HARVARD UNIVERSITY
Information Technology

Identity and Access Management

Technical Oversight Committee

October 2, 2014 | Thursday | 3-4 P.M. | 6 Story Street, Ground Floor

Agenda

- Meeting Purpose and Intended Outcome
- Approval of Previous Minutes
- Chair’s Report
- Shared Topics of Interest: Expansion of Identity Data Model
- Shared Topics of Interest: Identity Service
- Shared Topics of Interest: Connecting to Local Targets
- Shared Topics of Interest: Database to Cloud
- General Discussion

Meeting Purpose and Intended Outcome

Purpose

- Present the latest status of the IAM Program Plan
- Examine how an organization can prepare for integration with SailPoint IIQ

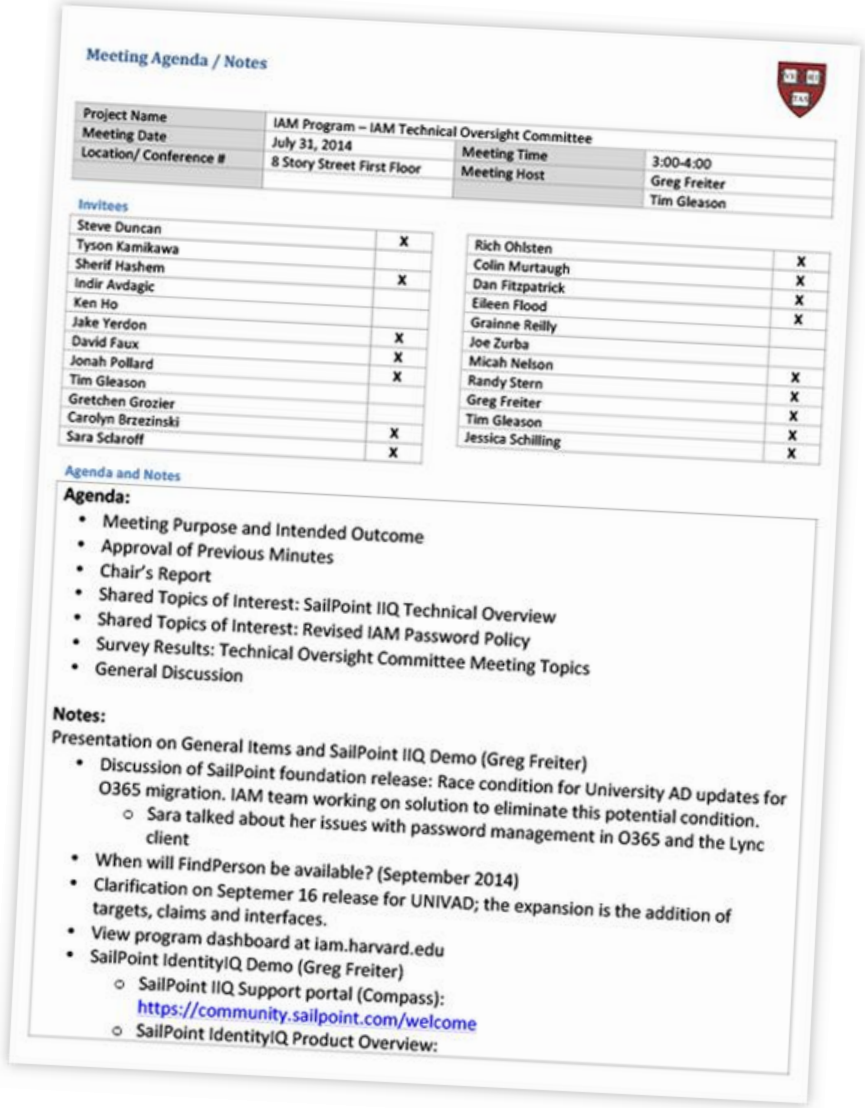
Intended Outcome

- The ability to start preparation for integration with SailPoint IIQ

Approval of Previous Minutes

July 31 Meeting

- Status updates: Change of focus to Provisioning and Directory projects — December 2015
- SailPoint IIQ Demo
- Revised Password Policy
- **Action Item:** FindPerson documentation. http://tinyurl.com/findperson-api
- **Action Item:** Security classification of IIQ hosts? *Category 4 classification.*
- **Action Item:** Preparation by schools for integration with IIQ? *Will be covered in this presentation.*
- **Action Item:** Cloud for AD environments? *Will be piloted this fall in lower environments.*



Meeting Agenda / Notes

Project Name	IAM Program – IAM Technical Oversight Committee		
Meeting Date	July 31, 2014	Meeting Time	3:00-4:00
Location/ Conference #	8 Story Street First Floor	Meeting Host	Greg Freiter
			Tim Gleason

Invitees

Steve Duncan		Rich Ohlsten	
Tyson Kamikawa	X	Colin Murtaugh	X
Sherif Hashem		Dan Fitzpatrick	X
Indir Avdagic	X	Eileen Flood	X
Ken Ho		Grainne Reilly	X
Jake Yerdon		Joe Zurba	
David Faux	X	Micah Nelson	
Jonah Pollard	X	Randy Stern	X
Tim Gleason	X	Greg Freiter	X
Gretchen Grozier		Tim Gleason	X
Carolyn Brzezinski		Jessica Schilling	X
Sara Sclaroff	X		X
	X		

Agenda and Notes

Agenda:

- Meeting Purpose and Intended Outcome
- Approval of Previous Minutes
- Chair's Report
- Shared Topics of Interest: SailPoint IIQ Technical Overview
- Shared Topics of Interest: Revised IAM Password Policy
- Survey Results: Technical Oversight Committee Meeting Topics
- General Discussion

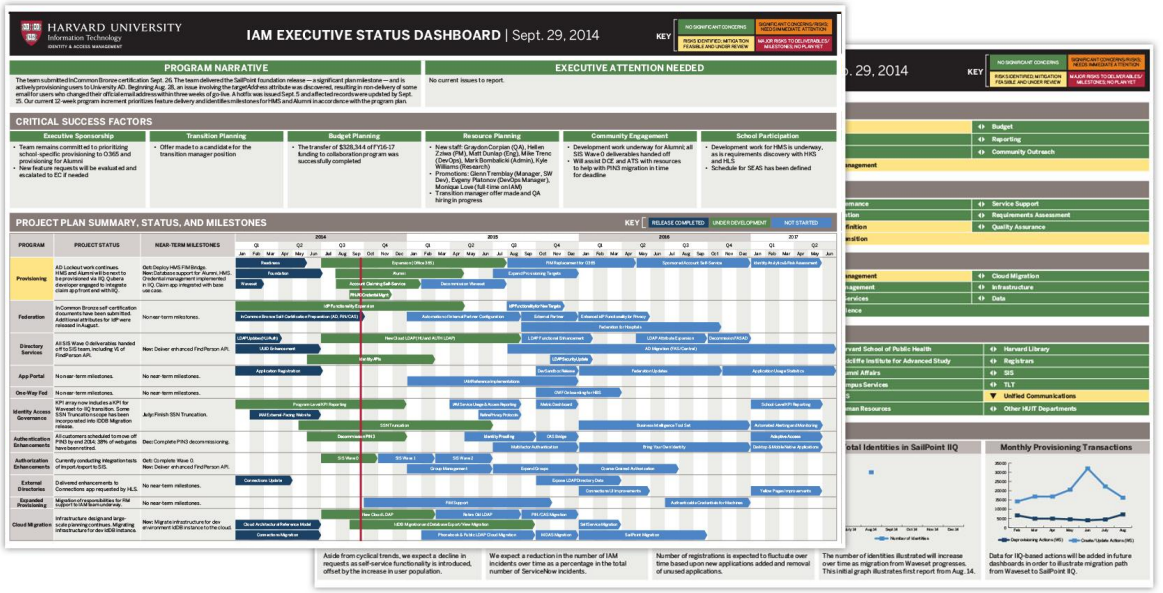
Notes:

Presentation on General Items and SailPoint IIQ Demo (Greg Freiter)

- Discussion of SailPoint foundation release: Race condition for University AD updates for O365 migration. IAM team working on solution to eliminate this potential condition.
  - Sara talked about her issues with password management in O365 and the Lync client
- When will FindPerson be available? (September 2014)
- Clarification on Septemer 16 release for UNIVAD; the expansion is the addition of targets, claims and interfaces.
- View program dashboard at iam.harvard.edu
- SailPoint IdentityIQ Demo (Greg Freiter)
  - SailPoint IIQ Support portal (Compass): https://community.sailpoint.com/welcome
  - SailPoint IdentityIQ Product Overview:

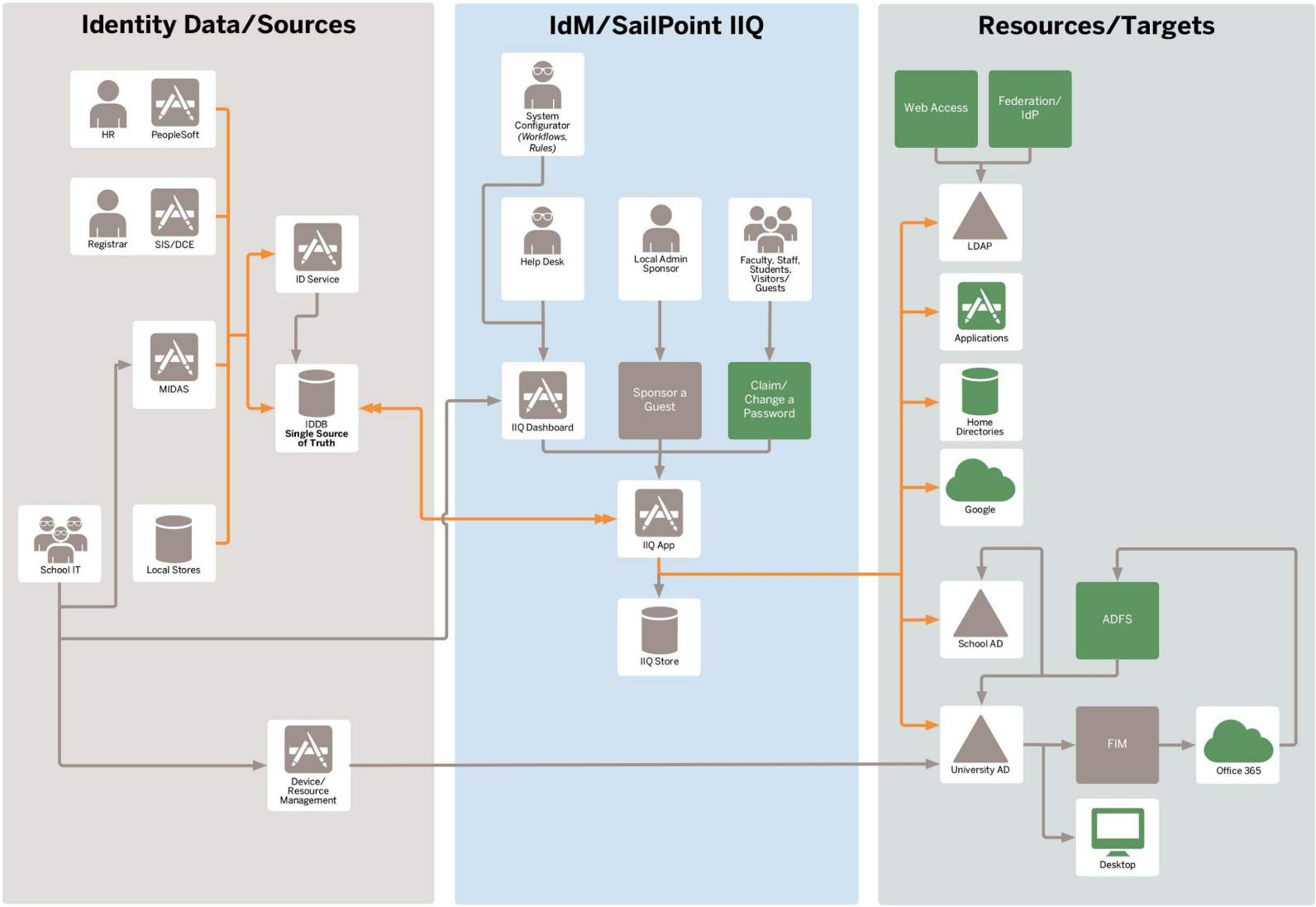
Chair's Report: September Executive Committee Meeting

See the latest Executive Status Dashboard at iam.harvard.edu/executive-dashboard.



- Program Status: Green
- Active provisioning of users to University AD via SailPoint continues
- Next PI prioritizes feature delivery and identifies milestones for HMS and Alumni
- Submitted InCommon Bronze certification documents
- PIN3 decommissioning continues as planned with extra help provided to FAS Registrar and DCE

SailPoint IIQ Technical Overview: Workflow



Shared Topics of Interest: Expansion of Identity Data Model

The role of IdDB as a "Single Source of Truth":

- All provisioning of accounts and resources will be driven from IdDB
- Any data that will be used to make decisions about provisioning, or data that needs to be in targets, needs to be in (or derived from) IdDB

The Identity Data Model needs to be expanded where gaps exist:

- Use current Identity Data Model as the foundation
- Roles (such as Alumni roles) may need to be expanded
- Attributes (such as titles for HMS) that are either general or attached to roles may need to be expanded
- Normalization rules may need expanding as data comes from more places

Shared Topics of Interest: Expansion of Identity Data Model

Process for onboarding a School or organization:

- Create a catalog of all data items used or needed for provisioning: eligibility, attributes, value ranges, directory …
- Map data items to existing data items in IdDB
- Design data model expansion for the gaps between needed and existing items

How to prepare for integration as a School or organization?

- Creating the catalog of needed data items is a critical first step, and you can do this now
- IAM is preparing a template of sample questions to help you identify data items

Shared Topics of Interest: Expansion of Identity Data Model

An example:

1. Define a new *EMAIL_ADDR_TYPE* value to identify the Alumni email address:
   a. Add row to *IDMRW.CD_CONTACT_EMAIL_ADDR_TYPE*
      i. *EMAIL_ADDR_TYPE='ALUMNI'*
      ii. *EMAIL_ADDR_TYPE_DESC='Alumni Preferred Email Address'*
   b. Add *CD_CONTACT_EMAIL_ADDR_TYPE* to the code tables XML export
2. Define three new Address Types:
   a. Add rows to *CD_CONTACT_ADDR_CATEGORY*
      i. *ALUMHOME* Alumni Home Address
      ii. *ALUMSEAS* Alumni Seasonal Address
      iii. *ALUMBUS* Alumni Business Address
3. Add two-character COUNTRY ISO codes to *CD_CONTACT_COUNTRY_ISO*:
   a. Add column *ADDR_ISO_COUNTRY_CD2 CHAR(2)* to *CD_CONTACT_COUNTRY_ISO (IDMRW and IDMRW2)*
   b. Create script to populate column
   c. Add trigger to synch changes to this table into corresponding table in IDMRW2
   d. Possibly add a not-null constraint (IDMRW and IDMRW2)

Shared Topics of Interest: Expansion of Identity Data Model

(Example continued …)

4. Add two new name types:
   a. Add trigger to *CD_PERSON_NAME_TYPE* to propagate updates to IDMRW2
   b. Add rows to *CD_PERSON_NAME_TYPE*
      i. *ALUMNI* Preferred Alumni Name
      ii. *ORIGINAL* Original Name

5. Create new table *PERSON_ROLES_ALU* to IDMRW:
   a. Include trigger to push changes to IDMRW2
   b. Assign names to all constraints, including not-null constraints

6. Create new table *PERSON_ROLES_ALU_DTL* to IDMRW2:
   a. Add new partition to *IDMRW2.PERSON_ROLES* for *ROLE_ILK='alu'*

Shared Topics of Interest: Expansion of Identity Data Model

- Example — new table such as *cd_role_alu_degree*:

ALUMNI_DEGREE_CD	VARCHAR2(10)	Not Null	Alumni-specific degree code
ALUMNI_DEGREE_DESC	VARCHAR2(50)	Not Null	Description for Alumni-specific degree code
EFF_STATUS	VARCHAR2(1)	Not Null	A for Active, I for Inactive
EFF_DT	TIMESTAMP	Not Null	
UPDATE_BY	VARCHAR2(8)	Null	
UPDATE_SOURCE	VARCHAR2(50)	Not Null	
UPDATE_DT	TIMESTAMP	Not Null	

Shared Topics of Interest: Identity Service

The role of the Identity Service is to manage the identities in the IdDB, a.k.a. the "Single Source of Truth".

- Service includes FindPerson and Create/Manage ID (previously discussed)
- Service also includes interfaces to manage role and attribute data
- As the new service is built out, it will replace current XML-based imports

The Identity Service is built iteratively.

- The service will be built and expanded by use case
- If an existing customer uses a service that needs to change, the interface will be versioned and will not require change for the customer
- Service expansion will be based on the work done for the expansion of the data model

Shared Topics of Interest: Identity Service

Process for onboarding a School or organization:

- On top of the expansion of data model work, identify the source of data not currently residing in IDDB, the workflow for data updates, and the ability of those sources to update data using an API
- Design the expansion of the Identity Service based on the above and the expansion of the data model

How to prepare for integration as a School or organization?

- Document the sources of data currently not residing in IDDB, the workflow of data updates, and the ability for those sources to use an API to update data
- IAM is preparing a template of sample questions to help you identify data sources, update workflow, and API readiness

Shared Topics of Interest: Identity Service

Alumni API design is still in development. An example of how it will look can be represented via the FindPerson API developed for SIS. Examples follow ...

- Example — Find Person by HUID:

GET /people/huid:12123467


```
{
        "status":"OK",
        "resultValue":{
                "resultSource":"HUIDA",
                        "huid":"12123467",
                "birthDate":"1973-08-09",
                "lastFourNationalId":"5555",
                "names":[{
                        "nameFirst":"John",
                        "nameLast":"Dow",
                        "nameType":"F"
                }]
        }
}
```

Shared Topics of Interest: Identity Service

- Example — Create Person if not present:

POST /people
firstName=art&lastName=abbb&birthDate=19991122&lastFourNationalId=4445


```
{
        "status":"OK",
        "resultValue":{
                "resultSource":"IDMRW",
                "huid":"10964741",
                "uuid":"77229f9694f84794b8f350dfd03a9a18",
                "birthDate":"1999-11-22",
                "lastFourNationalId":"4445",
                "names":[
                        {"nameFirst":"art","nameLast":"abbb","nameType":"OFFICIAL"}
                ]
        }
}
```


View the Find Person API Guide here:
http://tinyurl.com/findperson-api

Shared Topics of Interest: Connecting to Local Targets

"Connectors" in IIQ allow us to provision accounts in local targets.

- IIQ comes with 90+ connectors out of the box, and your local target (AD, LDAP, Exchange, Google, etc.) is likely to be supported
- Connectors must be configured/customized to adhere to the target's business rules (provisioning/deprovisioning events, attributes, access, privacy, licensing, etc.)

Connectors are added iteratively.

- As each School/organization is onboarded, new connectors will be configured for them
- Provisioning/deprovisioning events will be driven by data in IdDB, and who gets provisioned to what will be based on those attributes (drives what community you belong to)

Shared Topics of Interest: Connecting to Local Targets

Process for onboarding a School or organization:

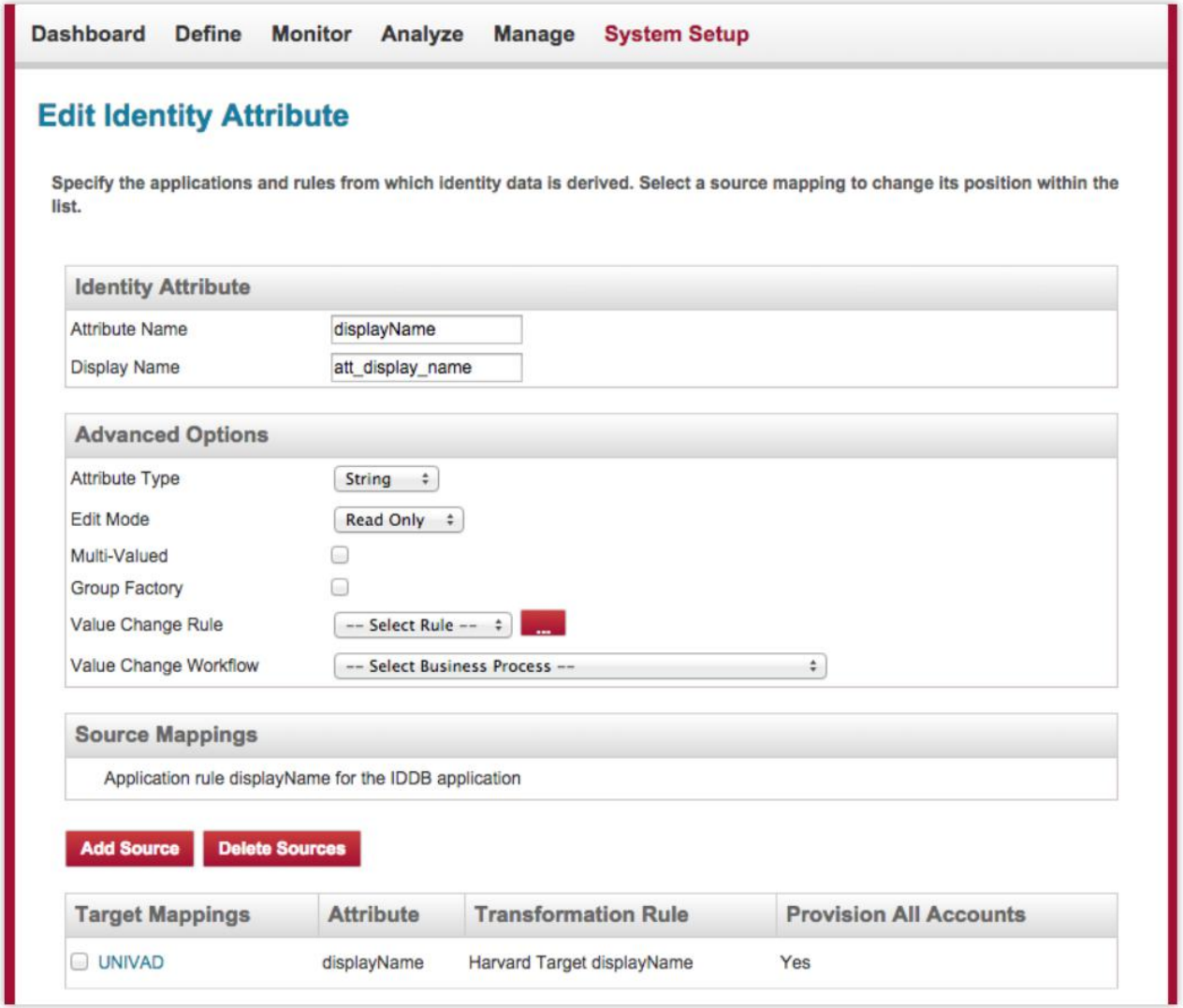
- On top of the expansion of data model work, define communities of users for which there are different rules
- Describe what each of those communities will be provisioned to
- List all the details around those provisioning events (attributes, access, privacy, licensing, etc.)

How to prepare for integration as a School or organization?

- Document the above communities, uses, and details
- IAM is preparing a template of sample questions to help you identify these

Shared Topics of Interest: Connecting to Local Targets

An example ...



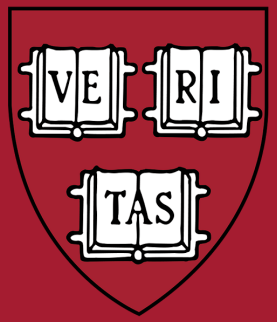
Shared Topics of Interest: Database to Cloud

- Move existing Identity schemas to an instance in the cloud; data will be moved via Oracle Data Pump, which will ensure that no data or database configurations will be lost or accidentally morphed
- Evaluate technologies to allow for replication of data between a database in the Harvard data center and the cloud instance
- Start by pointing all applications that update the database to the instance in the cloud over a VPN, while not yet moving the applications to the cloud
- Next, evaluate and migrate applications that read from the database to point to the cloud instance
- Applications that have issues with performance constraints will point to the Harvard database instance until they can be migrated to the cloud
- Activities are planned for the PI1/PI2 timeframe (Feb/March)
- Customers who connect connecting to our database may have to update their adapter and to where it points, since we are terminating all 10g instances
- In the future, we intend to migrate away from giving customers direct access to our databases

General Discussion

HARVARD

INFORMATION TECHNOLOGY



IDENTITY & ACCESS MANAGEMENT

Thank you!

Appendix A

Technical Oversight Committee Members

Technical Oversight Committee Members

Chair: Magnus Bjorkman, Director of IAM Engineering

Name	School/Group
Indir Avdagic	SEAS
Carolyn Brzezinski	SIS
Steve Duncan	Harvard Kennedy School
David Faux	HUIT Admin Tech/FAS & College
Dan Fitzpatrick	Partners
Eileen Flood	Campus Services
Tim Gleason	HUIT IAM/AD
Sherif Hashem	Harvard Law School
Ken Ho	GSE
Tyson Kamikawa	Harvard Medical School

Name	School/Group
Colin Murtaugh	HUIT Academic
Micah Nelson	HUIT Security
Rich Ohlsten	HUIT Admin Tech/Alumni
Jonah Pollard	Unified Communication/Cloud
Sara Sclaroff	HUIT Admin Tech/HR
Randy Stern	Library IT
Jake Yerdon	HSPH