IAM Committee
Meeting Notes
2/13/2017

Attending: Dash Ballarta, Cam Beasley, CW Belcher, Michael Bos, Bill Bova, John Chambers, Tim Fackler, Alison Lee, Ty Lehman, Darin Mattke, Jason Mayhew, Shelley Powers, Charles Soto, Karen Weisbrodt, Tiffany Yanagawa

Absent: Graham Chapman, Cesar de la Garza, Fred Gilmore, Andy Loomis, Steve Rung

IAM: Kenneth Dunbar (KPMG), Joel Guajardo, Rosa Harris, Justin Hill, Mario Leal, Kara Nicholas, Aaron Reiser, Drew Russell

1. **New Committee Member – Introduce Dash Ballarta (Michael Bos)**

2. **Removing Home Address and Phone from Public Directory – Discuss (CW Belcher)**

Legal Affairs and the Information Security Office have requested that the home address and home phone number should be removed from the online directory. The team is currently coordinating communications with Human Resources and the Office of the Registrar. This change is limited to the online directory and does not affect public records requests, release restrictions, etc.

Q: The previous paradigm was opt-out. Is this a switch to opt-in?
A: No, with this change the information will not be displayed at all.

A date for implementation is pending completion of the communications plan.

Comment: There is an expectation that this will be well-received.

3. **IAM Modernization Program – Group & Role Management Design – Overview (Joel Guajardo & Drew Russell)**

Reference presentation.

In Phase 1, only current and future employees, current and future students, and those with EID entitlements will be included in group and role management functionality. The early adopter applications that were previously discussed with the Committee are being included in Phase 1, though UT Box is no longer an early adopter due to resource constraints. Access request approval processes will be handled by SailPoint IIQ during Phase 1. Future phases will include integration with ServiceNow.

The Levels of Engagement describes the extent of systems' engagement with SailPoint IIQ and the benefits that are associated with more extensive engagement.

Q: Is the access request approval process limited to Level 3? Will this information filter down to lower levels?
A: There will be some limited options available in lower levels in Phase 1.

The role model was designed to anticipate future use of roles. Some examples are provided of how things fit together in the hierarchical model. Birthright roles are based on who you are (e.g. student, faculty, staff). Business roles are dependent on your position, title, or other attributes. IT roles will be dependent on particular applications, such as a need to access a particular system.

The Joiner Example in the presentation provide an example of a newly hired staff member. This employee receives some privileges based on their role as a current staff member, some privileges based on their being in a particular department, and some privileges based on their particular role in that department.

Phase 1 workflows will focus on Identity Lifecycle Management (e.g. new employees, change in department, etc.) and Access Request Approvals (e.g. TSC Tools access). All workflows will trigger email notifications to appropriate recipients (approvers, supervisors, application owners, etc.).

Lastly, Phase 1 will include reporting functionality for groups and roles.

The Group and Role Management Adoption Plan is scheduled for completion in April, and the completion of the build is scheduled for May.

Q: How will access be requested for TSC Tools, since it doesn't appear that the ServiceNow integration will be available yet?
A: In Phase 1, requests will go through a user interface in SailPoint IIQ. There are some wireframe mockups available. Approvals are also done through the same interface.

4. **Other Initiative Updates**
    a. **Recent IAM Incidents (Mario Leal)**

There were three IAM incidents in the last month. The first was an outage for the Duo Admin Portal. There was no effect on end users attempting to authenticate – the outage was scoped to Service Desk personnel attempting to access the administrative tool. The root cause was an issue with the Duo infrastructure. The second incident was on January 8 and was related to a UTLogin configuration. Steps have been taken to prevent this issue from recurring. The third incident was caused by an unexpected change to the Duo API. Steps have been take to increase our resiliency to API changes.

    b. **IAM Team Staffing (Mario Leal)**

The Senior Developer/Analyst position and the Business Analyst/Quality Assurance positions have been filled and the new hires will begin on February 27. Two additional positions on the IAM team, an Information Analyst and a Software Engineer, are being vacated on February 17. Onsite interviews for the open IT Manager position are expected to be completed this week. The team is still waiting on a final determination on the effects of the Governor's hiring freeze as it relates to our team.

    c. **IAM Integrations (Justin Hill)**
        i. Start (Jan. 1): 22
        ii. +5 New: (Academic Works, Jenkins, RecSports, ThousandEyes, Sona)

iii. 0 Completed: ()
iv. 0 Cancelled: ()
v. End (Jan. 31): 27

No integrations were completed in January due to customers being busy as a result of the start of the new semester. This number is expected to pick up in February. One of the departing engineers previously mentioned was an integration engineer, but there are four remaining engineers so the expected impact is minimal.

