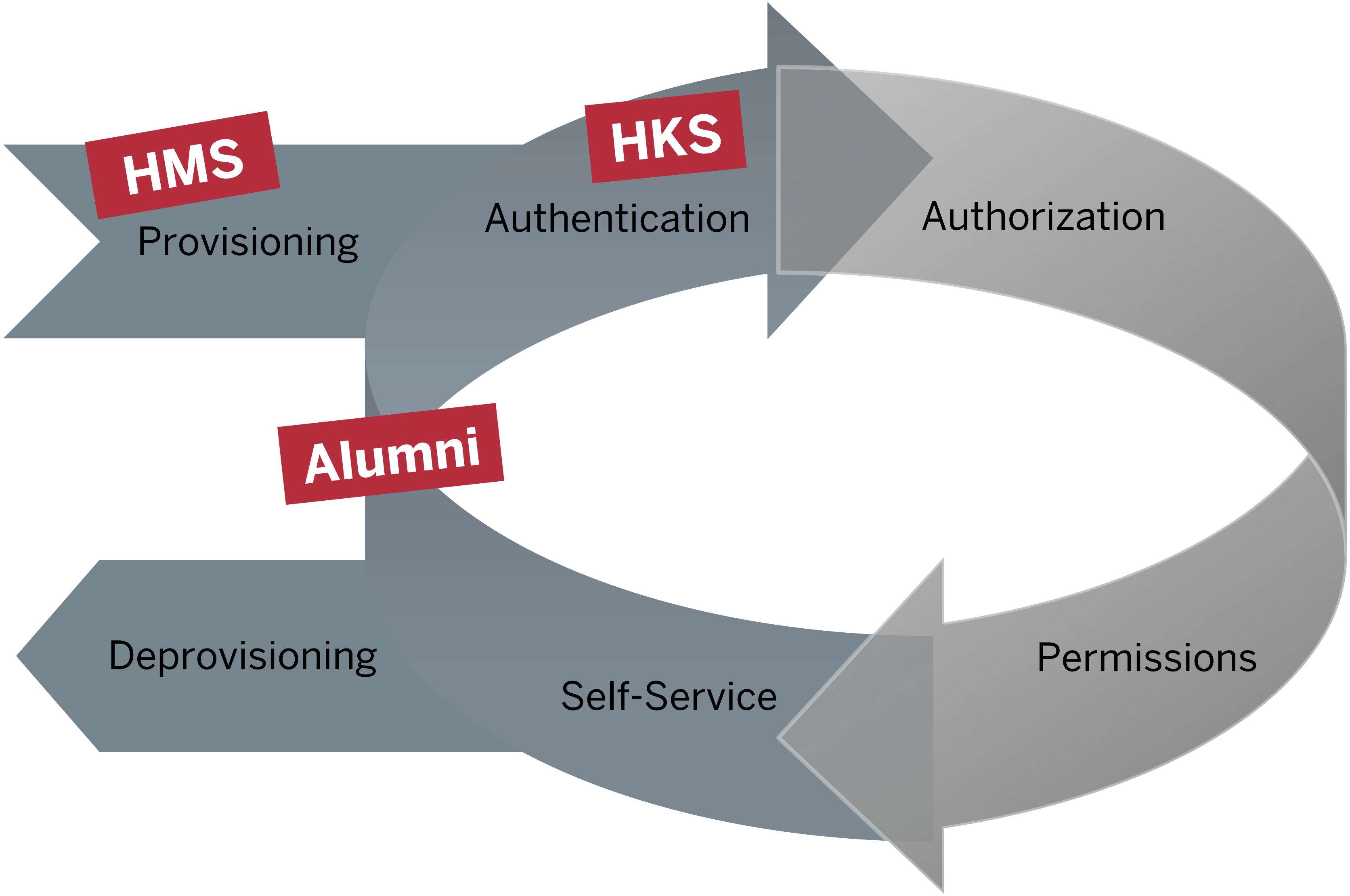
Monthly number of help desk requests relating to account management

