HARVARD UNIVERSITY
Information Technology

Identity and Access Management Program Plan

January 28, 2014

Revisions Table

Version	Date	Add/Delete/Change	Author	Document Section (Sec. #) and (Pg. #)	Description of Revision
1.0	1/28/14	Initial version	IAM Team		

Table of Contents

1.0 Program Plan Objectives

1.1 Document Purpose

The purpose of this plan is to provide a comprehensive overview of all facets of the Identity and Access Management Program (IAM) with a three-year horizon.

This plan will provide executive level overview of the IAM Program inclusive of the program goals, program structure, planning approach and overall implementation roadmap.

The IAM Program Team will review this plan on a quarterly basis. The status of the projects described by this document will be presented to Senior Leadership and Program Stakeholders by means of an Executive Dashboard on a monthly basis.

2.0 Program Overview

2.1 What is Identity and Access Management?

Identity and Access Management is a set of business processes and supporting technologies that enable the creation, maintenance, and use of a digital identity. As such, the impact of Identity and Access Management to Harvard's user community, application portfolio, and information resources is extensive. The IAM Program and Services are responsible for the management of faculty, administration, and student information, access to Harvard applications and information, and the distribution of such information externally. For a list of terms that are helpful for understanding the Program Plan, please refer to *Appendix A*.

2.2 Why is Identity and Access Management a Strategic Initiative?

The first impression of any Harvard student, faculty, researcher, or administrative staff of IT is formed from their experience at the login screen. Today, the implementation of Identity and Access Management at Harvard is maddeningly redundant and complex. The impact of such distributed complexity includes:

- **Lost User Productivity** - Reduced productivity results as users wait for their new accounts to be created. Delays in the ability of a user to access resources that result when manual, paper-based workflows and approvals can not be streamlined or easily orchestrated. There can be a lengthy wait time for users to get access to the resources they need and have the right to access.
- **Poor User Experience -** The issuance and management of multiple user accounts and passwords to support access to different applications and resources across the University results in user confusion and frustration.
- **Limited Information Sharing Across Applications** - The applications are unable to share information that they could share, such as contact information, files and common data for calendaring and other common functions.
- **Unnecessary Administrative Overhead -** The high volume of calls to the IT help desk to address basic account or application management functions, like a password management, creates an unnecessary burden on support staff.
- **Reduced Security Stature** - The inability to streamline the de-provisioning of users or to manage user access privileges to applications and resources exposes the University to the risk of unauthorized access and audit compliance issues.

The reach of these problems and their associated impact is vast; such that, universally, all School IT leadership has become united in their concern. Because IAM affects all of the University's people, resources and systems, the reputation of Harvard University IT is stigmatized as a direct result of the limitations of the current IAM solution set.

2.3 What are the Tenets of a Successful Identity and Access Management Program?

The IAM Program originated from the need to eliminate perceived complexities surrounding identities. Above all, the IAM Program activities and deliverables will focus on achieving this fundamental objective. Additionally, the IAM Program is designed to improve the core competencies of the University, particularly in the realms of research and learning. The founding IAM Program guiding tenets are described below:

Tenet #1 - Identity and Access Management Impacts Everyone and Everything

If implemented correctly, Identity and Access Management should be simple and intuitive to an end user. Nevertheless, its importance should not be underrated. IAM is a core technical service that exists to ensure that only verified people access online resources and knowledge assets of the University via managed permissions. Without IAM, the people at the University could not easily access, provide access to, or share information.

In the ideal state, IAM enables new applications and services to be brought up quickly, provides necessary user information to the applications so they can properly function, and allows users to partake in the new service with minimal effort. The identity stores central to IAM hold critical information about the identities and attributes of the University's internal and external user community. In addition to enabling account creation and application access decisions, this identity asset can be data mined by the University and leveraged to enable efforts that range from supporting business intelligence initiatives to mitigating information security risks to streamlining alumni fundraising by providing a continuous identity for a user despite affiliation changes.

Tenet #2 - Identity and Access Management Simplifies the User Experience

Identity and Access Management will reduce complexity for end users, application owners, and people administrators. IAM will streamline identity and account creation for end users through the elimination of paper-based, manual processes. It will enable the end user to have insight and control over their accounts through self-service account management, placing the control of basic requests, like user name creation, password changes and access requests, into the hands of the user and off the shoulders of a help desk.

IAM will allow a user to select the credential of their choice for access needs and will reduce the burden of remembering credentials that span the systems they use to work, study, or collaborate. IAM will enable productivity, by means of quick provisioning, granting user's access to protected systems, resources, and physical locations with little to no intervention by administrative staff.

Tenet #3- Identity and Access Management Enables Research and Collaboration

Identity and Access Management will facilitate collaboration. It will break down the barriers to access for the end users and open up the ability to share information and work safely together across School and institutional boundaries. IAM will demand the implementation of standards, and will leverage these standards to federate decision making with external systems.

Through the use of authentication standards set forth by InCommon, IAM lays the groundwork to carefully share identity information about users that enables access to resources that can't currently be viewed through any other means. It will provide the University with a competitive advantage over institutions that can't offer the same level of ease and expediency – enticing students and faculty to come to or stay at the University to study and perform research.

Tenet #4- Identity and Access Management Protects University Resources

Identity and Access Management is a vital information safeguard. It exists to protect sensitive data and information from the ever-evolving landscape of security threats. Properly implemented, IAM solutions help enable proactive security risk identification and mitigation, allowing the University to identify policy violations or remove inappropriate access privileges, without having to waste time and effort searching across disparate systems. IAM will allow the University to easily assert that proper controls and measures are in place that meets audit and regulatory requirements.

Tenet #5- Identity and Access Management Facilitates Technology Innovation

Identity and Access Management increases the agility of application development and deployment; it eliminates the need for application developers to reinvent and duplicate potentially vulnerable authentication systems. IAM also eliminates the need for application owners to manage such duplicate systems. IAM helps weather the storm of disruptive innovation; it positions the University to quickly and securely implement or integrate with cloud platforms and services.

IAM enables key technology initiatives; it is a key precursor to the successful implementation of new University initiatives. The Student Information System, the next generation Unified Communications System and the Learning Management Ecosystem rely on sound IAM process reengineering, design, and implementation to extend improved services to the end-user community.

2.4 What is the Vision of the Identity and Access Management Program for Harvard?

Simply stated, the vision of the IAM Program is to:

> "***Provide secure access to applications that is easy for the user, application owner, and IT administrative staff with solutions that require fewer login credentials, enable collaboration across Harvard and beyond, and improve security and auditing."***

The IAM Program will be implemented to meet the vision in accordance to the previously defined tenets. Additionally, there will be heightened emphasis placed upon an additional set of guiding principles for the program. These include:

- Harvard Community needs will drive how the technology supports the Identity and Access Program
- Tactical project planning will remain aligned with the Program strategic objectives
- Solution design will allow for other Schools to use the foundational services to communicate with the IAM system in a consistent, federated fashion
- Communication and socialization of the program are critical to its success

IAM Program Vision
Provide secure access to applications that is easy for the user, application owner, and IT administrative staff with solutions that require fewer login credentials, enable collaboration across Harvard and beyond, and improve security and auditing.

