HARVARD UNIVERSITY
Information Technology

Identity and Access Management
PROGRAM PLAN

Created January 2014 | **Revised June 2014**

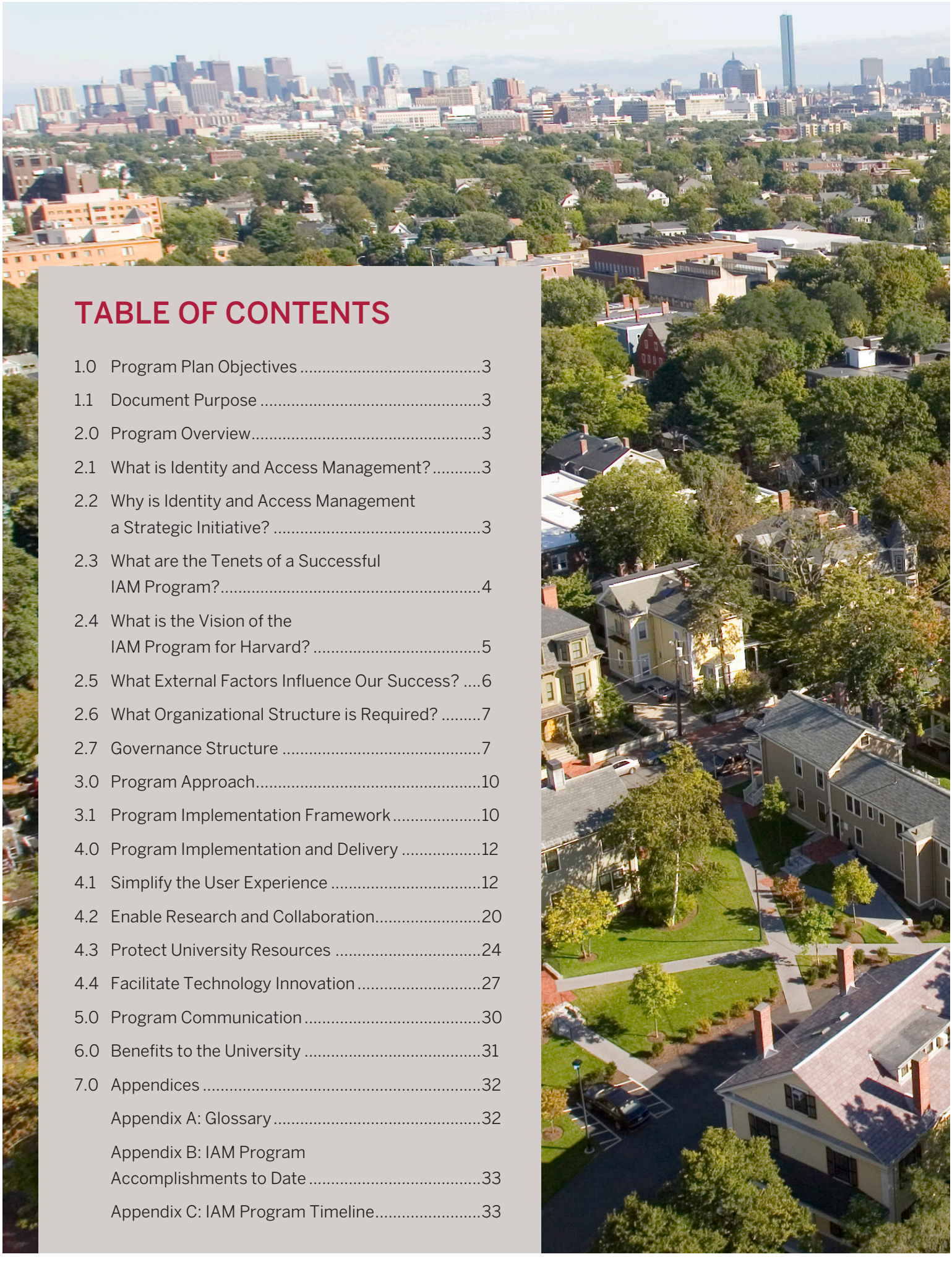
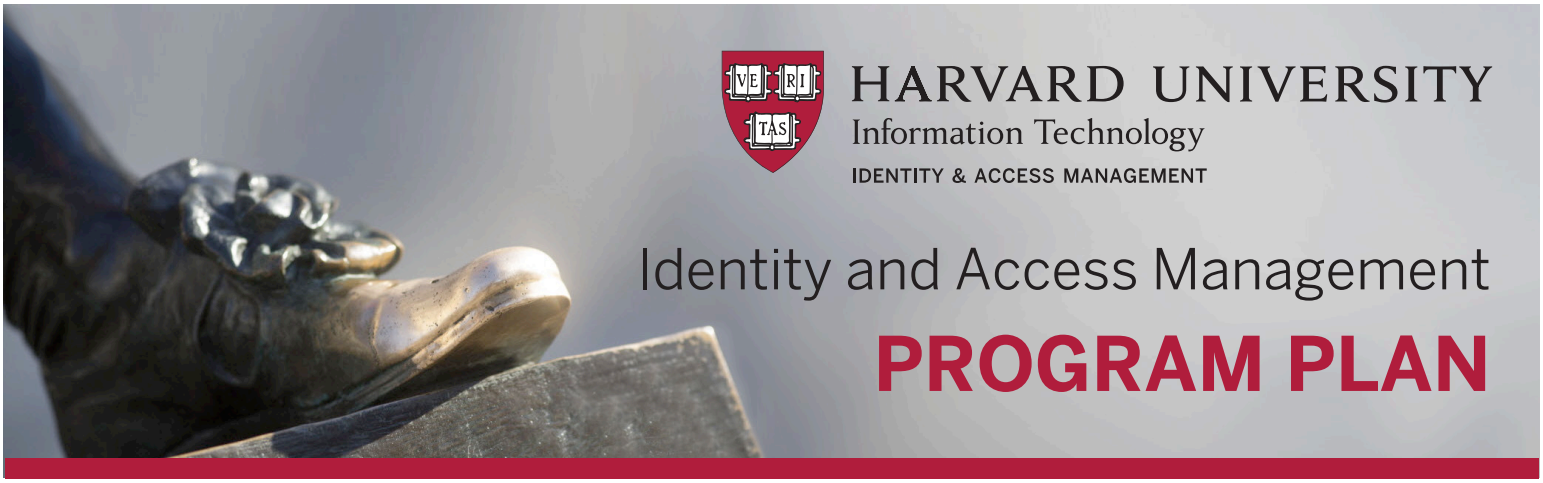


TABLE OF CONTENTS



HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

Identity and Access Management
PROGRAM PLAN

1.0 PROGRAM PLAN OBJECTIVE

1.1 Document Purpose

The purpose of this plan is to provide a comprehensive overview of all facets of the Identity and Access Management (IAM) program within 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 on a monthly basis, by means of an executive dashboard, to senior leadership and program stakeholders.

2.0 PROGRAM OVERVIEW

2.1 What is Identity and Access Management?

Identity and Access Management refers to 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 its related 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 may be helpful in understanding this program plan, please refer to Appendix A.

2.2 Why is Identity and Access Management a Strategic Initiative?

The first impression that any student, faculty member, researcher, or administrative staff member has of IT at Harvard is formed from his or her initial 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:** New users lose productivity and time as they wait for accounts to be created. Delays in users' ability to access resources often result when manual, paper-based workflows and approvals cannot be streamlined or easily orchestrated. There can often be lengthy wait times for users to gain access to resources they need, and have the right, to access.

- **Poor User Experience:** Issuing and managing 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:** Applications are unable to share information that should be shared, such as contact information, files, and common data for calendars and other frequently used functions.
- **Unnecessary Administrative Overhead:** The high volume of calls to the IT help desk to address basic account or application management functions, such as password management, creates an unnecessary burden on support staff.
- **Reduced Security Stature:** The inability to streamline the deprovisioning of users or 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 Information Technology is stigmatized as a direct result of the limitations of the current IAM solution set.

2.3 What are the Tenets of a Successful IAM Program?

The IAM program originated from the need to eliminate perceived complexities surrounding identity. Above all, the IAM program's activities and deliverables will focus on achieving this fundamental objective. Additionally, the program is designed to improve 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, people at the University cannot easily access, provide access to, or share information.

If implemented correctly, identity and access management should be simple and intuitive to an end user. Nevertheless, its importance as a core technical service should not be underrated.

In an ideal state, IAM enables new applications and services to be brought up quickly, provides necessary user information to applications so that they can properly function, and allows users to partake in new services 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 communities. In addition to enabling account creation and application access decisions, these identity assets 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 via continuous user identity despite affiliation changes.

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

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

IAM services will allow users 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 efforts will enable productivity by means of quick provisioning, granting user 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**

The Identity and Access Management program will facilitate collaboration. It will break down the barriers to access for end users, opening the ability to share information and work safely together across School and institutional boundaries. The IAM program 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, the IAM program will lay the groundwork to carefully share identity information that enables access to resources that cannot currently be viewed via any other means. It will provide the University with a competitive advantage over institutions that cannot offer the same level of ease and expediency — enticing students and faculty to come to or stay at Harvard 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, meeting 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 by eliminating the need for application developers to reinvent and duplicate potentially vulnerable authentication systems. IAM also removes the need for application owners to manage such duplicate systems. IAM helps weather the storm of disruptive innovation, including positioning the University to quickly and securely integrate with or implement cloud platforms and services.

> Good identity and access management practices help Harvard weather the storm of disruptive innovation, including positioning the University to quickly and securely integrate with or implement cloud platforms and services. IAM an important precursor to successfully implementing new University initiatives.

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

2.4 **What is the Vision of the IAM Program for Harvard?**

Simply stated, the vision of the IAM program is the following:

> **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.**

The IAM program will be implemented to fulfill this vision in accordance with the tenets defined above. Additionally, heightened emphasis will be placed upon a secondary set of guiding principles for the program:

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

Strategic objectives, guiding principles, and key performance indicators intended to guide the IAM program in achieving our vision are outlined below.

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 using a standard approach 4. **Facilitate Technology Innovation:** Establish a strong foundation for IAM to enable user access regardless of new or disruptive technologies	• Harvard Community needs will drive how technology supports the Identity and Access Management program • Tactical project planning will remain aligned with program strategic objectives • Solution design will allow for other Schools to use foundational services to communicate with IAM systems 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 IAM systems per month • The number of user logins and access requests via the IAM system per month • The number of production systems to which the IAM system provisions per month

Table 2.4.1: Strategic Objectives, Guiding Principles, and Key Performance Indicators

2.5 What External Factors Influence Our Success?

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 program to meet its goals, the following critical success factors must be closely managed:

Strategic Objectives	Guiding Principles
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, users within the School communities
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?

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 each team, its associated management, and its overall functional responsibilities are listed below.

Strategy and Planning Team (Erica Bradshaw)

The IAM Strategy and Planning Team is responsible for providing communication, strategic planning, and 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 (Jane 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 (Magnus 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 (Scott Bradner and Marlena 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 Governance Structure

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

Executive Committee

The primary objective for the IAM program's Executive Committee is to provide consistent, timely, and meaningful oversight for the Identity and Access Management program. The Executive Committee will identify and champion business process improvement, provide program oversight, and guide the strategy for implementation and rollout. 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's strategic objectives
• Provide direction for communication initiatives to stakeholders
• Determine prioritization of IAM program projects and strategic approaches
• Track the 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 will 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

Identity Lifecycle Committee

The mission of the Identity Lifecycle Committee is to work toward 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, as well as to serve as a catalyst for projects across the University that 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 teams 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 measurably improve onboarding and other lifecycle processes • Recommend IAM service enhancements and new offerings • Provide a forum for related policy discussion • Provide input on IAM product strategy • Serve as a sounding board for new ideas and approaches to providing identity and access management services • Help quantify the impact of proposed process changes and recommend implementation approaches	• 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 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 in process and decision making • Use criteria and metrics to evaluate ideas and measure them against desired outcomes • Accept uncertainty, ambiguity, and the absence of absolutes when necessary	• Approval of Prior Minutes • Chair's Report • Program Update • Requirements Discussion • Working Group Updates • General Discussion Topics

Table 2.7.2: IAM Identity Lifecycle Committee

Technical Oversight Committee

The primary objective for the Technical Oversight Committee is to provide consistent, timely, and meaningful review of proposals of architecture and standards for the IAM program. The committee will identify the need for technical solutions, architecture, and standards. When those have been developed, they will provide feedback as well as recommendation for adoption to the Executive Committee. It 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 a set of resources outside the IAM program Team to be involved in drafting architectures and standards • Coordinate around technical change management to ensure that 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 will 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 the lack of absolutes when necessary	• Approval of Prior Minutes • Chair's Report • Architecture • Standards • Working Group Updates • Proposal Review and Recommendations to Approve • General Discussion Topics

Table 2.7.3: IAM Technical Oversight Committee

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" delivery approach. This program plan will serve as the governing document, and all activities will be planned and managed in accordance with it. All releases will tie back to program strategic objectives, and each objective will be measurable. The development and delivery of IAM functionality will be iterative, following Agile processes, and based on evolving user requirements and stories. The scope of releases will be adjusted based upon changes in requirements and the evolving status of critical success factors.

Project Tracks

The IAM program will be broken down into 11 project tracks and tracked on a per-project basis. A project manager will be assigned to each track and will be responsible for both developing a project plan to govern work activities and reporting weekly status. The 11 projects are identified and summarized below.

Project	Description
SailPoint	Introduce improved user processes for account management. Replace an outdated solution with a new, feature-rich solution that can be expanded for local use by interested Schools across the University.
Federation	Enable Harvard users, users at Harvard-affiliated institutions, and non-Harvard users to collaborate and easily gain access to applications and resources both internal and external to the University.
Directory Services	Reduce the number of systems of record for user information while also expanding the data model and user attributes stored within the central IAM identity repository. This will allow for quick, consistent, and appropriate access across LDAP and Active Directory (AD) as well as web authentication protocols.
App Portal	Enable the Harvard application owner community to learn about and easily integrate applications and software services with central IAM services.
One-Way Federation	A series of authentication releases and School onboarding efforts to provide Harvard users with the flexibility to access applications using the credential of their choice.
Identity and Access Governance	Deliver visibility into IAM program metrics, new-user certification processes, and audit reporting. The project will evolve to encompass business intelligence and identity analytics to support risk management and strategic decision making.
Authentication Enhancements	Provide users with a simplified login experience, as well as enhanced security for sensitive data and applications.
Authorization Enhancements	Provide application owners and administrators with the ability to manage user access rights via groups, as well as the ability to manage authorization rules for access to an application or software service.
External Directories	Securely expose user identity information inside and outside of the University.
Expanded Provisioning	Enable identity creation, authentication, and account provisioning for non-person objects.
Cloud Migrations	Provide cloud reference architecture for Harvard application deployments, including migrating IAM services from on-premise hosting to Amazon Web Services.

Table 3.1.1: Project Tracks

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 manner in which the program will demonstrate this commitment to responsible experimentation is through controlled pilots both within the team and with willing participants. Quickly developing and testing 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 user requirements.

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

Proposed Pilot	Description	Proposed Date
One-Way Federation	Collaborate with Harvard Business School to enable one-way federation with the HBS authentication system	Anytime
Local Provisioning	Assist Harvard Medical School with SailPoint onboarding: • 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 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 (such as SailPoint or App Portal)	July 2015
Social Identities for Wireless Access	Allow use of social media identities (such as 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

4.0 PROGRAM IMPLEMENTATION AND DELIVERY

As previously mentioned, the IAM program will implement deliverables in accordance with four strategic objectives:

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

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

- **End Users:** A term used to generalize and reference multiple user types, such as Harvard users (i.e. staff, students, or faculty), sponsored guests, Harvard application users, or users external to the University (such as faculty from other institutions).
- **Application Owners:** Individuals responsible for deciding the business needs of their applications with respect to IAM. These members work with the IAM group to determine how best to integrate their applications with IAM services in order to meet business needs, as well as directing the configuration of their applications.
- **People Administrators:** Individuals who assign roles, group memberships, and/or other attributes to a user.

To date, the IAM program team has had a series of successful implementations that have delivered proven value to the Harvard Community. For a list of IAM program accomplishments, please refer to Appendix B.

The following sections identify the program's remaining 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

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. Since this community 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.

Key Benefits: End Users

The following table summarizes the key benefits of IAM program deliverables for end users across the University with regard to simplifying user experience.

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

Table 4.1.1: Simplify the User Experience — Key Benefits for End Users

Key Benefits: Application Owners

The following table summarizes the key benefits to application owners of IAM program deliverables, simplifying the user experience for IAM services across the University.

Key Benefit	Description
1. Simplify Application Setup	I. Application Owners will use an online portal to 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 info, 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 identifiers and attributes, with less development work. III. An Application Owner can easily manage groups that can be used for controlling access to the application.

Table 4.1.2: Simplify the User Experience — Key Benefits for Application Owners

Key Benefits: People Administrators

The following table summarizes the key benefits of IAM program deliverables for administrators of identities with regard to simplifying the user experience for IAM services across Harvard.

Key Benefit	Description
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 (such as types of non-employee, non-student users, or contractors): a. Sponsors will be able to see in SailPoint the list of people they have sponsored — including each person's role(s) and start/end dates for these role(s) — as well as extend access online b. Sponsors will be able to manage each sponsored person's access to systems and applications through SailPoint III. Provide an enhanced online means of discovering if a "new" user actually has an existing identity at the University. This results in fewer duplicate identities and accounts, as well as allowing end users to keep their existing credentials. IV. Enable bulk requests for account creation.
2. Reduce Number of User Management Toolsets	I. Enable person administrators to use a single tool to do more of the work required to give users needed access. This tool will also allow person administrators 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 access control. II. Allow for a given change to affect a set of users rather than forcing separate operations and multiple administrative updates for each user.

Table 4.1.3: Simplify the User Experience — Key Benefits for People Administrators

Deliverables

The following set of tables identify the key deliverables for the IAM program, organized by project.

SailPoint: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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 an internal, provisioning readiness release to transition from original 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 SailPoint functionality: • 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 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: Simplify the User Experience — SailPoint Deliverables

Directory Services: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
UUID Enhancement	Provide programmatic interfaces to Schools to allow Schools, applications, or organizations to find user UUIDs using 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 (AD) 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: Simplify the User Experience — Delivery Services Deliverables

App Portal: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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 Setup	Harvard Community	February 2015
Developer Sandbox Release	Update the App Portal to provide "turnkey" environments for testing applications with IAM services.	Simplify Application Setup Reduce Security Development Burden	Harvard Community	July 2015

Table 4.1.6: Simplify the User Experience — App Portal Deliverables

Authentication Enhancements: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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 (CAS) to support additional protocols: • Allow participation from federated organizations	Simplify Application Setup 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: Simplify the User Experience — Authentication Enhancements Deliverables

Authorization Enhancements: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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: Simplify the User Experience — Authorization Enhancements Deliverables

External Directories: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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, such as 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 in development efforts.	Expand Access to Resources	Harvard Community	June 2016
Yellow Pages Improvements	Create a new web application providing an enhanced internal directory for department information.	Expand Access to Resources Increase Self-Service	Harvard Community	June 2017

Table 4.1.9: Simplify the User Experience — External Directories Deliverables

Expanded Provisioning: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
Dionysus Update	Release updated Dionysus application for management of devices in University AD: • Updates to modern platform and functional enhancements • Simplify architecture • Migrate to the cloud	Simplify Account Setup	FAS, GSD, HDS, GSE, SPH, Central, HKS, SEASE	May 2014

Table 4.1.10: Simplify the User Experience — Expanding Provisioning Deliverables

4.2 Enable Research and Collaboration

Strategic Objective Reference

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 — as such, 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 who rely on IAM services. IAM services will support inter-faculty initiatives for research and collaboration.

Key Benefits: End Users

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

Key Benefit	Description
1. Increase Self-Service	I. Provide online, automated functionality for self-service creation of sponsored guests.
2. Improve Collaboration Across School and Institutional Boundaries	I. Allow the use of local School credentials for access to data and applications across the University. II. Allow the use of local School credentials for access to data and applications at outside institutions. III. Allow for external users to transition to a Harvard affiliation from other higher education institutions without disrupting 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 (such as HathiTrust). II. Provide the capability for users to share access to physical resources, such as computing clusters or lab equipment, for teaching and research. III. Provide the capability for users to access collaboration resources such as email, online forums, and secure file transfer.

Table 4.2.1: Enable Research and Collaboration — Key Benefits for End Users

Key Benefits: People Administrators

The following table summarizes the key benefits of the IAM program for people administrators with regard to enabling research and collaboration across the University.

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

Table 4.2.2: Enable Research and Collaboration — Key Benefits for People Administrators

Key Benefits: Application Owners

The following table summarizes key research and collaboration benefits of the IAM program for application owners.

Key Benefit	Description
1. Reduce Local Administrative Overhead	I. Enable user provisioning to local applications for easier management of access privileges for 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 emerging identity assurance attributes for increased confidence in user identity.
3. Reduce Complexity of IAM Integration	I. Reduce the complexity of application integration with third-party providers by using standard InCommon identifiers and attributes.
4. Expand Access to Resources	I. Facilitate the integration with a spectrum of research and collaboration applications through membership in InCommon.
5. Incorporate Discoverability	I. Incorporate researcher identifiers into directory services to enable global tracking of authorship of published resources (such as ORCID).

Table 4.2.3: Enable Research and Collaboration — Key Benefits for Application Owners

Deliverables

The following set of tables identifies the key deliverables for the IAM program, organized by project.

SailPoint: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
Foundation	Enable the HUIT help desk to use the new sponsored guest capabilities with existing Schools.	Reduce Manual Processes for Guest Sponsorship	FAS, GSD, HDS, GSE, SPH, Central	July 2014
HUIT Expansion	Enable people administrators for FAS- and HUIT-supported Schools by expanding SailPoint IIQ functionality for sponsored guest workflow from existing users: • Self-service creation of sponsored accounts replaces paper-based • 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 SailPoint functionality for sponsored guest workflow (such as 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 with Microsoft 0365 with SailPoint provisioning. • Deliver shared contacts and calendaring	Reduce Local Administrative Overhead Simplify User Access Management	FAS, GSD, HDS, GSE, SPH, Central, SEAS, HKS	May 2016

Table 4.2.4: Enable Research and Collaboration — SailPoint Deliverables

Federation: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
InCommon Deployment	Provide a means to federate with other external entities in a standardized manner using 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 Simplified Application Setup	Harvard Community External Communities	January 2016
Federation for Hospitals	Federate with the hospitals. Implement OWF or work with 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: Enable Research and Collaboration — Federation Deliverables

Directory Services: Deliverables

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

Table 4.2.6: Enable Research and Collaboration — Directory Services Deliverables

One-Way Federation: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
eCommons ID	Implement one-way federation to enable users to authenticate using their eCommons 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 to integrate their School base identities with the central administrative applications served by PIN.	Expand Access to Resources	Harvard Community	February 2015

Table 4.2.7: Enable Research and Collaboration — One-Way Federation Deliverables

Authentication Enhancements: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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 use their own existing identity (LinkedIn, Google, etc.) to access appropriate University resources.	Enable Choice of Identity	Executive Education External Communities	January 2017

Table 4.2.8: Enable Research and Collaboration — Authentication Enhancements Deliverables

Authorization Enhancements: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
Group Management	Implement the 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: Enable Research and Collaboration — Authorization Enhancements Deliverables

Expanded Provisioning: Deliverables

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

Table 4.2.10: Enable Research and Collaboration — Expanded Provisioning Deliverables

4.3 Protect University Resources

Strategic Objective Reference

Improve the security stature of the University using a standard approach.

Overview

In order to ensure compliance with federal and state regulations as well as 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, deprovision user access in a more efficient manner, and perform a continuous review of entitlements without having to perform extensive application analyses.

Key Benefits: End Users

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

Key Benefit	Description
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 in order to limit unauthorized access to a user's data.
3. Improve Privacy	I. Ensure the privacy of sensitive identity information.

Table 4.3.1: Protect University Resources — Key Benefits for End Users

Key Benefits: Application Owners

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

Key Benefit	Description
1. Reduce Security Development Burden	I. Provide lower application development environments (such as sandboxes) with IAM services that do not contain personally identifiable information. II. Provide application owners with standard authentication libraries to reduce the 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 the capability to track user activities within applications.
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: Protect University Resources — Key Benefits for Application Owners

Key Benefits: People Administrators

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

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

Table 4.3.3: Protect University Resources — Key Benefits for People Administrators

Deliverables

The following tables identify the key deliverables for the IAM program, organized by project.

SailPoint: Deliverables

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

Table 4.3.4: Protect University Resources — SailPoint Deliverables

Federation: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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: Protect University Resources — Federation Deliverables

Directory Services: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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: Protect University Resources — Directory Services Deliverables

Identity and Access Governance: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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 Toolset	Introduce business intelligence capabilities and analytics to support strategic decision-making and identification of areas of risk: • Pilot the use of SailPoint dashboards and out-of-the-box reports • Evaluate strategic benefits	Limit Unauthorized Access to User 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 Data Improve Situational awareness	Harvard Community	June 2017

Table 4.3.7: Protect University Resources — Identity and Access Governance Deliverables

Authentication Enhancements: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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: Protect University Resources — Authentication Enhancements Deliverables

Authorization Enhancements: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
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 Quickly Revoke User Access 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 Data	Harvard Community	June 2017

Table 4.3.9: Protect University Resources — Authorization Enhancements Deliverables

4.4 Facilitate Technology Innovation

Strategic Objective Reference

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, the IAM program launches pilots and adopts emerging technologies, such as cloud computing, to create guidance and establish best practices for the University to use for enterprise-wide implementations. By keeping apprised of emerging standards and systems, the IAM program offers an expanding array of services to application owners, developers, and administrators. This positions the University to be a leader in technology innovation.

Key Benefits: End Users

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

Key Benefit	Description
1. Improve Reliability of IAM Services	I. Leverage Amazon Web Services for hosting IAM services in order to increase the agility of service enhancements and improve the uptime of application authentication services.
2. Expand Integration with Desktop	I. Streamline user login experience to workstations and desktop applications.
3. Enable Choice of Identity	I. Allow users to use social media identity to access Harvard resources. II. Implement SocialSAML and OpenID Connect for authentication.

Table 4.4.1: Facilitate Technology Innovation — Key Benefits for End Users

Key Benefits: Application Owners

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

Key Benefit	Description
1. Reduce Development Costs	I. Reduce the costs associated with infrastructure deployment by taking advantage of cloud offerings and economies of scale.
2. Provide Best Practices	I. Provide guidance, best practices, and lessons learned for future Harvard implementers of cloud application hosting at Amazon Web Services.
3. Reduce Administrative Overhead and Development Time	I. Mobile app owners will be able to integrate with Harvard credentials using CAS/PIN.
4. Improve Security of Machine-to-Machine Communications	I. Verify that an initiating machine is who it asserts it is. II. Provide identities to non-standard users, such as user communities or resources (such as microscopes).
5. Improve Situational Awareness	I. Perform automated alerting and take action without human intervention.

Table 4.4.2: Facilitate Technology Innovation — Key Benefits for Application Owners

Key Benefits: People Administrators

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

Key Benefit	Description
1. Improve Reliability of IAM Services	I. Leverage Amazon Web Services for hosting IAM services in order 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 credentials to manage and reduce configuration errors by integrating the desktop login with the overall IAM solution.

Table 4.4.3: Facilitate Technology Innovation — Key Benefits for People Administrators

Deliverables

The following tables identify the key deliverables for the IAM program, organized by project:

Authentication Enhancements: Deliverables

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

Table 4.4.4: Facilitate Technology Innovation — Authentication Enhancements Deliverables

Expanded Provisioning: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
Authenticable Credentials for Machines	Provide provisioning support for 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: Facilitate Technology Innovation — Expanded Provisioning Deliverables

Cloud Migration: Deliverables

Deliverable	Description	Benefit	Users Impacted	Delivery
Cloud Architecture Reference Model	Document providing an overview of the IAM AWS cloud architecture.	Provide Best Practices	Harvard Community	May 2014 *(completed)*
Connections	Migrating the Connections application to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	July 2014
Phonebook and Public LDAP	Migrating the phonebook and public-facing LDAP systems to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	October 2014
HU LDAP and Auth LDAP	Migrating the HU LDAP and AUTH LDAP systems to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	January 2015
Authentication	Migrating the CAS, PIN, and IdP applications to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	July 2015
MIDAS and IDDB	Migrating MIDAS and IDDB to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	October 2015
IDGen	Migrating the IDGen application to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	October 2015
Self-Service	Migrating self-service and other web service applications to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	January 2016
SailPoint	Migrating the SailPoint application environment to the AWS cloud environment.	Reduced Development Costs Improved Reliability of IAM Services	Harvard Community	October 2016

Table 4.4.6: Facilitate Technology Innovation — Cloud Migration Deliverables

5.0 PROGRAM COMMUNICATION

The IAM program will provide regular, targeted communication about status and progress throughout its duration. A detailed communications plan will be developed by the IAM strategy and planning team with an in-depth overview and approach for internal and external communications. The table below summarizes key communications in the plan:

Type of Communication	Frequency	Mechanism	Initiated By	Recipient
Executive Status Dashboard	Monthly	Executive Committee meeting	Program Director	Executive Team
ITCRB Project Status Report	Monthly	SharePoint distribution	Program Director	ITCRB team
External-Facing Website	Monthly	Blog postings, plan updates	IAM Team	Public
User Requirements Dashboard	Monthly	Lifecycle Committee meeting School/community outreach meetings	Community Manager	Lifecycle Committee
Program-Level KPI Reporting	Monthly	Executive Committee meeting	Program Director	Executive Committee
School-Level KPI Reporting	Monthly	School outreach meetings	Community Manager	Schools
IAM Metrics Dashboard	Daily	Application	IAM Team	IAM Team

Table 5.0.1: IAM Program Communications

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, user impact, and new support requirements. The following table summarizes training activities:

Training Activity	Description	Date
Online Training Modules	Develop videos and/or online training modules to introduce new IAM products and processes to community and target end-user populations • Project general publicity video • Onboarding best practices and special topics • Sponsored and service account setup 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 communities of interest across the University to review delivery timelines and the impact of new processes and features. • FAS department administrators • CADM department administrators • School IAM teams • HR professionals • SIS professionals	Beginning Spring 2014

Table 5.0.2: IAM Training

6.0 BENEFITS TO THE UNIVERSITY

Implementing 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 the entirety of the Harvard Community. The benefits of implementing this project plan include:

- **Increased User Productivity:** Creating a shared understanding of identity management across the University will foster innovation and collaboration. Automatic provisioning of user access upon or before hire or registration will reduce onboarding delays. Further 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 is needed in order to grant access to protected resources, thereby 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 the wider use of all available resources.
- **Information Sharing Across Applications:** Identities and attributes stored within IAM systems will enable functionality such as shared calendars, common data, and integrated contact lists among Schools and applications. The University's participation in key international identity management bodies, such as InCommon, will ensure that Harvard stays positioned for improving interoperability within and outside of the University.
- **Reduced Administrative Overhead:** Greatly enhanced provisioning to an increasing number of 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 will further reduce the number of identity and access stores. IAM program support of cloud-based software-as-a-service offerings also reduces the cost to provide services to the Harvard Community.
- **Increased Security Stature:** The ability to quickly provision and deprovision access to resources, in addition to enhanced identity assurance through features such as multifactor 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.

The challenges that the IAM program seeks to address are myriad and experienced by users every day across and beyond the University. The benefits to Harvard include tools and processes that fulfill the needs of end users, application owners, and people administrators, while also reducing costs and building a foundation for future innovation and expansion.

As described throughout this document, the challenges that the IAM program seeks to address are myriad and experienced by users every day across and beyond the University. 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, while also reducing costs and building a foundation for future innovation and expansion.

7.0 APPENDICES

Appendix A: **Glossary**

Where appropriate, the following terms have been adapted from Wikipedia and the Gartner IT Glossary.

Access management The processes associated with a user's login across a realm of applications or information repositories. It is important to note that IAM services will authorize user access to protected resources, but will delegate the authorization decisions to the applications themselves.

Application owner The members responsible for deciding the business needs of a given application with respect to IAM. These members work with the IAM program team to determine how best to integrate their applications with IAM services in order to meet business needs, as well as directing the configuration of their applications.

Authentication The process of validating that people or entities are who they say they are. Authentication is commonly referred to as "logging in."

Authorization The process of determining if a user has the right to access a service or perform an action.

Central Authentication Service (CAS) A "single sign-on" protocol for the web, as well as an authentication engine implementation.

Credential An Item — such as a username/password combination — used by a person or entity to prove him/her/itself to a system.

Directory service The software system that stores, organizes, and provides access to information in a directory for entities such as people, groups, devices, resources, etc.

Federation Also known as federated identity management, this 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 lifecycle process that allows business owners of identities to have comprehensive governance of identities and access requests. It allows organizations to identify access risks and make sure access meets organization policies.

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

Identity provider (idP) A system that validates the identity of a user in a federated system. The service provider (or SP; see below) uses the idP to get the identity of the current user.

Identity stores Underlying information associated with users and stored across a variety of technologies, including databases, LDAP, Active Directory, text files, etc.

InCommon Operated by Internet2, InCommon provides a secure and privacy-preserving trust fabric for U.S. research and higher education institutions and their partners. InCommon operates an identity management federation and 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 (SP) A system that provides a generic service to the user in a federated system. To users, a service provider is the same thing as the application they are trying to use.

Sponsored guest 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, sponsored guest access must be requested by a University staff or faculty member with the appropriate authorization.

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

User provisioning 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**

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 an improved onboarding experience for all users.
- Implemented a new Central Authentication Service for faster, more flexible deployment of applications across the University.
- Implemented one-way federation with Harvard Medical School as proof of concept that users may select the credentials of their choice in order to access services.
- Implemented provisioning improvements to set the foundation for expanding cloud services, supporting Active Directory consolidation, and migrating email.
- 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 the 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 in compliance of funding requirements specific to grants (such as grants from the NSF, NIH, and 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 Amazon's offsite hosting facilities.

Appendix C: **IAM Program Timeline**

Please see attached for the most recently updated version of the program timeline.