Monthly number of registered production applications using IAM systems

Monthly number of user logins and access requests through IAM systems

Monthly number of production systems to which IAM provisions

ABOUT THE IDENTITY LIFECYCLE



ABOUT PROVISIONING

Provisioning and deprovisioning are key to the IAM program:

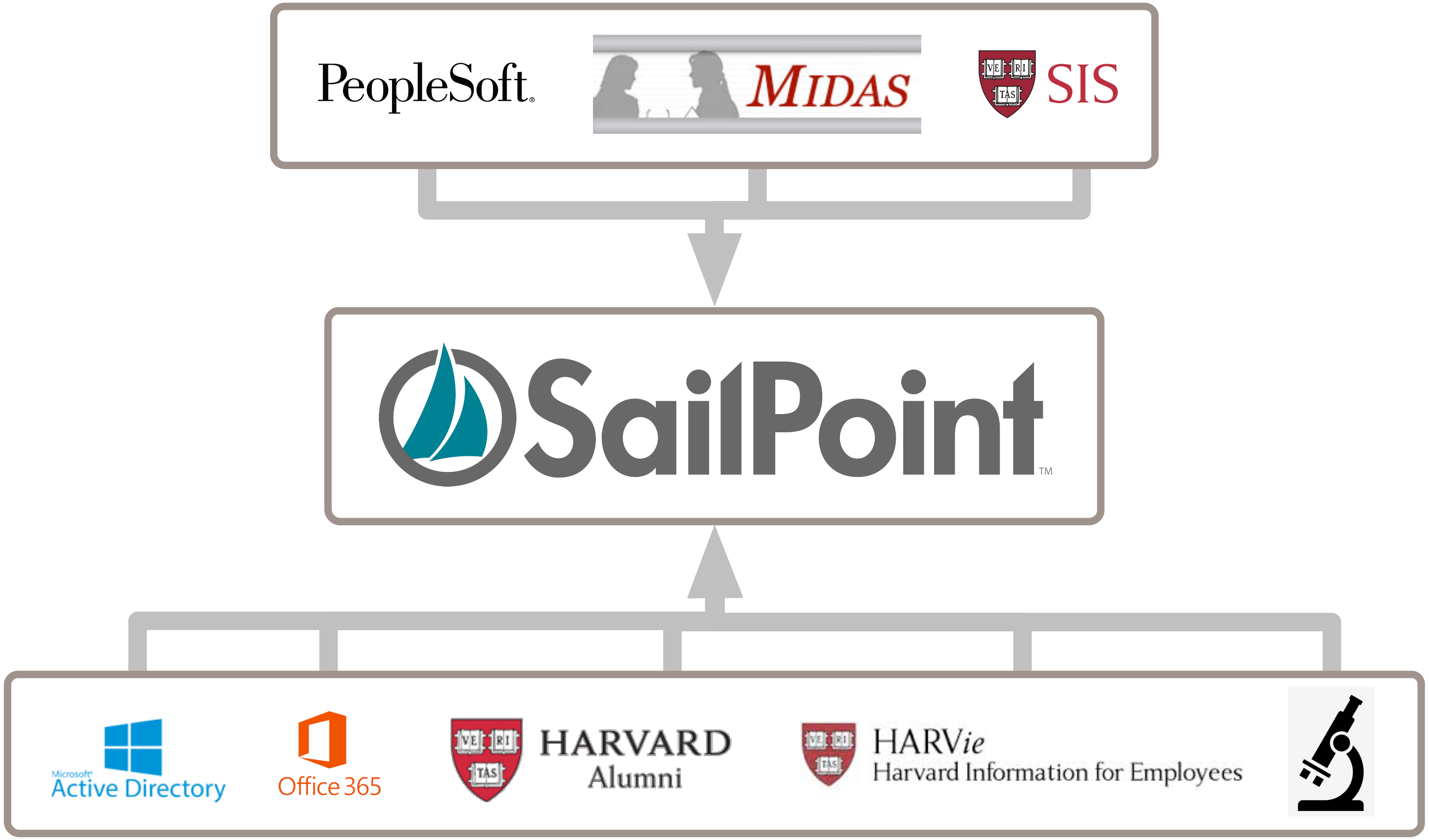
- Add new users quickly and accurately
- Reduce manual processes and delays by issuing access through a central identity store
- Make role changes simpler and easier
- Streamline the revocation of access when it’s necessary