Strategic Objectives	Guiding Principles	Key Performance Indicators
1. **Simplify the User Experience** • "To simplify and improve user access to applications and information inside and outside of the University." **2. Enable Research and Collaboration** • "Simplify the ability for faculty, staff, and students to perform research and collaboration within the University and with colleagues from other institutions." **3. Protect University Resources** • "Improve the security stature of the University with a standard approach." **4. Facilitate Technology Innovation** • "Establish a strong foundation for IAM to enable user access regardless of new and/or disruptive technologies."	• Harvard Community needs will drive the technology supporting the Identity and Access Management Program • Tactical project planning will remain aligned with the Program strategic objectives • Solution design should allow for other Schools to use the foundational to communicate with the IAM system in a consistent, federated fashion • Communication and socialization of the program are critical to its success	• The number of help desk requests that relate to account management per month. • The number of registered production applications that use the IAM system per month. • The number of user logins and access requests through the IAM system per month. • The number of production systems that the IAM system provisions to per month.

Table 2.4.1 – IAM Program Vision table

2.5 What External Factors Influence the Success of the Identity and Access Management Program?

The definition of a critical success factor is an external area of influence that has significant impact upon program scope and delivery. In order for the Identity and Access Management to meet the program goals, the following critical success factors must be closely managed

Critical Success Factor	Description
Executive Sponsorship	Engage proactively with key stakeholders to maintain program support and make key decisions.
Resource Planning	Recruit qualified staff according to project timelines.
Budget Planning	Retain and maintain ability to spend at budgeted funding levels over the course of FY14 - FY17.
School Partnership and Participation	Form strong relationships with and understanding of the users within the School community.
Transition Planning	Garner support for Cloud Infrastructure and ITSM Transition Processes.

Table 2.5.1 – Critical Success Factors for the IAM Program

2.6 What Organizational Structure is required to Support the Program?

IAM Organizational Overview

Under the direction of the IAM Program Director, the IAM Program is organized into four distinct teams: Strategy and Planning, Product, Technical, and Architecture. A summary of the each team, associated management and overall functional responsibilities are listed below:

Strategy and Planning Team - (E. Bradshaw)
The IAM Strategy and Planning team is responsible for providing communication, strategic planning, outreach across Schools, HUIT, and the IAM Program itself. Staff will be added to assist in the development of the focus areas listed below:

- Program Plan Creation
- Community Planning and Outreach
- Cloud Infrastructure Planning
- Communications
- IAM Human Resources
- IAM Finance

Product Team – (J. Hill)
The IAM Product team provides functional and product support, including business process evaluation, service definition, and the development of IAM as a series of supportable products. Staff will be added to assist in the development of the focus areas listed below:

- Business Analysis
- Service Definition
- Product Management
- Solution Support Services
- Quality Assurance

Technical Team - (M. Bjorkman)
The IAM Technical Team implements, tests, and releases the IAM solution set. Staff will be added to assist in the development of the focus areas listed below:

- Project Planning
- Identity Management
- Access Management
- Identity Repositories
- Practice Management
- Systems Integration

Architecture Team - (S. Bradner, M. Erdos)
The IAM Architecture Team provides subject matter expertise, best practices and patterns for implementation, technical problem resolution approaches, and strategic direction recommendations. Responsibilities include:

- IAM Policy Creation
- IAM Solution Architecture and Design
- University IAM Standards

2.7 What is the Governance Structure for the Identity and Access Management Program?

The IAM Program is split into three individual governing committees: the IAM Executive Committee, Lifecycle Advisory Group, and Technical Oversight Committee. The following is a description of the responsibilities and objectives for each group:

IAM Executive Committee

IAM Executive Committee
The primary objective for the IAM Program Executive Committee is to provide consistent, timely and meaningful oversight for the Identity and Access Management Program. The IAM Program Executive Committee will identify and champion business process improvement, provide program oversight, and guide the strategy for the implementation and roll out. The Committee will meet on a monthly basis.

Objectives	Guiding Principles	Standing Agenda

• Guide and approve suggested business process changes and provide strategic direction for their introduction
• Provide direction and approve program policy
• Identify and assist in the resolution of obstacles to the program strategic objectives
• Provide direction for communications to stakeholders
• Determine prioritization of IAM Program projects and strategic approaches
• Track status of projects and assist in the mitigation strategy for identified risks
• Monitor ongoing impact, service levels, and service improvements
	• Promote change and acknowledge areas that need improvement across the University
	• Urge the crossing of silos where it would improve business processes
	• Encourage broad communication and support among stakeholders
	• Be transparent in our processes and decisions
	• Use criteria and metrics to evaluate ideas and measure them against desired outcomes
	• Accept uncertainty, ambiguity, and lack of absolutes when necessary
		• Approval of Prior Minutes
		• Co-Chairs Report
		• Program Report
		• Decisions
		  ▪ Policy
		  ▪ Business Process
		  ▪ Communications
		• Areas for Assistance
		• General Discussion Topics

Table 2.7.1 – IAM Executive Committee table

IAM Identity Lifecycle Committee

IAM Identity Lifecycle Committee
The mission of the IAM Identity Lifecycle Committee is to work towards improving the end-user experience at Harvard. This will be accomplished by bringing the collective and varied expertise of a representative set of campus business process owners to bear on topics related to the management of identity related processes and services. The primary objective of the group is to contribute meaningful recommendations on process improvement and service offerings, and to serve as a catalyst for projects across the University that will improve onboarding and the lifecycle of user experience through better systems, processes, education and raising awareness of process and policy. The group will advise the product and practice management team of the Identity and Access Management Program, including endorsing recommendations to the IAM Executive Committee. The Committee will meet on a monthly basis.

Objectives	Guiding Principles	Standing Agenda
• Participate in improving the end-user experience at Harvard • Provide a catalyst for projects across the University that will measurably improve onboarding and other lifecycle processes • Recommend IAM service enhancements and new offerings • Provide forum for related policy discussion • Provide input on the IAM product strategy • Serve as a sounding board for new ideas and approaches to providing identity and access management services • Assist with quantifying the impact of proposed process changes and recommending implementation approach	• Commit to improving the user experience • Act in the interest of Harvard as a whole • Openly acknowledge problem areas and promote change when needed • Work towards eliminating the historical silos that may have previously hindered the improvement of processes and systems • Encourage broad communication and offer direct support as a stakeholder • Operate with transparency around process and decision making • Use criteria and metrics to evaluate ideas and measure them against desired outcomes • Accept uncertainty, ambiguity, and absence of absolutes when necessary	• Approval of Prior Minutes • Chairs Report • Program Update • Requirements Discussion • Working Group Updates • General Discussion Topics

Table 2.7.2 – IAM Identity Lifecycle Committee table

IAM Technical Oversight Committee

IAM Technical Oversight Committee
The primary objective for the IAM Technical Oversight Committee is to provide consistent, timely and meaningful review of proposals of architecture and standards for the Identity and Access Management Program. The IAM Technical Oversight Committee will identify the need for technical solutions, architecture, and standards. When those have been developed, provide feedback as well as recommendation for adoption to the IAM Executive Committee. The Committee will meet on a monthly basis.