d. Directory Services Roadmap (Mario Leal)

Due to resource constraints and the need to make the Directory Services Roadmap more holistic in scope, the development of this roadmap will be deferred to FY ’17-’18, with planning for the roadmap resuming this summer.

e. Legacy Authorization Roadmap (Mario Leal)

The Legacy Authorization Systems Roadmap is three weeks behind schedule due to resource constraints. It is expected to be completed by February 24.

f. IAM Modernization Program / SailPoint Implementation (Kara Nicholas)

Reference handout.

The team recently completed four Phase 1 deliverables. In Technical Architecture, the team completed training and operations maintenance deliverables. The last deliverable in the Technical Architecture task is in final review and should be completed soon. The team also completed the Identity Hub design blueprint and a quarterly status report. Efforts are underway to build out the new Identity Hub. Currently, the team is focused on completing the design blueprint for Group and Role Management, as presented earlier. Earlier plans to re-baseline are still ongoing, and current estimates indicate a completion of Phase 1 in mid-September 2017.

Group and Role Management Design Overview

IAM Committee

February 13th, 2017

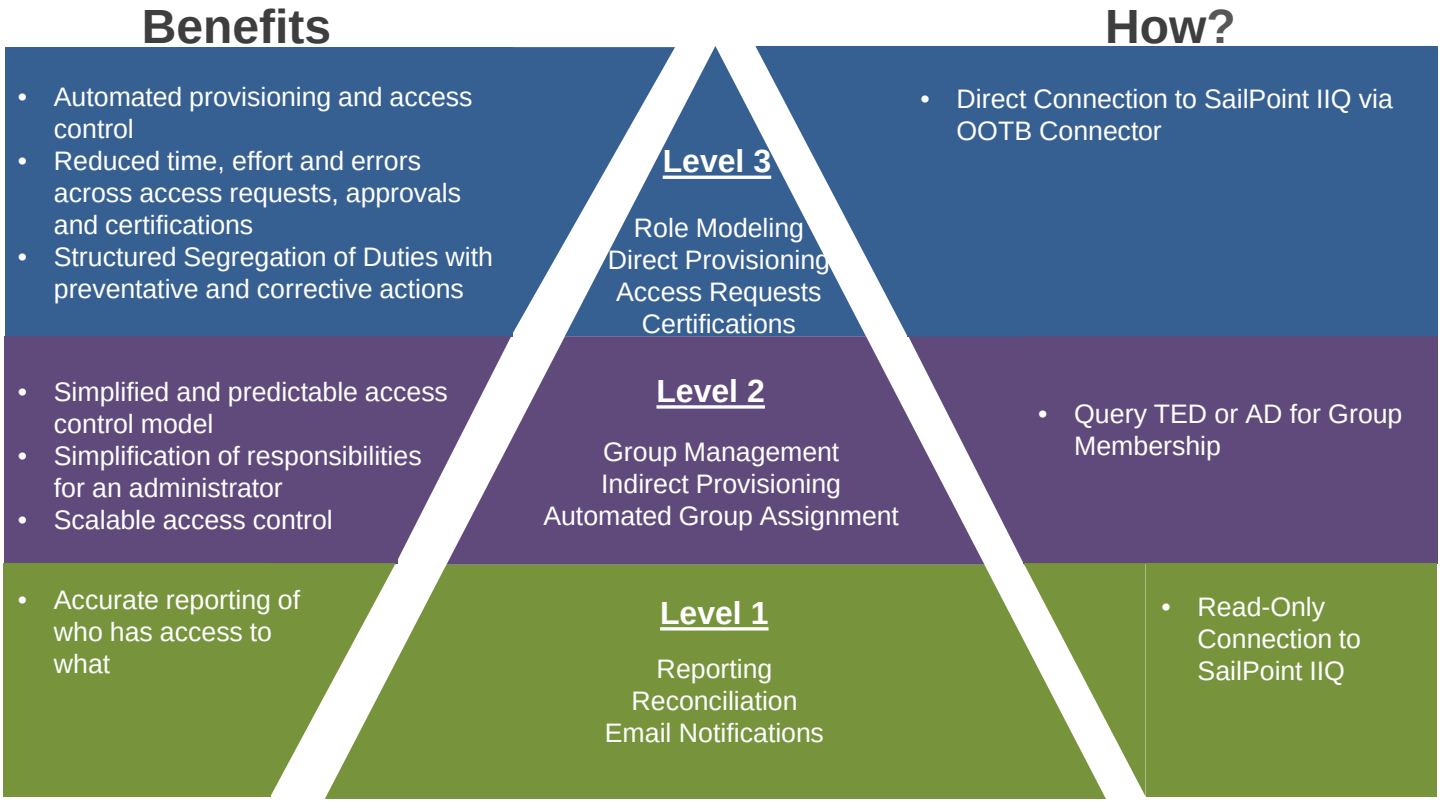
Agenda

- High Level Design Decisions
- System Interface Design
- Role Model
- Access Request
- Workflows
- Reports
- Next Steps

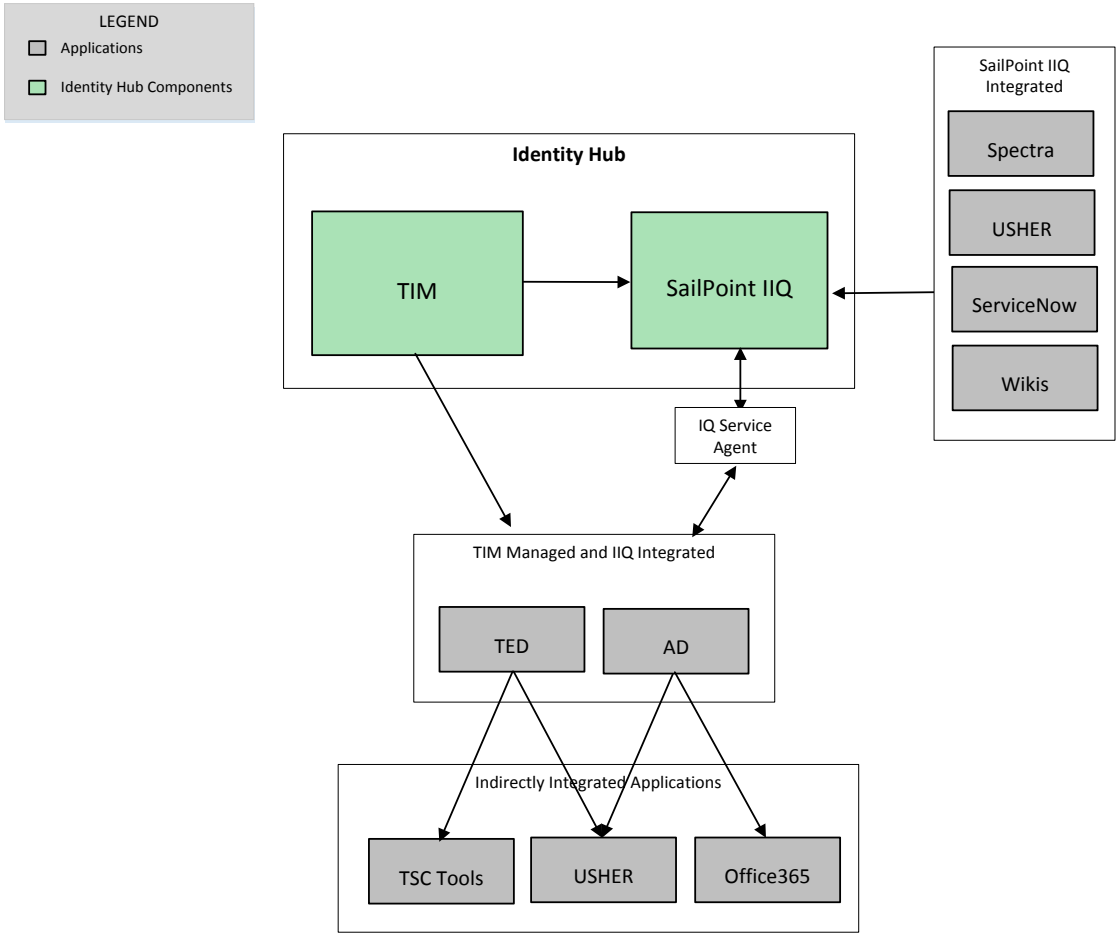
High Level Design Decisions

- Phase 1
  - Group and Role Management functionality will be available to UT Austin identities with a current or future student or employee affiliation or entitlement in TIM
  - Group and Role Management functionality will be available to the following early adopter applications in Phase 1:
    - Office 365 - Eligibility Role Modeling & Reporting
    - Spectra - Reporting
    - TSC Tools - Access Request Management, Group Management, & Reporting
    - USHER - Group Management, Deprovisioning Notifications, & Reporting
    - Wikis - Deprovisioning Notifications & Reporting
    - ServiceNow - Entitlement Modeling
  - Access request approval processes will be handled by SailPoint IIQ
- Future Phases
  - Workday security roles availability within SailPoint IIQ
  - SailPoint IIQ and ServiceNow integration for access requests