The IAM program will be using SailPoint IdentityIIQ to manage provisioning and deprovisioning.

SailPoint™

A SINGLE SOURCE OF RECORD

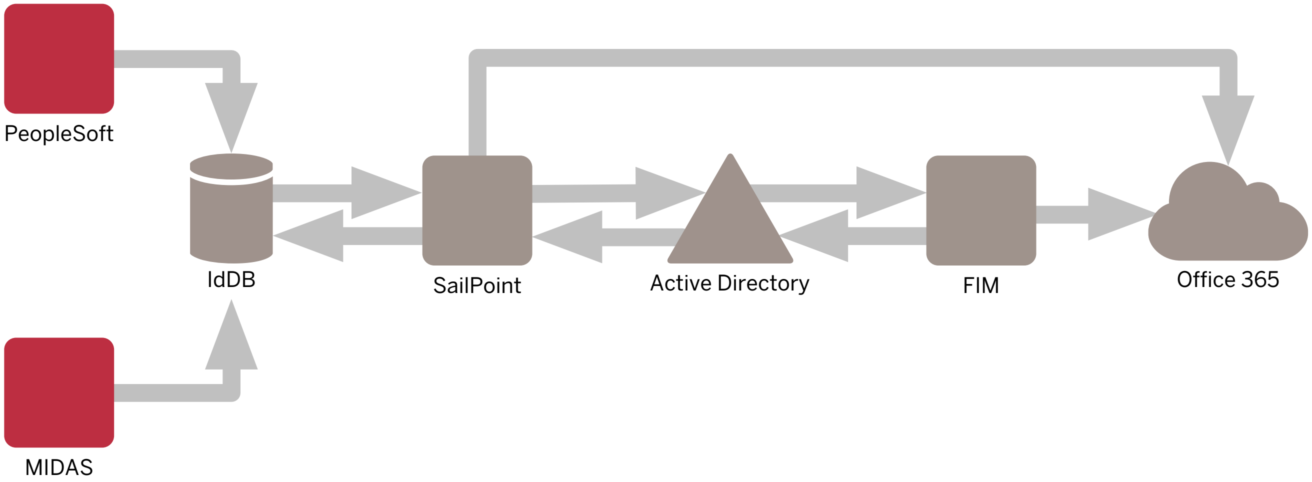
As a “single source of truth” for identity data, Sailpoint IdentityIQ will be used to manage identities across the University that then feed into all Harvard systems of record.



CHANGES TO SAILPOINT RELEASE TIMELINE

However, initial integration is complex work. Complications exist because we have a lot of ways for records to be updated today.

Example: A critical defect found while testing the SailPoint foundation release would have allowed University Active Directory (AD) email attributes to be overwritten — including email addresses.



Process Flow	Time Period	0 min	5 min	10 min	20 min	30 min	40 min	50 min	60 min
1. IdDB Read	Every 15 min	🟦	🟦		🟦	🟦	🟦		🟦
2. Provisioning Update AD	User-controlled	🟥		🟥 XXXXX	🟥	🟥		🟥	🟥 XXXXX
3. AD Read	End of IdDB read		X				X		

Red areas indicate overwrite danger time period.