Objectives	Guiding Principles	Standing Agenda
• Guide and approve recommendations to the IAM Executive Committee for architectures and standards • Identify the need for technical solutions, architectures and standards • Recommend the set of resources outside the IAM Program Team to be involved in drafting architectures and standards • Coordinate around technical change management to ensure change will be included in local planning	• Promote change and acknowledge areas that need improvement to improve the University • Urge the crossing of silos where it would improve business processes • Encourage broad communication and support among stakeholders • Be transparent in our processes and decisions • Use criteria and metrics to evaluate ideas and measure them against desired outcomes • Accept uncertainty, ambiguity, and lack of absolutes when necessary	• Approval of Prior Minutes • Chairs Report • Architecture • Standards • Working Group Updates • Proposal Review and Recommendations to Approve • General Discussion Topics

Table 2.7.3 – IAM Technical Oversight Committee table

3.0 Program Approach

3.1 Program Implementation Framework

"Top-Down" Planning

In order for the IAM Program to successfully meet its objectives, the team will follow a "top-down" approach to delivery. The Program Plan will serve as the governing document for the team and all activities will be planned and managed in accordance to it. All releases within the team will tie back to the IAM Program's strategic objectives and each strategic objective will be measurable. The development and delivery of IAM functionality will be iterative in nature, following Agile processes, and be based on evolving user requirements and stories. The scope of releases will be adjusted based upon changing requirements and the evolving status of critical success factors.

Project Tracks

The IAM Program will be broken down into eleven project tracks and tracked on a per project basis. A project manager will be assigned to each project track and will be responsible for developing a project plan to govern the work activities and report weekly status. The eleven projects are identified and summarized below:

Project	Project Description
SailPoint	The SailPoint Project introduces improved user processes for account management. The team will replace an outdated solution with a new, feature rich, solution that can be expanded for local use by interested Schools across the University.
Federation	The Federation Project enables Harvard users, users at Harvard affiliated institutions and non-Harvard users to collaborate and easily gain access to applications and resources, internal and external to the University.
Directory Services	The Directory Services Project 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. This will allow quick, consistent and appropriate access across LDAP, Active Directory (AD) and as well as web authentication protocols.
App Portal	The App Portal Project enables the Harvard Application Owner community to learn about and easily integrate applications and software services with central IAM Services.
One Way Federation	The One Way Federation Project consists of a series of authentication releases and School onboarding efforts that provide Harvard user with the flexibility to access applications with a credential of their choice.
Identity and Access Governance	The Identity and Access Governance Project will deliver visibility into the IAM Program metrics, new user certification processes and audit reporting. It will evolve to encompass business intelligence and identity analytics to support risk management and strategic decision-making.
Authentication Enhancements	The Authentication Enhancements Project provides users with a simplified login experience as well as enhanced security options for sensitive data and applications.
Authorization Enhancements	The Authorization Enhancements Project provides 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 an application or software service.
External Directories	The External Directories Project securely exposes user identity information inside and outside of the University.
Expanded Provisioning	The Expanded Provisioning Project enables identity creation, authentication, and account provisioning for non-person objects.
Cloud Migrations	The Cloud Migration Project provides the University with cloud reference architecture for Harvard application deployments and includes the migration of IAM Services from on premise hosting to Amazon Web Services.

Table 3.1.1 – Project Tracks table

Pilot Implementations

One of the core beliefs of the IAM Program is to experiment and continuously refine our solutions based on lessons learned. A key way that the IAM Program will demonstrate this commitment to responsible experimentation is through controlled pilots, within the team and with willing participants. Quickly developing functionality and testing the functionality with real users and applications is a way to improve our solutions prior to production deployment. These pilots demonstrate the value of our services early in the delivery lifecycle, and mitigate the risk of failing to meet our user requirements.

The table below represents the pilot implementations that are currently under consideration by the IAM Program. Many of the pilots will require significant participation with interested Schools:

Proposed Pilots	Description	Proposed Date
One Way Federation	Collaborate with Harvard Business School to enable one-way federation with the Harvard Business School authentication system.	Anytime
Local Provisioning	Assist Harvard Medical School with onboarding to SailPoint: ● Pilot Functionality in IAM Stage Environment	October 2014
Local Provisioning	Assist Harvard Kennedy School with onboarding to SailPoint: ● Pilot Functionality in IAM Stage Environment	December 2014
Inter-School Collaboration	Explore cross registration between Tufts Fletcher School and MIT with the Harvard Kennedy School through InCommon federation.	July 2015
Self Registered Guests	Explore cross registration mechanisms with Harvard Graduate Schools: ● Implement a New Model for Handling Prospective and Registered Students from Other Schools ● Merge XID Functionality into SailPoint	July 2015
Group Management	Explore use of a group management system for access to IAM's own administrative applications (e.g., SailPoint, App Portal)	July 2015
Social Identities for Wireless Access	Allow use of social identities (e.g., Facebook) for access to the Harvard wireless network.	August 2015
Multifactor Authentication	Explore the use of multifactor authentication with University Health Services.	December 2015
Research Computing Collaboration	Explore opportunities to replace homegrown identity systems with IAM services.	December 2015
Bring Your Own Identity	Explore the use of social identities for authentication with the Harvard School of Education and School of Public Health for their Executive Education Program.	December 2016
Identity and Access Governance	Work with the Harvard Security Office to use identity analytics for risk assessment.	December 2016

Table 3.1.2 - Proposed Pilots table

4.0 Program Implementation and Delivery

As previously mentioned, the IAM Program will be implemented in accordance to the four strategic objectives:

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

For each strategic objective, the benefits of IAM improvements are identified and categorized by the following three user types:

- End User
- Application Owners
- People Administrators

To date, the IAM Program Team has had a series of successful implementations that have delivered value to the Harvard Community. To see a list of IAM Program Accomplishments, please refer to *Appendix B.*

The following sections below identify the remaining program deliverables. These are organized by strategic objective and aligned to both the user benefit and the Program projects. For a visual representation of the IAM Program Timeline, please refer to *Appendix C.*

4.1 Simplify the User Experience

Strategic Objective Reference
Strategic Objective: • "To simplify and improve user access to applications and information inside and outside of the University"

Overview

The most significant stakeholder group affected by the IAM Program is the user community. For many users, their very first experience of the University will be through a login screen. Since this list of users includes faculty, researchers, administrative staff, students, contractors, guests, and affiliates, updates to a wide array of applications and infrastructure components are required to improve the Harvard user experience.

End User - Key Benefits

The following table summarizes the key benefits of the IAM Program for end users across the University:

Key Benefit	Description of Benefit
1. Simplify Account Management	I. A user will have a single application in SailPoint for requesting and receive access to an increasing number of target systems and applications over time. II. A user will accomplish changing their password on multiple key target systems (e.g., PIN, Exchange and Google Apps) via a single operation using SailPoint.
2. Allow Choice of Credentials	I. A user will be able to have a single preferred login name and password for access to an increasing number of applications both internal and external to the University (e.g., PeopleSoft (internal) and HathiTrust (external)). II. A user will have a say in their login name including the capability to use a social login.
3. Reduce Number of User Logins	I. A user will have fewer instances of being asked to log in after accessing an application, and then another application, and another. II. Users at participating Schools will be able to have the same login for their desktop as they have to web based IAM Services and an increasing number of applications and systems.
4. Expand Access to Resources	I. A user will be able to see what applications they have access to right away and which applications they can request access to via SailPoint (e.g., resource catalog). II. A user will be able to find contact and calendar information (e.g., free/busy) for users across all participating Harvard Schools. III. A user will have access to an increasing number of external resources via InCommon and via IAM relationships with external communities. IV. A user will be able to access PIN-authenticated central applications using local school credentials instead of their HUID
5. Increase Self Service	I. A user will be able to make account management updates and request access to resources directly through SailPoint rather than going through the help desk.
6. Simplify Role Transitions	I. A user who has transitioned from one role (e.g., contractor) to another (e.g., employee) within a School will keep the key accounts (e.g., PIN and Exchange) and access to resources they have without need of a complex migration process. II. A user who transitions from one School to another will have a smoother transition process.

Table 4.1.1 – End User, Simplify the User Experience, Key Benefits table

Application Owner - Key Benefits

The following table summarizes the key benefits of the IAM Program for application owners, simplifying the user experience for IAM Services across the University.

Key Benefit	Description of Benefit
1. Simplify Application Setup	I. Application Owners will use an online application portal that will lead them through integrating their application with IAM Services. This integration covers: A. Guidance on which IAM Services best fit their needs B. Simplified application registration and management with IAM C. Code libraries that reduce development costs and time D. Guidance on application configuration II. IAM will provide "turnkey" environments for testing the application with IAM Services. III. IAM will provide reference implementations to aid speed of development and deployment. IV. IAM will support the evolving set of standard industry protocols related to user authentication and access, thus simplifying integration of third party applications and cloud services with IAM.
2. Simplify Application Administration	I. An Application Owner can easily use an enhanced IAM authorization service to manage coarse-grained access control to their application. II. An application will be able to access an enhanced set of attributes about a user for each access control decision: A. "Higher level" attributes that better fit typical access use cases will allow for simpler access rules B. Group membership information, as attribute, also promote simpler access rules C. A consistent core set of identifiers and attributes will be available for each and every user no matter what the user's role, again enabling simpler access rules for many applications D. Easier access to the identifiers and attributes, with less development work needed. III. An Application Owner can easily manage groups that can be used for controlling access to the application.

Table 4.1.2 – Application Owner, Simplify the User Experience, Key Benefits table

People Administrator- Key Benefits

The following table summarizes the key benefits of the IAM Program for administrators of identities that simplify the user experience for IAM Services across the University.

Key Benefit	Description of Benefit
1. Simplify Account Management	I. Provide a simplified means of sponsoring an external person into a role at Harvard: A. A single, consistent, online process for creation of the sponsored identity and role II. Simplify the management of sponsored persons (e.g., types of non-employee, non-student users, contractors): A. A sponsor will be able to see the list of people they have sponsored through SailPoint; including each person's roles and the start/end date for the role, as well as extend access online B. The sponsor will be able to manage each sponsored person's access to systems and application through SailPoint III. Provide an enhanced online means of finding if a "new" user has an existing identity at the University. This results in fewer duplicate identities and accounts, as well as for allowing the end user to keep their existing credentials. IV. Enable bulk requests account creation.
2. Reduce Number of User Management Toolsets	I. Enable a person administrator to do more of the work required to give a user the access they need within this single tool. This tool will also allow the person administrator insight into which users have access to which resources.
3. Simplify administration of groups of users	I. Provide a group service that can be used for both mailing lists and for access control. II. Allow for a given change to affect a set of users rather than forcing a separate operation and multiple administrative updates for each user.

Table 4.1.3 – People Administrator, Simplify the User Experience, Key Benefits table

Deliverables

The following set of tables identify the Key Deliverables for the IAM Program organized by Project:

SailPoint – Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Waveset Update	Support the transition of student users to the @g Google domain, including FERPA status to support implementation of online directories.	Expand Access to resources	FAS GSD HDS GSE SPH Central	March 2014
Readiness	Implement internal, provisioning readiness release to transition from outdated solution to SailPoint: • Implement Connectors for Provisioning • Expand Data Model	Simplify Account Management	No user impact	April 2014
Foundation	Implement the first production release of SailPoint: • Implement Self Service for Account Claiming and Password Management • Begin Migration of Provisioning to New Platform • Update the IAM Service Definition	Simplify Account Management	FAS GSD HDS GSE SPH Central	July 2014
HUIT Expansion	Expand the functionality of SailPoint: • Complete Migration of Provisioning • Implement Self Service Creation of Sponsored Accounts to Replace Paper-based Requests • Update the IAM Service Definition	Simplify Account Management Reduce Number of User Management Toolsets	FAS GSD HDS GSE SPH Central	October 2014
Decommission Waveset	Decommission the Oracle Waveset Solution: • Milestone Representing a “Like for Like” Replacement of Waveset Functionality in SailPoint	Simplify Account Management	No user impact	November 2014
Role Transition	Expand user populations within SailPoint: • Introduce Capability for Better Sign-on Experience for Externally Cross Registered Students • Introduce New POI User Types	Simplify Role Transitions	External Community Harvard Community	January 2015

Expand Provisioning Targets	Onboard SEAS, HKS, and HMS to central account management and provisioning solution: • User Account Management • Sponsored Account Creation • Provisioning from Central Solution to Local Systems and Data Stores	Simplify Account Management	SEAS HKS HMS	January 2015

Table 4.1.4 - SailPoint, Simplify the User Experience, Deliverables table

Directory Services - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
UUID Enhancement	Provide programmatic interfaces to Schools to allow Schools, applications, or organizations to find user UUIDs by a variety of criteria.	Simplify Account Management Simplify Application Administration	Harvard Community	July 2014
AD Consolidation Preparation	Prepare the University and the FAS Active Directory domains for consolidation: • Application Remediation • Desktop Changes • User Name Collision Remediation	Simplify Account Management Simplify Application Administration Expand Access to Resources	FAS	October 2014
Consolidated LDAP	Consolidate the HU and AUTH LDAPs to simplify the process for application owners to make authentication and authorization decisions: • Enable Cloud Applications to Query IAM Services for Attributes	Simplify Application Administration	Harvard Community	February 2015
LDAP Functional Enhancement	Expand attributes to provide clearer role and affiliation information, and incorporate standard attributes to support participation in internal and external federations.	Simplify Application Administration	Harvard Community	July 2015

AD Migration	Move resources from FAS AD to University AD in conjunction with Unified Communications and Desktop teams: • Move Devices and Computers including Field Visit • Move Applications • Move Accounts	Simplify Account Management Simplify Application Administration Expand Access to Resources	FAS	September 2016
Decommission FAS AD	Decommission FAS AD environment.	Simplify Account Management Simplify Application Administration	FAS	September 2016

Table 4.1.5 - Delivery Services, Simplify the User Experience, Deliverables table

App Portal - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Application Registration	Implement a new Application Portal to streamline application integration with IAM Services.	Simplify Application Setup Reduce Complexity of IAM Integration	Harvard Community	July 2014
IAM Reference Implementation	Expand the App Portal to include reference implementations inclusive of pre-developed code.	Simplify Application Set up	Harvard Community	February 2015
Developer Sandbox Release	Update the App Portal to provide "turnkey" environments for testing the application with IAM Services.	Simplify Application Set-up Reduce Security Development Burden	Harvard Community	July 2015

Table 4.1.6 - App Portal, Simplify the User Experience, Deliverables table

Authentication Enhancements - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Decommission PIN3	Decommission the PIN3 application and migrate all current PIN3 user communities to the central authentication solution.	Simplify Application Administration	GSE FAS Central	April 2015
CAS Bridge	Enhance the Central Authentication System to support additional protocols. • Allow Participation From Federated Organizations	Simplify Application Set-up Expand Access to Resources	Harvard Community	April 2015
PIN UI Improvements	Improve the PIN application user interface to be in-line with Harvard UI guidelines. • Implement improved user functionality in a federated environment, including “Remember Me” functionality for users.	Allow Choice of Credentials Reduce Number of User Logins	Harvard Community	July 2015

Table 4.1.7 - Authentication Enhancements, Simplify the User Experience, Deliverables table

Authorization Enhancements - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
SIS Data Model Release	Release IAM Services for SIS implementation: • Expand central identity store to include new user types	Simplify Application Administration Expand Access to Resources	SIS	November 2014
SIS Wave 2	Perform application and data changes in concert with a wider release of the SIS initiative.	Simplify Application Administration Expand Access to Resources	SIS	March 2015

Table 4.1.8 - Authorization Enhancements, Simplify the User Experience, Deliverables table

External Directories - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Connections Update	Replace the IBM Connections product with a homegrown product.	Meet License Requirement	Harvard Community	May 2014
Expose LDAP Directory Data	Expose enhanced LDAP directory data through alternative protocols to fit the needs of applications; e.g., attributes through SAML, AD and CAS.	Simplify Application Administration	Harvard Community	September 2015
Connections User Interface Improvements	Provide improved search capabilities and a new interface for application owners to use for development efforts.	Expand Access to Resources	Harvard Community	June 2016
Yellow Pages Improvements	Create a new web application that provides an enhanced internal directory for department information.	Expand Access to Resources Increase Self Service	Harvard Community	June 2017

Table 4.1.9 - External Directories, Simplify the User Experience, Deliverables table

Expanded Provisioning - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Dionysus Update	Release updated Dionysus application for management of devices in University AD: • Updates to Modern Platform and Functional Enhancements • Simplify Architecture • Migrate to Cloud	Simplify Account Set-up	FAS GSD HDS GSE SPH Central HKS SEASE	May 2014

Table 4.1.10 - Expanding Provisioning, Simplify the User Experience, Deliverables table

4.2 Enable Research and Collaboration

Strategic Objective Reference
Strategic Objective: • "Simplify the ability for faculty, staff, and students to perform research and collaboration within the University and with colleagues from other institutions."

Overview

Harvard is a premier research institution; making it simple to work within, across, and outside School boundaries is fundamental to the mission of the University and essential to facilitating productivity for users that rely on IAM Services. IAM Services will support inter-faculty initiatives for Research and Collaboration.

End User – Key Benefits

The following table summarizes the key benefits of the IAM Program for end users that participate in research and collaboration across the University:

Key Benefit	Description of Benefit
1. Increase Self Service	I. Provide online, automated functionality for self-service sponsored guest creation.
2. Improve Collaboration across School and Institutional Boundaries	I. Allow use of local, School credentials to access to data and applications across the University. II. Allow use of local, School credentials for access to data and applications at outside institutions. III. Allow for an external user to transition to a Harvard affiliation from other higher education institutions without disruption of previous access privileges.
3. Expand Access to Resources	I. Enable access to an expanded set of applications and resources available through Harvard's participation in InCommon (e.g., Hathitrust). II. Provide capability for users to share access to physical resources, such as computing clusters or lab equipment, for teaching and research purposes. III. Provide capability for users to access resources for collaboration such as email, online forums, and secure file transfer functionality.

Table 4.2.1 – End User, Enable Research and Collaboration, Key Benefits table

People Administrator - Key Benefits

The following table summarizes the key benefits of the IAM Program for administrators of identities that enable research and collaboration across the University.

Key Benefit	Description of Benefit
1. Reduce Manual Processes for Guest Sponsorship	I. Shift the manual creation of a sponsored guest from administrators of identities to end users initiating the request. II. Allow the sponsor to manage an external person's identity and access.
2. Simplify Management of User Access	I. Simplify the ability to revoke and request access for users.

Table 4.2.2 – People Administrator, Enable Research and Collaboration, Key Benefits table

Application Owner - Key Benefits

The following table summarizes the key benefits of the IAM Program for application owners that manage applications used for research and collaboration across the University.

Key Benefit	Description of Benefit
1. Reduce Local Administrative Overhead	I. Enable the provisioning of users to local applications for easier management of access privileges to research resources. II. Introduce ability to leverage groups to synchronize access and mailing lists between applications. III. Reduce the need to manage point-to-point relationships with other application owners in order to implement access to protected resources.
2. Improve Security of Information	I. Leverage the emerging identity assurance attributes for increased confidence in a user's identity.
3. Reduce Complexity of IAM Integration	I. Reduce the complexity of application integration with third-party providers through the use of a standard set of identifiers and attributes about Harvard users found within InCommon.
4. Expand Access to Resources	I. Facilitate the integration with a spectrum of research and collaboration applications through InCommon membership.
5. Incorporate Discoverability	I. Incorporate the use of researcher identifiers into the directory services to enable global tracking of authorship of published resources (e.g., ORCID).

Table 4.2.3 – Application Owner, Enable Research and Collaboration, Key Benefits table

Deliverables

The following set of tables identify the Key Deliverables for the IAM Program organized by Project:

SailPoint - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Foundation	Enable HUIT help desk to use the new sponsored guest capabilities for existing Schools.	Reduce Manual Processes for Guest Sponsorship	FAS GSD HDS GSE SPH Central	July 2014
HUIT Expansion	Enable the people administrators for FAS and HUIT supported Schools by expanding the functionality of SailPoint IIQ for sponsored guest workflow from existing users: • Implement Self-Service Creation of Sponsored Accounts to Replace Paper-based Request • Implement Batch Processing for Sponsored Accounts for the HUIT Help Desk • Updated Service Definition	Reduce Manual Processes for Guest Sponsorship	FAS GSD HDS GSE SPH Central	October 2014
Onboard New Schools	Expand the functionality of SailPoint for sponsored guest workflow (e.g., new people administrators): • Sponsored Account Creation	Reduce Manual Processes for Guest Sponsorship	SEAS HKS HMS	January 2015
FIM Replacement for 0365	Replace the current FIM provisioning process to Microsoft O365 with SailPoint provisioning. • Deliver Shared Contacts and Calendaring	Reduce Local Administrative Overhead Simplify Management of User Access	FAS GSD HDS GSE SPH Central SEAS HKS	May 2016

Table 4.2.4 – SailPoint, Enable Research and Collaboration for the Administrator of Identities, Deliverables table

Federation - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
InCommon Deployment	Provide a means to federate with other external entities in a standardized way through InCommon. Expose IAM user attributes to other higher education InCommon communities.	Expand Access to Resources Improve Collaboration across School and Institutional Boundaries	Harvard Community External Communities	December 2013 *(Complete)*
idP Functionality Expansion	Expand the baseline idP with additional functionality needed by service providers and other institutions: • Additional User Attributes • Technical Profiles and Standard Attribute Sets	Expand Access to Resources Improve Collaboration across School and Institutional Boundaries	Harvard Community External Communities	November 2014
Automation of Internal Partner Configuration	Improve the App Portal to allow self-service registration for internal partner services: • Certificates • Metadata • InCommon Federation Registration	Expand Access to Resources Simplified Application Setup	Harvard Community	July 2015
Automation of External Partner Configuration	Improve the App Portal to allow self-service registration for the sponsor of an external partner: • Certificates • Metadata	Expand Access to Resources Simplify Application Setup	Harvard Community External Communities	January 2016
Federation for Hospitals	Federate with the hospitals. Implement OWF or work with the hospitals setting up their own IdP.	Expand Access to Resources	Hospitals HMS	June 2016
Enhanced idP Functionality for Privacy	Improve user privacy choices over the release of PII to external entities: • Targeted ID • Attribute Release Policies	Expand Access to Resources	Harvard Community	June 2016

Table 4.2.5 – Federation, Enable Research and Collaboration for the Administrator of Identities, Deliverables table

Directory Services - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
LDAP Attribute Expansion	Implement Researcher ID (e.g., ORCID) and other attributes into the central identity repository to support the library.	Incorporate Discoverability Improve Security of Information Expanded Access to Resources	Harvard Community Library	June 2016

Table 4.2.6 – Directory Services, Enable Research and Collaboration for the Administrator of Identities, Deliverables table

One Way Federation - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
eCommons ID	Implement "One Way Federation" to enable users to authenticate using iCommons account or Central/FAS account.	Expand Access to Resources	HMS FAS Central	January 2014 *(Complete)*
OWF Onboarding	Release of updates to the base code to allow for other Schools and departments to use "One Way Federation" in order to integrate their School base identities with the central administrative applications served by PIN.	Expand Access to Resources	Harvard Community	February 2015 *(Ongoing)*

Table 4.2.7 – One Way Federation, Enable Research and Collaboration, Deliverables table

Authentication Enhancements - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Multifactor Authentication	Implement multifactor authentication for sensitive research equipment and data.	Reduce risk of Identity and Account Compromise	Harvard Community	January 2016
Bring Your Own Identity	Allow external users to bring their own identity and use that to access appropriate University resources e.g., LinkedIn, Google, etc.)	Enable Choice of Identity	Executive Education External Communities	January 2017

Table 4.2.8 – Authentication Enhancements, Enable Research and Collaboration, Deliverables table

Authorization Enhancements - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Group Management	Implement ability to create user groups for access and authorization decisions for collaboration and research: • Grouper Implementation	Reduce Local Administrative Overhead Simplified Application Administration	Harvard Community	July 2015

Table 4.2.9 – Authorization Enhancements, Enable Research and Collaboration, Deliverables table

Expanded Provisioning- Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
FIM Support	Provide interim support for MS FIM Provisioning to O365.	Simplified Application Administration	No user impact	November 2015

Table 4.2.10 – Expanded Provisioning, Enable Research and Collaboration, Deliverables table

4.3 Protect University Resources

Strategic Objective Reference
Strategic Objective: • "Improve the security stature of the University with a standard approach."

Overview

In order to ensure compliance with federal and state regulations, and University policies, it is imperative that the University has an effective, streamlined approach to managing access to user information and protected resources. Through the implementation of central IAM Services, the University will have the ability to centrally manage user access, de-provision user access in a more efficient manner, and perform a continuous review of entitlements without having to perform extensive application analyses.

End User - Key Benefits

The following table summarizes the key IAM Program security benefits for end users:

Key Benefit	Description of Benefit
1. Reduce Risk of Identity and Account Compromise	I. Implement multifactor authentication to provide additional authentication assurance.
2. Limit Unauthorized Access to User's Data	I. Introduce alerting of unusual access patterns and other security events to limit unauthorized access to a user's data.
3. Improve Privacy	I. Ensure privacy of sensitive identity information.

Table 4.3.1 – End User, Protect University Resources, Key Benefits table

Application Owner - Key Benefits

The following table summarizes the key IAM Program security benefits for application owners:

Key Benefit	Description of Benefit
1. Reduce Security Development Burden	I. Provide lower application development environments (e.g., sandboxes) with IAM Services that do not contain personally identifiable information. II. Provide standard authentication libraries to application owners to reduce likelihood of errors resulting from duplicate development efforts.
2. Improve Visibility into Application Access	I. Provide access reports and key performance metrics for IAM Services. II. Provide guidance and libraries for access audit and logging messages. III. Introduce capability to track user activities within an application.
3. Improve Security Posture of IAM Services	I. Replace end-of-life infrastructure that is no longer vendor supported and hence cannot receive security updates. II. Implement InCommon security best practices for identity management.

Table 4.3.2 – Application Owner, Protect University Resources, Key Benefits table

People Administrator - Key Benefits

The following table summarizes the key IAM Program security benefits for people administrators:

Key Benefit	Description of Benefit
1. Revoke User Access Quickly	I. Remove end-user access across resources in a streamlined fashion. II. Reduce administrative touch points to remove user access.

Table 4.3.3 – People Administrator, Protect University Resources, Key Benefits table

Deliverables

The following set of tables identify the Key Deliverables for the IAM Program organized by Project:

SailPoint - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
HUIT Expansion	Provide ability for people administrators to revoke user access quickly for the user populations provisioned by SailPoint.	Reduce Risk of Identity and Account Compromise Revoke User Access Quickly	Harvard Community	October 2014

Table 4.3.4 – SailPoint, Protect University Resources, Deliverables table

Federation- Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
InCommon Bronze Self Certification Preparation	Prepare for bronze InCommon certification: • Self-Certification • Improve Internal IAM Processes	Improve Security Posture of IAM Services	Harvard Community	January 2015

Table 4.3.5 – Federation, Protect University Resources, Deliverables table

Directory Services - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
LDAP Updates	Update the end of support software and infrastructure for HU LDAP and AUTH LDAP: • Stabilize Outdated Environment • Reduce Security Vulnerabilities	Improve Reliability of IAM Services	Harvard Community	March 2014
LDAP Security Update	Apply security best practices in-line with InCommon and industry.	Improve Security Posture of IAM Services	Harvard Community	July 2015

Table 4.3.6 – Directory Services, Protect University Resources, Deliverables table

Identity and Access Governance - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Refine Privacy Protocols	Assess and update IAM services to align with the final Barron Committee report on privacy. • Publish the aligning IAM Privacy Policy and associated IAM Privacy Procedures for access to sensitive identity information.	Improve Privacy	Harvard Community	September 2014
Business Intelligence Tool Set	Introduce business intelligence capabilities and analytics to support strategic decision making and identification of areas of risk: • Pilot Use of SailPoint Dashboards and Out-of-the-box Reports • Evaluate Strategic Benefit	Limit Unauthorized Access to User's Data Improve Visibility into Application Access	Harvard Community	January 2017
Automated Alerting and Monitoring	Introduce more governance processes using SailPoint tools: • Implement Audit Reporting to Identify Risky Patterns of Excessive Access	Limit Unauthorized Access to User's Data Improve Situational awareness	Harvard Community	June 2017

Table 4.3.7 – Identity and Access Governance, Protect University Resources, Deliverables table

Authentication Enhancements - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Identity Proofing	Implement multiple levels of identity assurance safeguards for sensitive applications.	Reduce Risk of Identity and Account Compromise	Harvard Community	September 2015

Table 4.3.8 – Authentication Enhancements, Protect University Resources, Deliverables table

Authorization Enhancements - Deliverables

Key Deliverable	Description	Benefit	Users Impacted	Delivery Date
Group Management	Implement group management to improve access control administration: • IAM Managed Groups (Authoritative) • "Build Your Own" Groups (Application-Level)	Simplify Application Administration Reduce Local Administrative Overhead Revoke User Access Quickly Simplify administration of groups of users	Harvard Community	July 2015
Adaptive Access	Identity risky patterns of access and alert, and/or remediate with minimal human intervention: • Select Toolset • Implement Pilot	Limit Unauthorized Access to User's Data	Harvard Community	June 2017

Table 4.3.9 – Authorization Enhancements, Protect University Resources, Deliverables table

4.4 Facilitate Technology Innovation

Strategic Objective Reference
Strategic Objective: • "Establish a strong foundation for IAM to enable user access regardless of new and/or disruptive technologies"

Overview

The IAM Program actively participates in leading edge technology development by participating in higher education and industry standards bodies. Further, IAM performs pilots and adopts emerging technologies, such as cloud computing, to create guidance and best practices for the University to use for enterprise-wide implementations.

By keeping apprised of emerging standards and systems, IAM offers an expanding array of services to application owners, developers, and administrators; this positions the University to be a leader in technology innovation.

End User – Key Benefits

The following table summarizes the key technology innovation benefits of the IAM Program for end users:

Key Benefit	Description of Benefit
1. Improve Reliability of IAM Services	I. Leverage Amazon Web Services to provide hosting for IAM Services to increase the agility of service enhancements and improve the uptime of application authentication services.
2. Expand Integration with Desktop	I. Streamline login experience for the user to the workstation and desktop applications.
3. Enable Choice of Identity	I. Allow users to bring their own identity from participation in Social Media Online Communities to access Harvard resources. II. "Implement SocialSAML" and "OpenID Connect" in authentication.

Table 4.4.1 – End User, Facilitate Technology Innovation, Key Benefits table

Application Owner – Key Benefits

The following table summarizes the key technology innovation benefits of the IAM Program for application owners:

Key Benefit	Description of Benefit
1. Reduce Development Costs	I. Reduce the costs associated with infrastructure deployment by taking advantage of the cloud offerings and economies of scale.
2. Provide Best Practices	I. Provide cloud guidance and best practices, along with lessons learned, for future implementers of cloud application hosting at Amazon Web Services for Harvard
3. Reduce Administrative Overhead and Development Time	I. Mobile App Owners will be able to integrate with Harvard credentials using CAS/PIN for their mobile applications.
4. Improve security of machine to machine communications	I. Verify that the initiating machine is who it asserts it is. II. Provide identities to non-standard users such as: A. User Communities/Resources (e.g., microscopes)
5. Improve Situational awareness	I. Perform automated alerting and take actions without human intervention.

Table 4.4.2 – Application Owner, Facilitate Technology Innovation, Key Benefits table

People Administrator – Key Benefits

The following table summarizes the key technology innovation benefits of the IAM Program for people administrators:

Key Benefit	Description of Benefit
1. Improve Reliability of IAM Services	I. Leverage Amazon Web Services to provide hosting for IAM Services to increase the agility of service enhancements and improve the uptime of application authentication services.
2. Expand Integration with Desktop	I. Reduce the number of separate credentials to manage and reduce the number of configuration errors by integrating the desktop login to the overall IAM solution.

Table 4.4.3 – Application Owner, Facilitate Technology Innovation, Key Benefits table

Deliverables

The following set of tables identify the Key Deliverables for the IAM Program organized by Project:

Authentication Enhancements- Deliverables

Key Releases	Description	Benefit	Users Impacted	Date
Desktop and Mobile Native Apps	Provide authentication services for desktops and mobile applications, including OAuth.	Enable Choice of Identity Expand Integration with Desktop	Harvard Community	June 2017

Table 4.4.4 – Authentication Enhancements, Facilitate Technology Innovation, Deliverables table

Expanded Provisioning- Deliverables

Key Releases	Description	Benefit	Users Impacted	Date
Authenticable Credentials for Machines	Provide provisioning support to allow academic research devices to have authenticable identities in order to access other devices and data repositories.	Improve Security of Machine to Machine Communications	Harvard Community	January 2017

Table 4.4.5 – Expanded Provisioning, Facilitate Technology Innovation, Deliverables table

Cloud Migration- Deliverables

Key Releases	Description	Benefit	Users Impacted	Date
Cloud Architectural Reference Model	A document that provides an overview of the IAM AWS cloud architecture.	Provide Best Practices	Harvard Community	July 2014
Connections	Migration of the Connections application to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	July 2014
Phonebook and Public LDAP	Migration of the phonebook and public-facing LDAP systems to AWS cloud environment.	Reduced Development Costs Improve Reliability of IAM Services	Harvard Community	October 2014
HU LDAP and Auth LDAP	Migration of the HU LDAP and AUTH LDAP systems to AWS cloud environment.	Reduce Development Costs Improved Reliability of IAM Services	Harvard Community	January 2015
Authentication	Migration of the CAS, PIN, and IdP applications to AWS cloud environment.	Reduce Development Costs Improve Reliability of IAM Services	Harvard Community	July 2015
MIDAS and IDDB	Migration of MIDAS and IDDB to the AWS cloud environment.	Reduce Development Costs Improve Reliability of IAM Services	Harvard Community	October 2015
IDGen	Migration of IDGen application to the AWS cloud environment.	Reduce Development Costs Improve Reliability of IAM Services	Harvard Community	October 2015

Self Service	Migration of self-service and other web service applications to AWS cloud environment.	Reduce Development Costs Improve Reliability of IAM Services	Harvard Community	January 2016
SailPoint	Migration of the SailPoint application environment to AWS cloud environment.	Reduce Development Costs Improve Reliability of IAM Services	Harvard Community	October 2016

Table 4.4.6 – Cloud Migration, Facilitate Technology Innovation, Deliverables table

5.0 Program Communication

The IAM Program will provide regular and targeted communication about the program status and progress at predefined intervals throughout the duration of the Program. A detailed Communications Plan will be developed by the IAM Strategy and Planning team and will provide an in depth overview and approach for internal and external communications. The table below summarizes a subset of key communications that will be addressed in the Communications Plan Deliverable:

Type of Communication	Communication Schedule	Communication Mechanism	Who Initiates	Recipient
Executive Status Dashboard	Monthly	Executive Committee Meeting	IAM Program Director	IAM Executive Team
ITCRB Project Status Report	Monthly	SharePoint Distribution	IAM Program Director	ITCRB team
External Facing Website	Monthly	Blog postings, Plan Updates	IAM Team	Public
User Requirements Dashboard	Monthly	IAM Lifecycle Committee Meeting School/Community Outreach Meetings	IAM Community Manager	IAM Lifecycle Committee
Program Level KPI Reporting	Monthly	Executive Committee Meeting	IAM Program Director	IAM Executive Committee
School Level KPI Reporting	Monthly	School Outreach Meetings	IAM Community Manager	Schools
IAM Metrics Dashboard	Daily	Application	IAM Team	IAM Team

Table 5.0.1 – IAM Program Communication table

Training

Minimizing disruption to the end user, by means of clear communication and coordinated training, is vital to the success of the Program. As each release is prepared for Production deployment, there will be an equal focus on communicating release features, impact to users, and new support requirements. The following table summarizes the training activities that are currently planned:

Training Activity	Description	Date
Online Training Modules	Develop YouTube videos and/or online training modules to introduce the new IAM product and processes to community and target end-user populations • Project General Publicity Video • Onboarding best practices and special topics • Sponsored and Service Account set-up by Service Desk • Overview of Account Management for All Users • Self Service Sponsored Account Requests • Dionysus User Guide	Beginning Spring 2014
Seminars for Internal Audiences	Present "town halls" for different communities of interest across the University to review impact of new processes and feature sets, as well as timeline of delivery. • FAS Department Administrators • CADM Department Administrators • School IAM Teams • HR Professionals • SIS Professionals	Beginning Spring 2014

Table 5.0.2 – IAM Training table

6.0 Benefits to the University

The implementation of an effective end-to-end IAM strategy, as envisioned in this document, will provide a solid foundation for supporting and fostering innovation and collaboration across all the Harvard Community. The benefits include:

- **Increased User Productivity** - Creating a shared understanding of identity management across the University will foster innovation and collaboration. Automatic creation of user access upon or before hire or registration will reduce onboarding delays. More standardization of processes and increased education and awareness will enhance efficiency and return valuable time to staff so that they can focus on supporting the core teaching and research mission.

- **Enhanced User Experience –** Well-defined University- supported processes will eliminate confusion over what's needed to grant access to protected resources, greatly increasing user satisfaction. Concerted efforts to increase awareness of IAM Services and best practices will result in a more knowledgeable user base and more realistic expectations of IAM systems. Access to a more fully populated Service Catalog will ensure wider use of all available resources.

- **Information Sharing Across Applications** - The identities and attributes stored within the IAM Systems will enable functionality such as shared calendars, common data, and integrated contacts lists among Schools and applications. Harvard participation in key international Identity Management bodies, such as InCommon, will ensure the University stays positioned for stays positioned for improving interoperability within and outside of the University.

- **Reduced Administrative Overhead –** Greatly enhanced provisioning to an increasing number systems reduces application owner and people administration overhead. Federation services eliminate the need for local identities for external users thus simplifying application administration. By expanding the IAM program to encompass more Schools we further reduce the number of identity and access stores. IAM support of cloud-based software-as-a-service offerings reduces the cost to provide services to the Harvard Community.

- **Increased Security Stature** - The ability to quickly provision and de provision access to resources, in addition to enhanced identity assurance (through features such as multi-factor authentication), will improve our security posture. The ability for the University to use IAM Business Intelligence and identity analytics will allow for improved risk management and strategic decision-making.

As described throughout this document, the challenges that the IAM Program seeks to address are myriad and experienced by users every day across the University and beyond. The benefits to Harvard of the successful execution of this plan will result in tools and processes that fulfill the needs of end users, application owners, and people administrators, and will also reduce costs and build a foundation for future innovation and expansion.

7.0 Appendix

Appendix A - Glossary

The following terms have been adapted from Wikipedia and Gartner's IT Glossary:

Access Management – The processes associate with the login of a user across a realm of applications or information repositories. It is important to note that the IAM services will authorize user access to protected resource, but will delegate the authorization decisions to the application.

Application Owner – The members responsible for deciding the business needs of the application with respect to IAM, work with the IAM group to determine how best to integrate the applications with IAM services to meet the business needs, and direct the configuration of the application.

Authentication – The process to validate that a person or entity is who they say they are. People commonly think of this as logging in.

Authorization – The process to determine if the current user has the right to access a service or perform an action.

CAS – The Central Authentication Service (CAS) is a single sign-on protocol for the web as well as an authentication engine implementation.

Credential – A credential is used by a person or entity to prove themselves to a system (e.g., a username/password combination).

Directory Service – A directory service is the software system that stores, organizes and provides access to information in a directory, for entities like people, groups, devices, resources, etc.

Federation - According to Gartner's IT Glossary, federated identity management is a technical implementation that "enables identity information to be developed and shared among several entities and across trust domains".

Identity and Access Governance – Identity and access governance tools establish a life cycle process for business owners of identities to have comprehensive governance of identities and access requests. It allows organizations identifies access risks and make sure access meets organization policies.

Identity Management – The processes and solutions that provide the creation and management of user information.

idP/Identity Provider – A system that validates the identity of a user in a federated system. The service provider uses it to get the identity of the current user.

Identity Stores - The underlying information associated with the user, across a variety of technologies including databases, LDAP, Active Directory, and text files.

InCommon - InCommon, operated by Internet2, provides a secure and privacy-preserving trust fabric for research and higher education, and their partners, in the United States. InCommon operates an identity management federation, a related assurance program, and offers certificate and multifactor authentication services.

People Administrator – A person who assigns roles, group memberships, and/or other attributes to a user.

Service Provider – A system that provides a generic service to the user in a federated system. To the user, it is the same thing as the application they are trying to use.

Sponsored Guest - A sponsored guest is defined as a user that currently does not have a standard affiliation with the University, but requires access to University information and resources. As the name implies, a sponsored guest access must be requested by a University staff or faculty member with the appropriate authorization to request this function.

User – The term "user" is used to generalize and reference multiple user types, such as Harvard users (e.g., staff, students, faculty), sponsored guests, Harvard application users, and users external to the University (e.g., faculty from other institutions). Where the distinction is pertinent to the context of the section, the user type will be referenced explicitly.

User Provisioning - According to the Gartner IT Glossary, user provisioning is defined as a set of technology that "creates, modifies, disables and deletes user accounts and their profiles across IT infrastructure and business applications."

Appendix B - IAM Program Accomplishments to Date

The IAM Program teams and work activities were consolidated in October 2013. A single program was launched to focus on meeting both the IAM needs of HUIT, as well as the needs of the University as a whole. The following list categorizes the activities that are complete, to-date.

Program Improvements

- Consolidated and centralized University IAM Program.
- Adopted the Agile Software Development Methodology to account for iterative requirement definition and test driven development practices.
- Focused on integrated IAM Planning and Strategy Development, including the finalization of a revised project and operational budget.

Simplify the User Experience

- Selected and purchased a new identity creation toolset that will lead to improved onboarding experience for all users.
- Implemented a new Central Authentication Service for faster, flexible deployment of applications across the University.
- Implemented One-Way Federation with the Harvard Medical School to prove the concept that users can select the credentials they would like to use, to access services.
- Implemented Provisioning improvements to set the foundation for the expansion of cloud services, support Active Directory consolidation, and email migrations.
- Integrated a new ID Card Application into IAM that enables the University to handle large-scale replacement of expired cards.

Enable Research and Collaboration

- Joined InCommon Federation and enabled authorized Harvard users to access protected resources at Hathitrust.
- Enabled access to a planning tool that Harvard researchers can use 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 Password Policy to the HUIT Security Organization to standardize password strength and expiration requirements for the University.
- Drafted a Cloud Security Architecture with the HUIT Security Organization to provide Level 4 security assurance for application deployments within Amazon Web Services.
- Refreshed the AUTH LDAP software and infrastructure to current, supported versions.

Facilitate Technology Change

- Created a conceptual architecture for IAM Services to be deployed within the Amazon's offsite hosting facilities.

Appendix C - IAM Program Timeline

<Attached>