Levels of Engagement



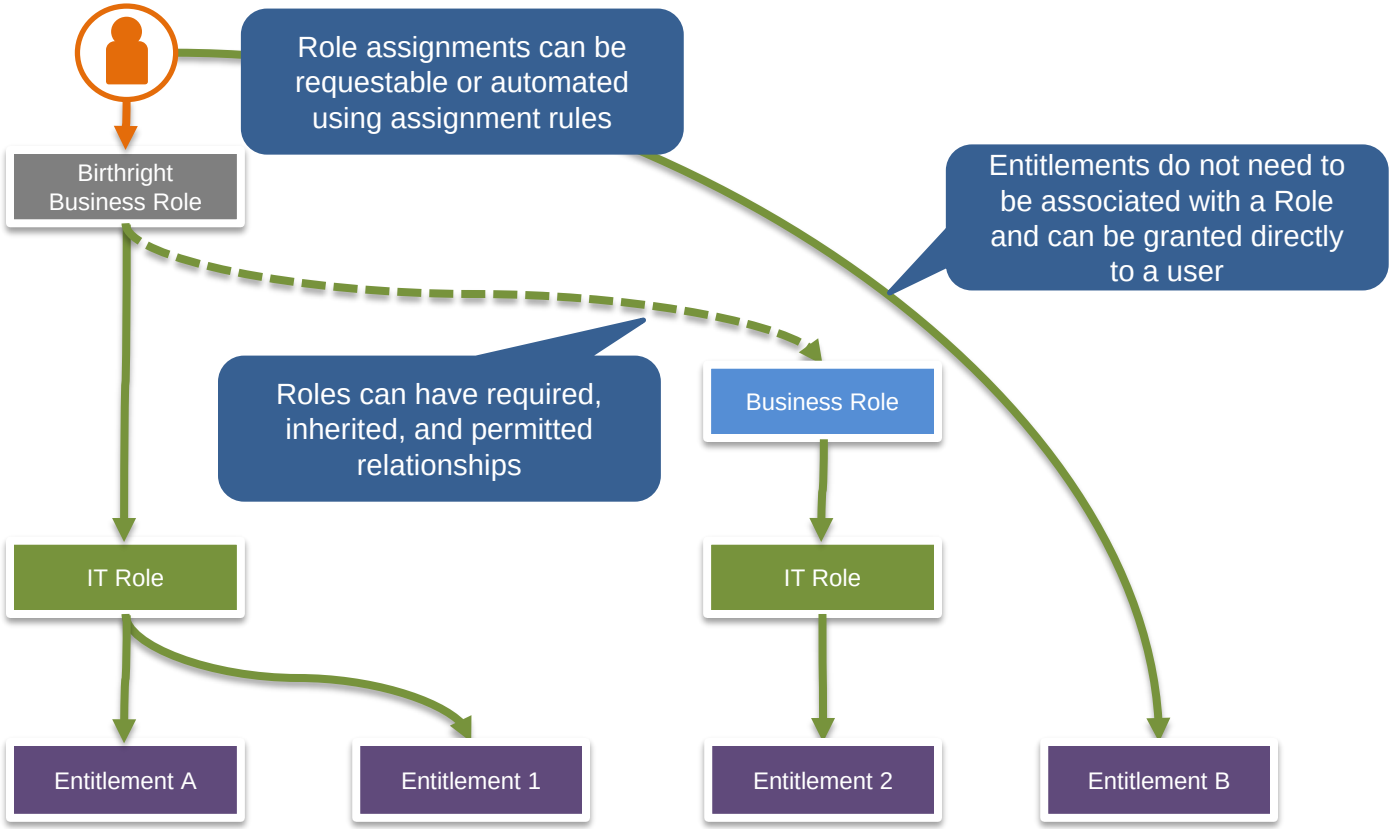
System Interface Design



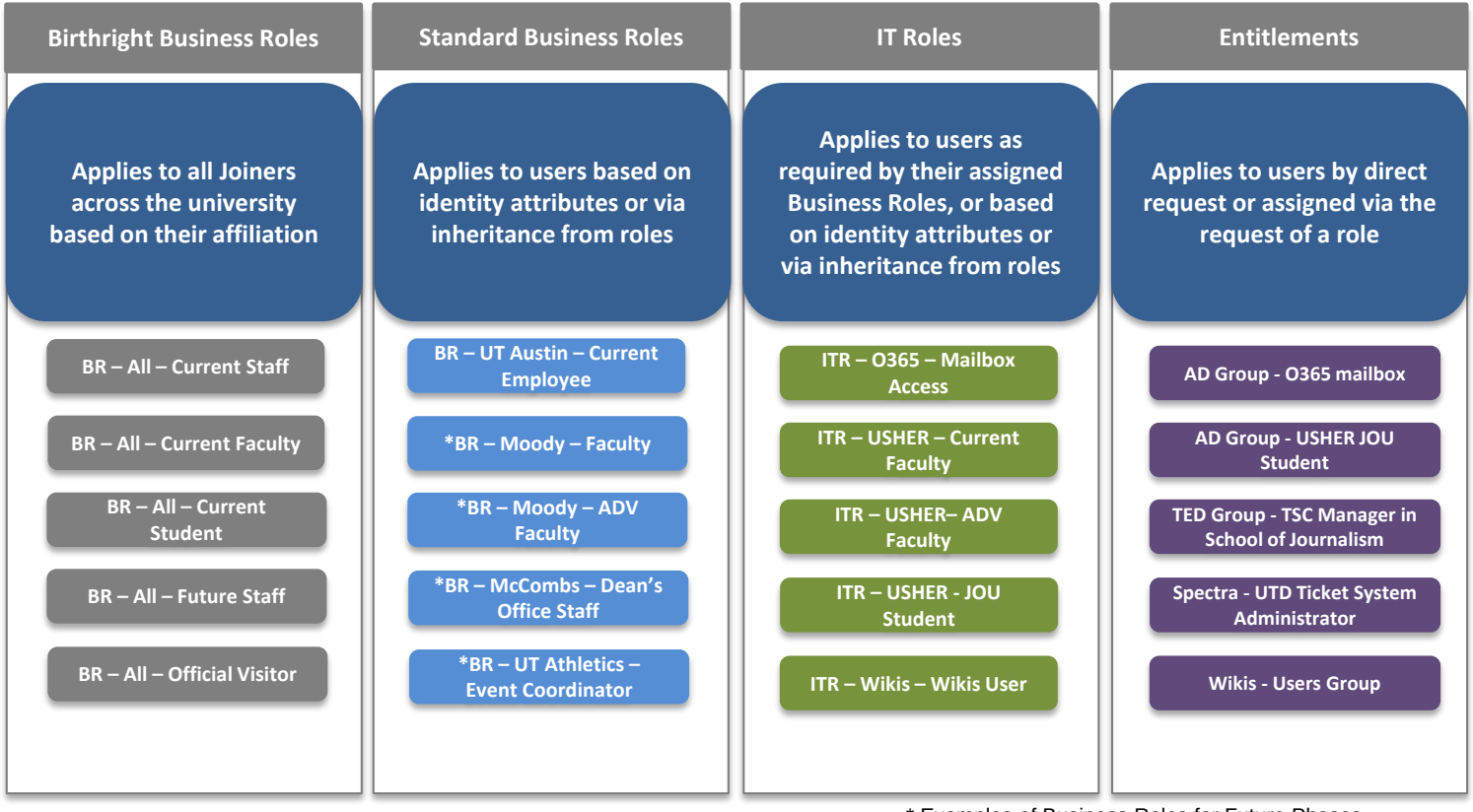
Role Model Principles

- Follow the principle of least privilege
- Follow standardized naming convention
- Design a role model that fits the University's organizational structure and the access model of target onboarded applications
- Design a role model that is modifiable, expandable and scalable
- Group common access (entitlements) by roles without violating all of the above principles
- Utilize role abstraction, inheritance, permitted, and required functions when beneficial
- Avoid role explosion and roles with overlapping access

Role Model

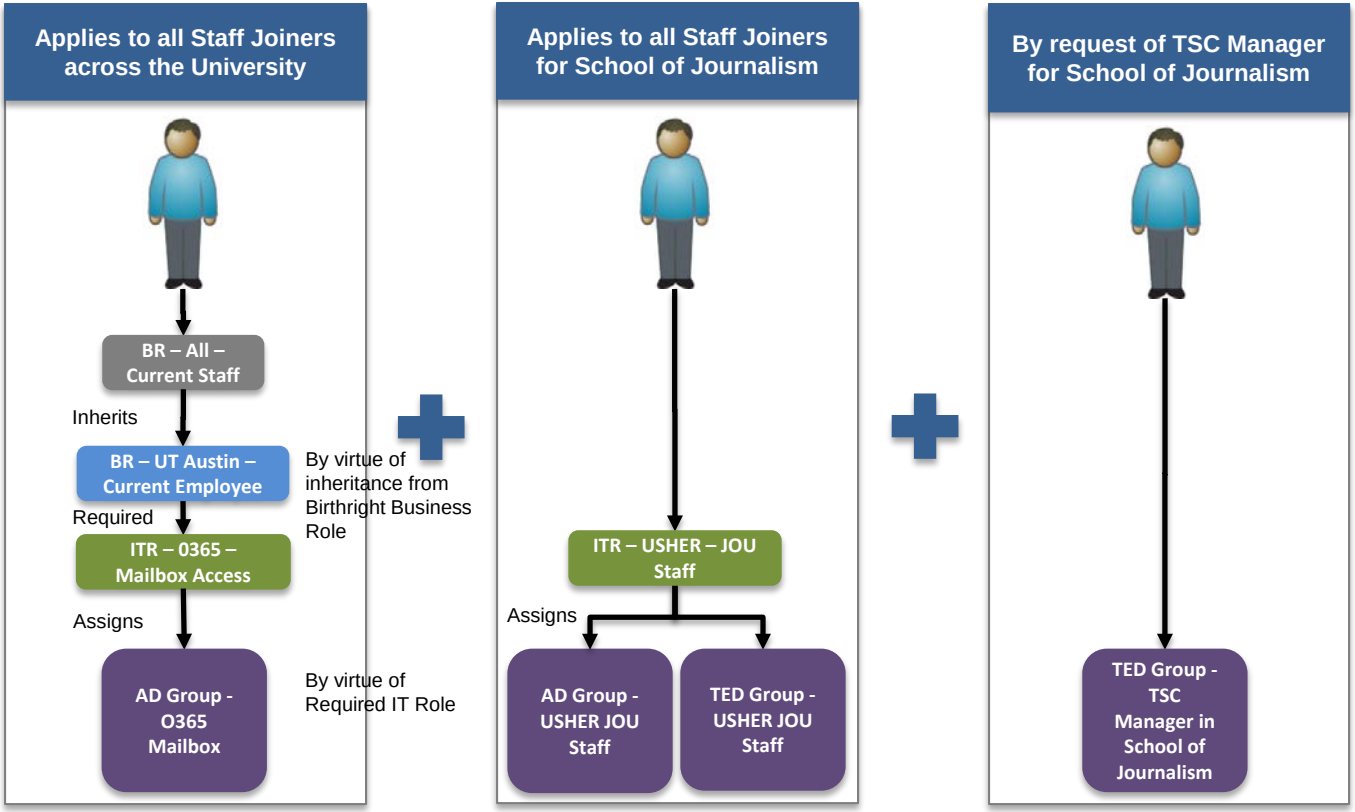

Role assignments can be requestable or automated using assignment rules
Birthright Business Role
Entitlements do not need to be associated with a Role and can be granted directly to a user
Roles can have required, inherited, and permitted relationships
Business Role
IT Role
IT Role
Entitlement A
Entitlement 1
Entitlement 2
Entitlement B

Role Definition



* Examples of Business Roles for Future Phases

Joiner Example



Access Requests

- Phase 1
  - Access requests and approvals for TSC Tools will be handled in SailPoint IIQ
  - Bulk access requests will be available in SailPoint IIQ to help with the transition to groups and roles
- Future Phases
  - Shopping cart access request functionality available within SailPoint IIQ for requestable roles/entitlements
  - SailPoint IIQ creation of ServiceNow requests for manual provisioning of onboarded disconnected applications
  - ServiceNow will be the front-end for all access requests and will be integrated with SailPoint IIQ using “Launch-In-Context”

Workflows

- Identity Lifecycle Management - Attribute Change
  - Joiner
    - New Employee or Student Record
    - Rehire Employee or reinstated Student
  - Mover
    - Modified Employee or Student Record
    - No Current Employee or Student Affiliation
- Access Request Approvals - On Demand
  - TSC Tools – Managerial Access
  - TSC Tools – Non-Managerial Access
- All workflows will trigger email notifications to be sent to the designated recipients

Reports – Phase 1

- Identity Entitlement Detail
  - Provide complete visibility of all in scoped identities and their access within the onboarded applications
- Role Membership
  - Provide a list of users granted a certain role to ensure accuracy based on latest data from an authoritative source
- User Account Attribute
  - Provide a view into a specific application, its accounts and access for the determination of access accuracy and if deprovisioning is required
- Uncorrelated Accounts
  - Identify orphan or stale accounts within an application
- Spaces without Qualified Admins - Wikis
  - Identify spaces not meeting admin requirements which require follow up

Next Steps

- **April** - Group and Role Management Adoption Plan
- **May** – Group and Role Management Build

Identity and Access Management Modernization Program (IAMMP)

Phase 1 Status

Monday, February 13, 2017

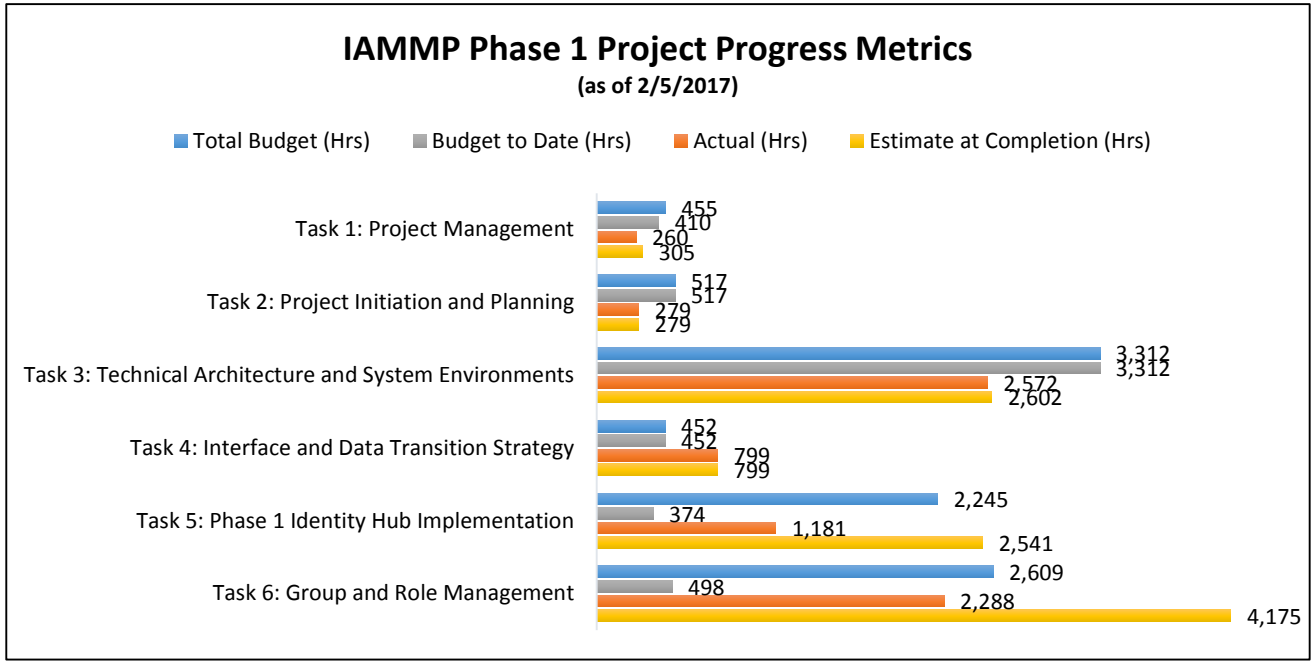
Items for Management Attention

- Several issues with KPMG performance have been closed. Weekly project management issue reviews are ongoing.
- The rebaselining of the Phase 1 schedule has been delayed due to other project priorities. Draft deliverable due dates are provided below but have not been finalized.

Executive Summary

The following four tasks are in progress:

- Task 1: Project Management – The October-December quarterly status report has been approved.
- Task 3: Technical Architecture and System Environments – The Technical Architecture Training and Operations and Maintenance Plan deliverables have been approved. The Testing deliverable is in review by the UT project manager.
- Task 5: Phase 1 Identity Hub Implementation – The Phase 1 Identity Hub Design Blueprint has been approved. The Build and Training deliverables are in progress. The second round of Workday integrations testing is on track for completion this week.
- Task 6: Group and Role (G&R) Management – The G&R Design Blueprint is in team review. The Adoption Plan documentation and governance model are in development.



Deliverable Status					
Project Task Area	**Deliverable**	**Deliverable Name**	**Status**	**Planned Finish**	**Actual Finish**
Task 1: Project Management	D1.1	Project Work Plan	Complete	3/21/2016	3/14/2016
	D1.2.1	Q1 Quarterly Status Report	Complete	4/25/2016	4/29/2016
	D1.2.2	Q2 Quarterly Status Report	Complete	7/25/2016	7/29/2016
	D1.2.3	Q3 Quarterly Status Report	Complete	10/24/2016	12/2/2016
	D1.2.4	Q4 Quarterly Status Report	Complete	1/30/2017	1/20/2017
	D1.3	Risk and Issue Register	Complete	3/21/2016	3/17/2016
	D1.4	Change Control Process	Complete	4/4/2016	4/11/2016
	D1.5	Communication Plan	Complete	7/18/2016	12/2/2016
Task 2: Project Initiation and Planning	D2.1	Application Development and Configuration Standards	Complete	4/18/2016	4/8/2016
	D2.2	Project Kick-off Meeting	Complete	2/29/2016	2/29/2016
	D2.3	Comprehensive Test Plan	Complete	6/6/2016	10/7/2016
	D2.4	Deployment Plan	Complete	4/25/2016	7/22/2016
	D2.5	Training Plan	Complete	5/23/2016	8/26/2016
Task 3:Technical Architecture and System Environments	D3.1	Technical Architecture Approach	Complete	5/2/2016	5/20/2016
	D3.2	Prototype Environment(s)	Complete	5/2/2016	4/18/2016
	D3.3	Technical Architecture Requirements	Complete	5/16/2016	6/10/2016
	D3.4	Technical Architecture Design Blueprint	Complete	6/20/2016	8/26/2016
	D3.5	Technical Architecture Build	Complete	8/8/2016	12/2/2016
	D3.6	Technical Architecture Testing	Behind	8/22/2016	EC: 2/17/2017
	D3.7	Technical Architecture Training	Complete	8/29/2016	2/6/2017
	D3.8	Technical Architecture Deployment Playbook	Complete	8/22/2016	12/2/2016
	D3.9	Technical Architecture Deployment	Complete	9/12/2016	12/13/2016
	D3.10	Technical Architecture Operations and Maintenance Plan	Complete	9/26/2016	1/20/2017
Task 4: Interface and Data Transition Strategy	D4.1	Interface and Data Transition Strategy Requirements	Complete	5/9/2016	6/3/2016
	D4.2	Interface and Data Transition Strategy	Complete	5/23/2016	9/16/2016
Task 5: Phase 1 Identity Hub Implementation	D5.1	Phase 1 Identity Hub Design Blueprint	Complete	8/1/2016	1/20/2017
	D5.2	Phase 1 Identity Hub Build	In Progress	~~9/6/16~~ 4/14/17	
	D5.3	Phase 1 Identity Hub Test	In Progress	~~10/24/16~~ 9/15/17	
	D5.4	Phase 1 Identity Hub Training	In Progress	~~10/31/16~~ 4/28/17	
	D5.5	Phase 1 Identity Hub Deployment Playbook		~~10/10/16~~ 5/12/17	
	D5.6	Phase 1 Identity Hub Deployment		~~10/31/16~~ 5/19/17	
	D5.7	Phase 1 Identity Hub Operations and Maintenance Plan		~~11/14/16~~ 6/2/17	
Task 6: Group and Role Management	D6.1	Group and Role Management Use Cases	Complete	8/22/2016	12/5/2016
	D6.2	Group and Role Management Requirements	Complete	9/6/2016	1/6/2017
	D6.3	Group and Role Management Design Blueprint	Behind	~~9/26/16~~ 3/10/17	EC: 3/24/17
	D6.4	Group and Role Management Adoption Plan	In Progress	~~11/7/16~~ 6/2/17	
	D6.5	Group and Role Management Build		~~10/24/16~~ 7/7/17	
	D6.6	Group and Role Management Testing		~~11/21/16~~ 9/15/17	
	D6.7	Group and Role Management Training		~~12/12/16~~ 9/1/17	
	D6.8	Group and Role Management Deployment Playbook		~~10/24/16~~ 7/21/17	
	D6.9	Group and Role Management Deployment		~~12/12/16~~ 9/15/17	
	D6.10	Group and Role Management Operations and Maintenance Plan		~~12/19/16~~ 9/22/17	
Task 7: Optional Post Implementation Support	D7.1	Optional Post Implementation Support			