CHANGES TO SAILPOINT RELEASE TIMELINE

There are known cases of when University AD is manually updated outside of a central provisioning toolset like SailPoint:

- AD system administrators perform routine updates to individual user accounts
- When migrating to O365, scripts update University AD to account for modified email attributes
- Adding new user Exchange mailboxes and Lync accounts also requires edits to attributes managed by SailPoint

The *timing* of these update cases could impact the accuracy of account attributes managed by SailPoint.

HOW DOES THIS BENEFIT ME?

Stakeholder	Experience Today	Future Goals
End Users	Different user names and credentials to access Harvard and non-Harvard apps and data Creating and managing user accounts is manual and paper-based No access to external sites, or forced to register for accounts Access to services and resources interrupted when users change, add, or leave roles	Access information and perform research across schools (and with other institutions) using a single credential Manage own accounts and sponsor others through a centralized web application Use internal Harvard credentials to access common external sites Use the same set of credentials despite changes in status, roles, or affiliations
Application Owners	Tough to integrate access management, meaning long implementation timelines and higher costs Forced to grant application access to users with the same rights on a one-by-one basis	Easily integrate Harvard users with internal and external applications via an application portal Control user access in groups, not individuals
People Administrators	Must create sponsored guest identities manually, resulting in delays and loss of productivity Can't streamline deprovisioning of users' access privileges across multiple systems	Sponsors can create and manage external parties' identity and access Automated provisioning reduces the burden on people administrators of disparate systems and improves Harvard's security posture

HOW DOES THIS BENEFIT ME?

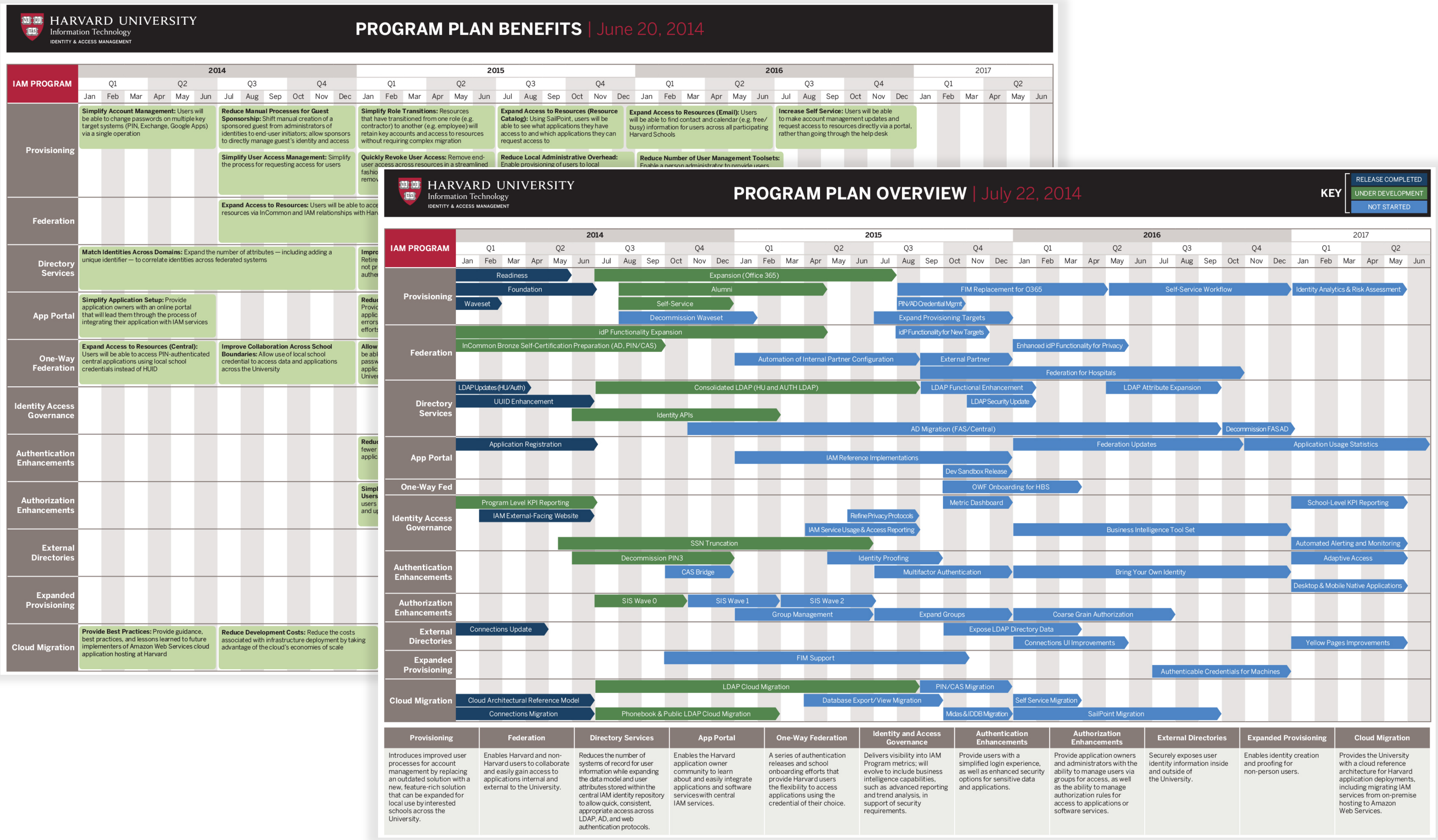
Stakeholder	Experience Today	Future Goals
End Users	Different user names and credentials to access Harvard and non-Harvard apps and data Creating and managing user accounts is manual and paper-based No access to external sites, or forced to register for accounts Access to services and resources interrupted when users change, add, or leave roles	Access information and perform research across schools (and with other institutions) using a single credential Manage own accounts and sponsor others through a centralized web application Use internal Harvard credentials to access common external sites Use the same set of credentials despite changes in status, roles, or affiliations
Application Owners	Tough to integrate access management, meaning long implementation timelines and higher costs Forced to grant application access to users with the same rights on a one-by-one basis	Easily integrate Harvard users with internal and external applications via an application portal Control user access in groups, not individuals
People Administrators	Must create sponsored guest identities manually, resulting in delays and loss of productivity Can't streamline deprovisioning of users' access privileges across multiple systems	Sponsors can create and manage external parties' identity and access Automated provisioning reduces the burden on people administrators of disparate systems and improves Harvard's security posture

HOW DOES THIS BENEFIT ME?

Stakeholder	Experience Today	Future Goals
End Users	Different user names and credentials to access Harvard and non-Harvard apps and data Creating and managing user accounts is manual and paper-based No access to external sites, or forced to register for accounts Access to services and resources interrupted when users change, add, or leave roles	Access information and perform research across schools (and with other institutions) using a single credential Manage own accounts and sponsor others through a centralized web application Use internal Harvard credentials to access common external sites Use the same set of credentials despite changes in status, roles, or affiliations
Application Owners	Tough to integrate access management, meaning long implementation timelines and higher costs Forced to grant application access to users with the same rights on a one-by-one basis	Easily integrate Harvard users with internal and external applications via an application portal Control user access in groups, not individuals
People Administrators	Must create sponsored guest identities manually, resulting in delays and loss of productivity Can't streamline deprovisioning of users' access privileges across multiple systems	Sponsors can create and manage external parties' identity and access Automated provisioning reduces the burden on people administrators of disparate systems and improves Harvard's security posture

HOW DOES THIS BENEFIT ME?

Check the handout to see our plan and benefits broken down by deliverable.



HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

PROGRAM PLAN BENEFITS | June 20, 2014

IAM PROGRAM — 2014 / 2015 / 2016 / 2017 — Q1 Q2 Q3 Q4 — Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

Provisioning

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-user initiators; 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 fashio remov

Reduce Local Administrative Overhead: Enable provisioning of users to local

Reduce Number of User Management Toolsets: Enable a person administrator to provide users

Federation

Expand Access to Resources: Users will be able to acce resources via InCommon and IAM relationships with Harv

Directory Services

Match Identities Across Domains: Expand the number of attributes — including adding a unique identifier — to correlate identities across federated systems

Impro Retire not pr authe

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

Reduc Provic applic errors efforts

One-Way Federation

Expand Access to Resources (Central): Users will be able to access PIN-authenticated central applications using local school credentials instead of HUID

Improve Collaboration Across School Boundaries: Allow use of local school credential to access data and applications across the University

Allow be abl passw applic Univer

Identity Access Governance

Authentication Enhancements

Reduc fewer applic

Authorization Enhancements

Simpl Users users and up

External Directories

Expanded Provisioning

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

HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

PROGRAM PLAN OVERVIEW | July 22, 2014

KEY: RELEASE COMPLETED / UNDER DEVELOPMENT / NOT STARTED

IAM PROGRAM — 2014 / 2015 / 2016 / 2017 — Q1 Q2 Q3 Q4 — Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

Provisioning
- Readiness
- Expansion (Office 365)
- Foundation
- Alumni
- FIM Replacement for O365
- Self-Service Workflow
- Identity Analytics & Risk Assessment
- Waveset
- Self-Service
- PIN/AD Credential Mgmt
- Decommission Waveset
- Expand Provisioning Targets

Federation
- idP Functionality Expansion
- idP Functionality for New Targets
- InCommon Bronze Self-Certification Preparation (AD, PIN/CAS)
- Enhanced idP Functionality for Privacy
- Automation of Internal Partner Configuration
- External Partner
- Federation for Hospitals

Directory Services
- LDAP Updates (HU/Auth)
- Consolidated LDAP (HU and AUTH LDAP)
- LDAP Functional Enhancement
- LDAP Attribute Expansion
- UUID Enhancement
- LDAP Security Update
- Identity APIs
- AD Migration (FAS/Central)
- Decommission FAS AD

App Portal
- Application Registration
- Federation Updates
- Application Usage Statistics
- IAM Reference Implementations
- Dev Sandbox Release

One-Way Fed
- OWF Onboarding for HBS

Identity Access Governance
- Program Level KPI Reporting
- Metric Dashboard
- School-Level KPI Reporting
- IAM External-Facing Website
- Refine Privacy Protocols
- IAM Service Usage & Access Reporting
- Business Intelligence Tool Set
- SSN Truncation
- Automated Alerting and Monitoring

Authentication Enhancements
- Decommission PIN3
- Identity Proofing
- Adaptive Access
- CAS Bridge
- Multifactor Authentication
- Bring Your Own Identity
- Desktop & Mobile Native Applications

Authorization Enhancements
- SIS Wave 0
- SIS Wave 1
- SIS Wave 2
- Group Management
- Expand Groups
- Coarse Grain Authorization

External Directories
- Connections Update
- Expose LDAP Directory Data
- Connections UI Improvements
- Yellow Pages Improvements

Expanded Provisioning
- FIM Support
- Authenticable Credentials for Machines

Cloud Migration
- LDAP Cloud Migration
- PIN/CAS Migration
- Cloud Architectural Reference Model
- Database Export/View Migration
- Self Service Migration
- Connections Migration
- Phonebook & Public LDAP Cloud Migration
- Midas & IDDB Migration
- SailPoint Migration

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

IAM: IN SUMMARY

- Identity begins at the first login screen
- IAM exists to make onboarding, day-to-day use, role changes and access to resources easier for everyone in the Harvard Community
- Our efforts will improve productivity and make day-to-day life simpler for faculty, staff, students, researchers, people administrators, application owners, and more
- And when IAM services are done right, you don’t even notice the effects — things just work

Take the mystery out of identity.

Learn more about our program at **iam.harvard.edu**

HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT