IAM Committee
Meeting Notes
10/17/2016

Attending: Cam Beasley, CW Belcher, Tim Fackler, Fred Gilmore, Alison Lee, Ty Lehman, Andy Loomis, Jason Mayhew, Shelley Powers, Charles Soto, Karen Weisbrodt, Tiffany Yanagawa

Absent: Michael Bos, Bill Bova, John Chambers, Graham Chapman, Seth Feder, Cesar de la Garza, Darin Mattke, Steve Rung

IAM: Kenneth Dunbar (Contractor – KPMG), Joel Guajardo, Marta Lang, Mario Leal, Aaron Reiser, Andrew Russell

1. **UTLogin Issues – Update (Mario Leal)**

UTLogin is currently stable and has not had any issues in several weeks. Some issues were due to configuration changes that have seen been rolled back. Future action items include patching systems and making a ForgeRock-recommended change to load balancing. Testing is underway and a schedule for moving forward should be available by the end of the week.

2. **IAMMP/SailPoint Group & Role Management – Update (Joel Guajardo)**

Reference: Presentation

At the previous meeting, a list of group and role management use cases was shared and the next steps were set as prioritizing applications and roles.

Applications and roles were prioritized based on risk criteria and technical complexity for implementation. Pain points were also considered, as well as birthright roles. A list of recommended early adopter applications has been developed for Phase 1.

Q: What consideration has been taken to account for the differences between faculty, staff, and student employee insofar as the employee role?
A: Currently the focus is on faculty and staff, since those roles have the larger impact. When the source system shifts to Workday, however, SailPoint will rely upon the information from Workday.

Q: Will distinctions be made between permanent staff and temporary/contract staff?
A: Those employee types have different classifications and details will be determined at a later date.

Q: Where does the UT wireless network fit into the roadmap?
A: Due to technical challenges, the wireless network will be considered at a later phase. This will most likely happen when the TIM notifiers are due to be replaced.

Next steps are to confirm readiness with early adopters, finalize the requirements, and proceed with the integrations.

There are slides in the presentation appendix with additional information, as well as another example of a sample employee with various roles, and an architectural diagram.

3. IAM FY16-17 Planning – Review (CW Belcher)

Reference: Presentation

The approach the team takes every year is to estimate the number of FTEs available, determine the vacancy rate, determine the workload for basic sustainment, determine project priorities, and account for the IAM Roadmap and other important items.

Currently, the team is authorized for 27 FTEs. A 15% vacancy rate is assumed based on historical averages.

Required sustainment accounts for 8.99 FTEs and consists of making sure that systems are up and running and functioning properly.

Integration support involves a significant amount of work with customers to determine provisioning and deprovisioning processes, as well as the technical effort for implementation.

Work on the Shibboleth/Duo multifactor authentication integration is almost complete. With Shibboleth upgraded to v3, all that is left is the multifactor implementation in Shibboleth.

OpenAM is the software that underlies UTLogin and needs to be upgraded to the most recent version, which implements new functionality as well as stability and performance improvements.

IAMMP Phase 1 continues into the next fiscal year.

TRAC (Technical Resource Account Control) is a system used to provision certain IT services. The original plan was to migrate the functionality to ServiceNow in the initial ServiceNow rollout, but it had to be taken out of scope for ServiceNow Phase 1. It is currently near the top of the ServiceNow priority list with a projected ETA of Spring 2017.

The uTexas Enterprise Directory (TED) is 11 years old, so the team is assessing what campus's needs are for directory services. In addition, the team is talking with peer institutions and with Gartner to help determine a way forward for directory services, which will be captured in the Directory Services Roadmap. The actual implementation will be a separate project.

Apollo/OHSC (Organizational Hierarchy System Contacts)/DPUSER need changes to prepare for Workday going live. They also need a roadmap for retirement since they will be retired as legacy infrastructure.

OAuth is a type of federated authentication and there have been a number of requests from campus for OAuth support. The goal is to allow additional methods for allowing campus stakeholders to leverage central authentication in a secure manner.

Q: When counting FTEs, are you also including management? Also, are you considering a full 40 hours per week or a reduced amount?

A: The calculations take into account direct hours, so they do not include leave, administrative overhead, professional development, etc. The estimates are based on historical actuals from previous fiscal years. For non-manager employees, the metric is approximately 25 available hours per week. The calculations include management time.

There were a number of projects which had to be deferred due to a lack of resources.

IAMMP Phase 2 was deferred. IAMMP Phase 1 is in the middle of re-baselining, but some Phase 1 hours will be used to make some advances.

There aren't enough resources or funding for Lightweight Authentication. A resolution will be needed since retiring guest EIDs is critical.

The Central Authentication Resiliency Enhancement (CARE) is meant to provide authentication resiliency via cloud-based systems. The requirements and solution analysis have already been completed. As the team proceeds with the OpenAM upgrade, work will be done to ensure that UTLogin is cloud-ready.

The Shibboleth SSO (single sign-on) is a user experience enhancement to help reduce the number of times users need to log in.

The IAM Team runs over 100 servers that need patches and updates, so the team will need to leverage automation to free up resources for other efforts.

Q: For the 100+ servers, are those machines for testing or to distribute load?
A: It varies depending on the service. There are QUAL and TEST environments for testing, as well as multiple machines in various environments in order to handle load.

The ID Card System is mainframe-based and needs to be replaced. Next year, the team will work with ITS Customer Support Services (CSS) to replace the system.

Q: Are you making any pitches to potential funding groups?
A: The biggest deferment is CARE, and the team is looking into a smaller scope that will allow the team to move forward with iterative solutions. The team is also investigating getting assistance with the UTLogin upgrade from ForgeRock, freeing up other resources to work on CARE.

4. **Other Initiative Updates**
    a. **IAM Team Staffing (Mario Leal)**

The team is currently scheduling phone screens for the IT Manager position. On-site interviews have been held for the Business Analyst position. Phone screens for the Quality Assurance Tester have been set up for this week. On-site interviews for the Software Developer/Analyst have been completed and reference checks will be conducted this week.

    b. **IAM Integrations (Mario Leal)**

Start (Sep 1): 24
+4 New: (WordPress, Cisco Spark, OpenShift, Hadoop)
-2 Completed: (GitHub, Symplicity Advocate)
-0 Cancelled: ()
End (Sep 30): 26

The team is investigating ways to make the integrations process more efficient, including integrating more of the steps into ServiceNow.

c. Directory Services Roadmap (Mario Leal)

Work on the directory services assessment is almost complete. Peer institution reviews are complete. The team is preparing for a call with Gartner, which will be conducted by a cross-functional team including the Active Directory team.

d. Legacy Authorization Roadmap (Mario Leal)

The team has engaged with the ASMP application modernization team to help identify use cases for authorization services as campus areas replace their legacy systems. These use cases will be incorporated into a roadmap for the legacy authorization systems like Apollo and OHSC.

e. Two-Factor Authentication / Duo Implementation – Update (Mario Leal)

The Shibboleth v3 upgrade was completed on October 13, paving the way for the Duo integration with Shibboleth (ETA December 1). There are no longer any applications using Toopher and Toopher will be retired in the next month.

f. IAM Modernization Project / SailPoint Implementation (Marta Lang)

Reference: Handout

Work on Phase 1 is ongoing and the team is working with KPMG to address issues encountered during the project. The team is also reassessing how to approach future project phases, possibly switching from waterfall to a more iterative project methodology.

Q: At the end of Phase 1, could the team provide the committee with a list of applications that will be integrated into SailPoint, a synopsis, and an explanation as to why the use case is where it is?
A: Yes, one of the project deliverables is the adoption plan, which will cover much of the requested information.

g. Lightweight Authentication (Marta Lang)

The team is putting the project on hold until resources become available.

IAMMP Group and Role Management Update

October 17, 2016

Agenda

- Application and Role Prioritization Criteria
- Early Adopter Applications and Roles
- Next Steps

Prioritization Process

Application interviews were held and applications and roles were prioritized based on Technical Readiness and Risk criteria as well as overall impact.

Technical Readiness Criteria

Criteria	Description
Integration Effort	Effort required to integrate the application with IIQ
Role Mapping	Coverage of roles for the organization (birthright, business, etc.)
Connector Capability	Ability to leverage out-of-box connector functionality
Development Environment	Availability of development environment of target application

Risk Criteria

Criteria	Description
Data Classification	Sensitivity of the data
Regulatory Requirements	Audit and compliance requirements for the application
User Population	Number of end-users impacted

Application and Role Prioritization

Other Factors Considered:

- Pain points
- Sampling of application, role, and population types

Early Adopter Roles

Proposed Roles

Role	Description	Birthright?	Driving Applications
UT Austin Employee	A birthright business role assigned to all active employees of The University of Texas at Austin including faculty, staff, and student workers.	Y	UTBox, Wikis*, VPN Service*
College of Communication Employees	A birthright business role assigned to all active employees in the College of Communication.	Y	Usher Web Apps, LANDesk Service Desk*, Room Reservation System*
College of Communication Student	A birthright business role assigned to all active students in the College of Communication.	Y	Usher Web Apps, Equipment Checkout*, STAR*
ITS Staff Member	A birthright business role assigned to all active IT Staff members	Y	MS Office 365, Wiki - ITS Staff Wiki*
MS Office 365 Access	Requestable role to get basic access to MS Office 365; Birthright role for ITS Staff	Y	MS Office 365
TSC Tool Access Roles (multiple roles)	Roles to request access to TSC tools (e.g. IT Networking Custodian)	N	TSC Tools
Red Hat Satellite Access Role	Role to request standard access to Red Hat Satellite application	N	Red Hat Satellite
ServiceNow Access Roles (multiple roles)	Roles defined by mining ServiceNow application data	N	ServiceNow
Paciolan Access Roles (multiple roles)	Roles defined by mining Paciolan application data	N	Paciolan

* Planned for Future Phase

Early Adopter Applications

Proposed Target Applications

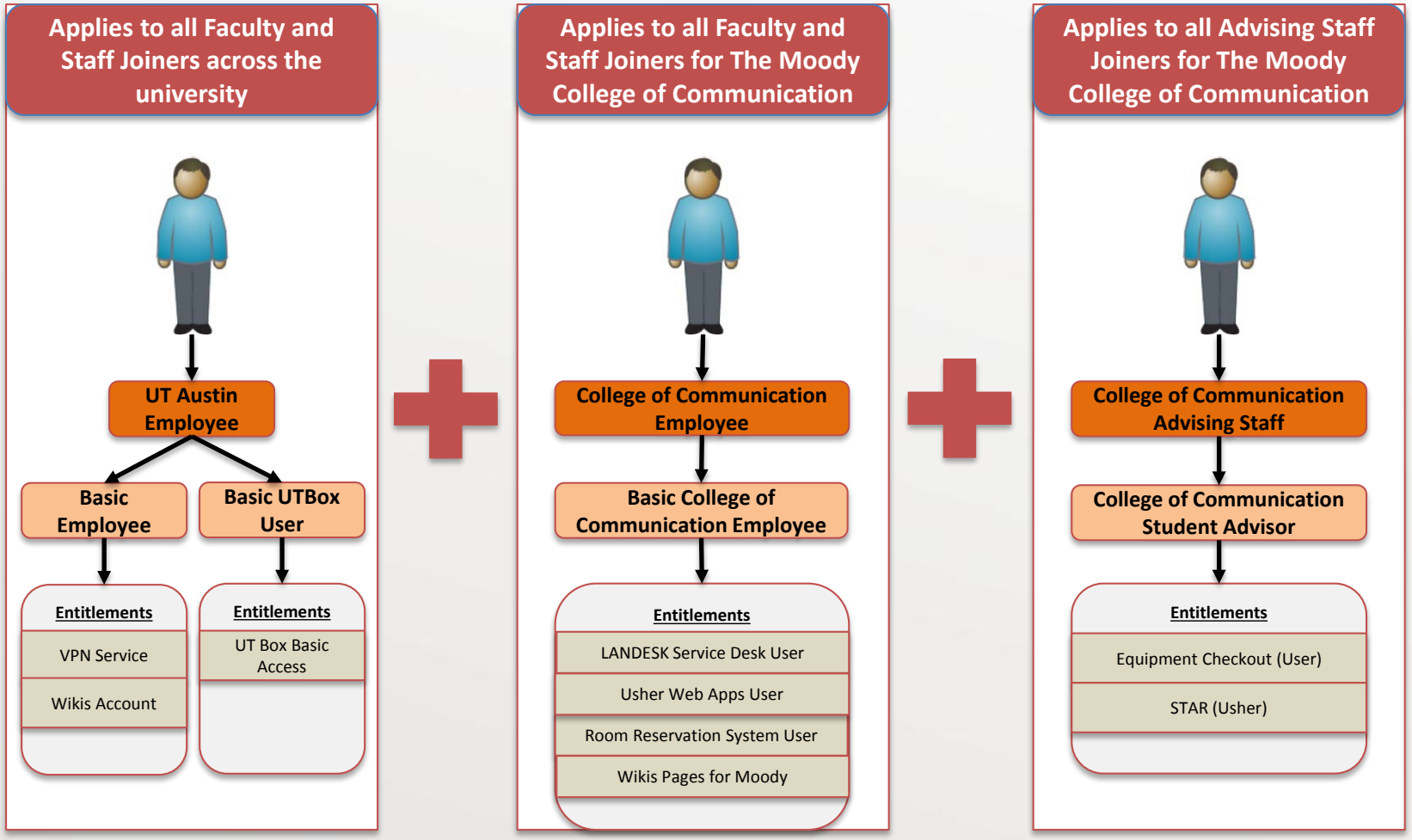
Application	Organization	Application Type	Justification
TED	Identity and Access Management	Connected (Direct Connector)	Foundational Application
Active Directory	ITS Systems	Connected (Direct Connector)	Foundational Application
UTBox	Information Security Office	Connected (Direct Connector)	Birthright for Employees and Students
MS Office365	ITS Systems	Connected (Direct Connector)	Significant impact on manual processes; Birthright for ITS Staff
TSC Tool	ITS Networking	Connected (MySQL DB / TED)	Identified by ITS Networking
Usher Web Apps	College of Communication	Connected (TED & AD)	Birthright for College of Communication
Red Hat Satellite	ITS Systems	Connected (AD)	Partial provisioning and task notification for local account creation
ServiceNow	ITS Customer Support Services	Disconnected (Direct Connector)	Strategic Application
Paciolan	UT Athletics	Disconnected (Flat File)	Audit issues with separations

Early Adopter Applications

On The Radar

Application	Organization	Application Type	Justification
Adobe Connect	ITS Systems	Connected (TBD)	May require some changes to current process or custom logic. Additional investigation needed.
Shared Drive and Desktop Access	College of Communication	Connected (AD)	May require custom logic for automatic group creation. Additional investigation needed.
VPN Service	ITS Networking	Connected (TBD)	Birthright for Employees
Wikis	Web & Contract Services	Disconnected (TBD)	Birthright for ITS Staff and helps address pain point for separations
Workflow	UT Athletics	Disconnected (Flat File)	Audit issues with separations

Student Advising Staff Joiner Proposed Roles

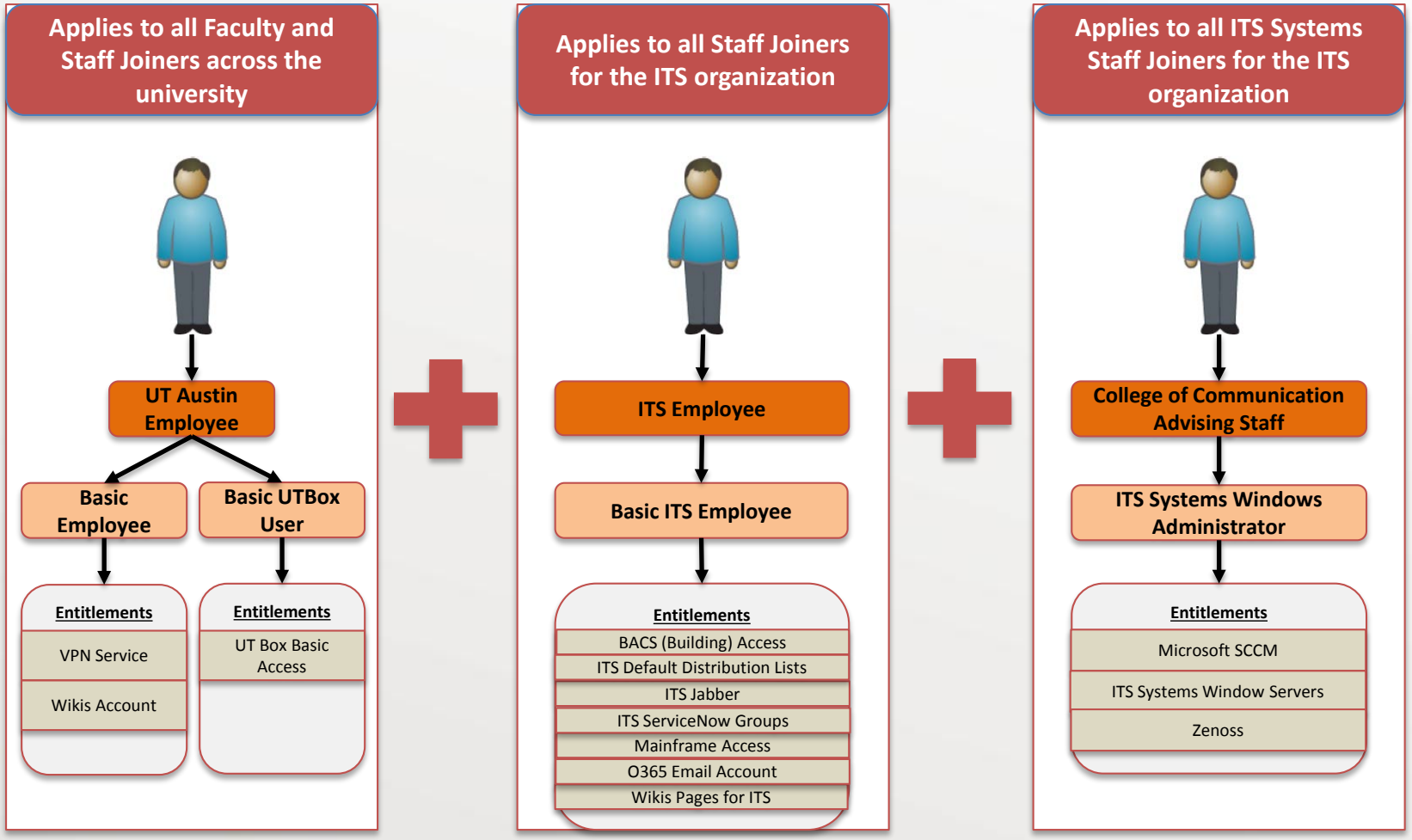


Next Steps

- Receive buy in from early adopter application owners by end of October.
- Finalize requirements by mid November.
- Proceed with application integration process.
  - Follow Up Interview -> Integration Spec -> Prep Work -> UAT -> Deployment

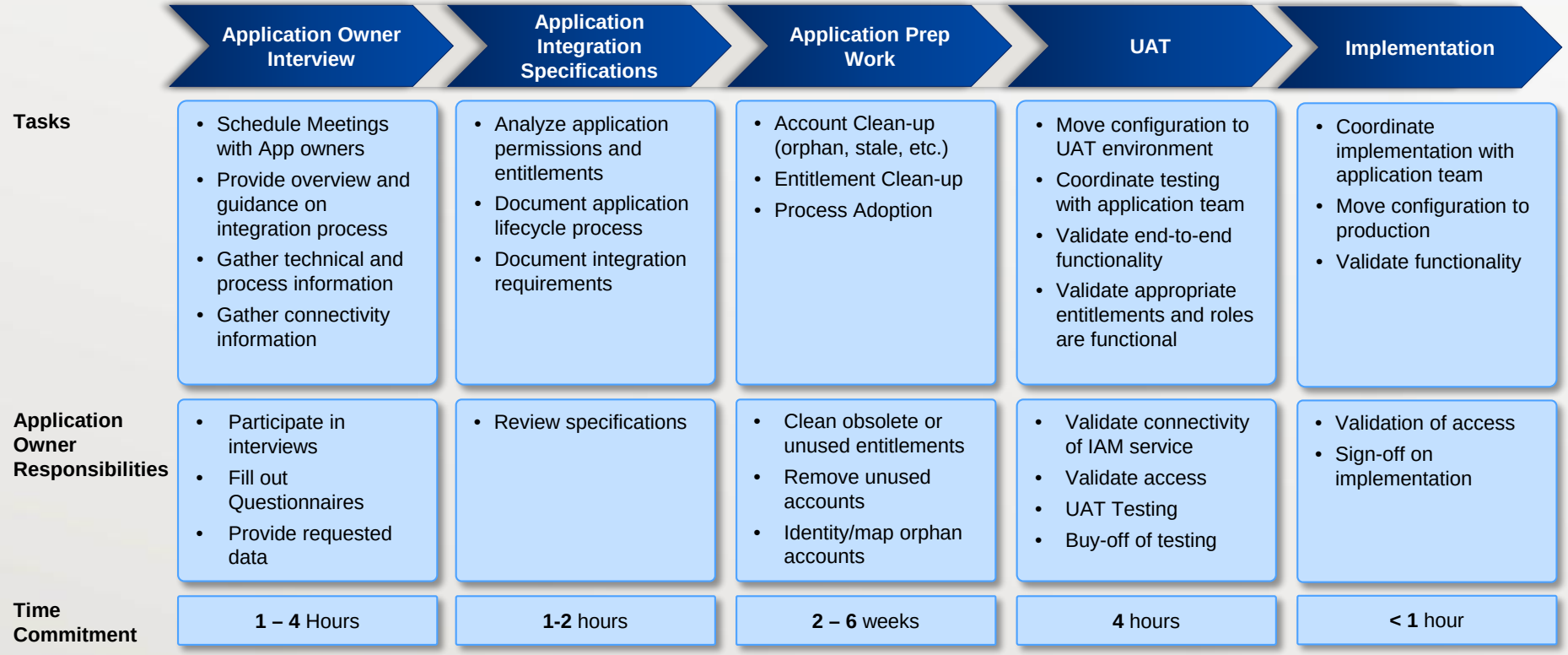
APPENDIX

ITS Systems Windows Administrator Joiner Proposed Roles

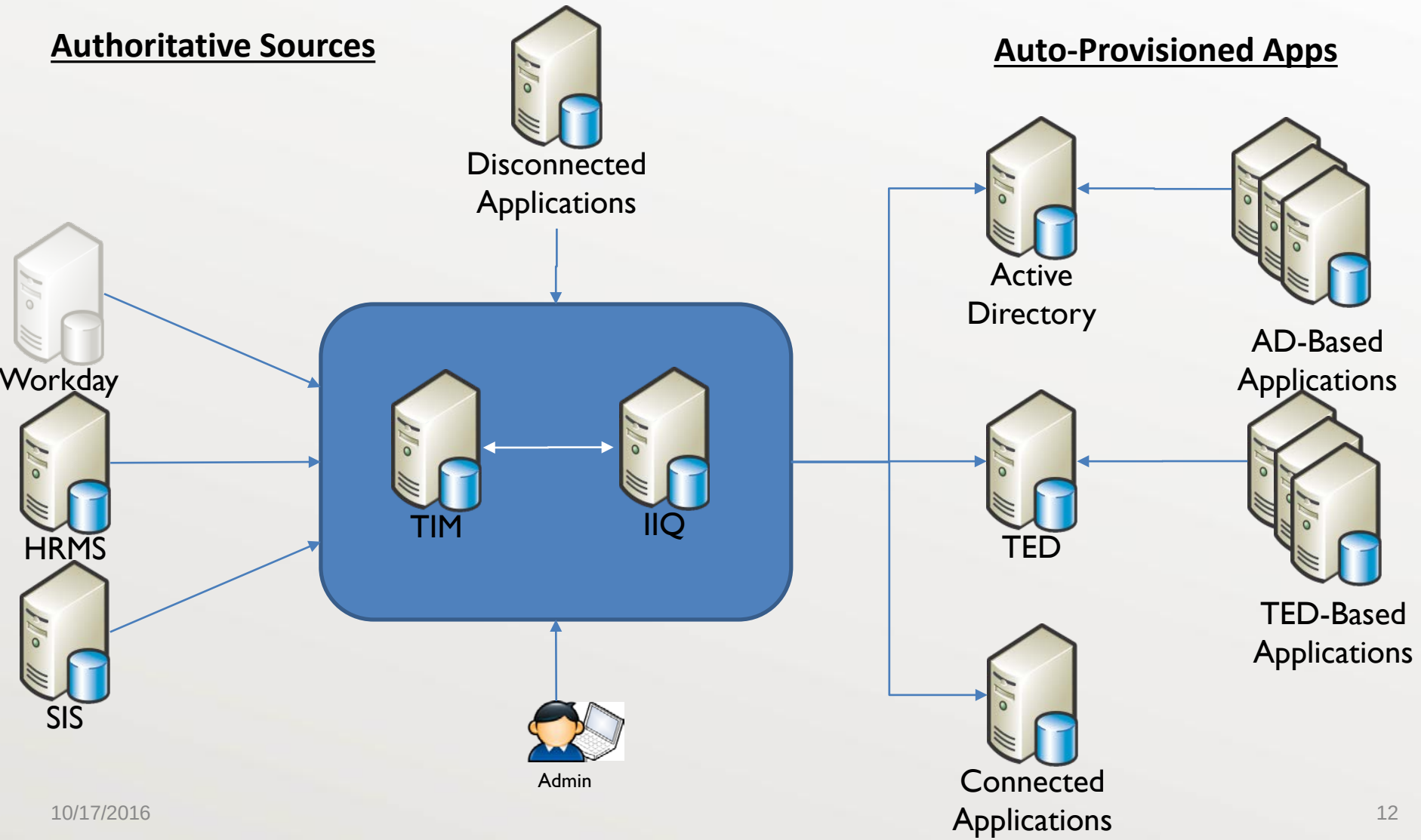


Application Integration Process

- This is an iterative process for each application for integration onto the IAM System.



Conceptual System Architecture – Phase 1



FY16-17 IAM Service Plan

IAM Committee

October 17, 2016

FY16-17 Planned Activities/Projects

Activity/Project	FTEs
Required Sustainment	8.99
IAM Integration Support	1.56
MFA: Shibboleth/Duo Integration	0.23
Shibboleth v3 Upgrade	0.09
OpenAM 13 Upgrade	1.96
IAMMP Phase 1	6.95
TRAC Replacement	0.65
Directory Services Roadmap (no implementation)	0.06
Apollo/OHSC/DPUSER Roadmaps & Required ASMP changes	1.54
OAuth Implementation	0.92
Total (assumes 15% vacancy rate)	**23.0**

FY16-17 Deferred Activities/Projects

Activity/Project	FTEs
IAMMP Phase 2 (SOW and Implementation)	3.91
Lightweight Authentication & BYOId	0.96
CARE (Centralized Authentication Resiliency Enhancement)	2.31
Shibboleth SSO	0.52
IAM Maintenance Automation	0.56
UTLogin User Store Enhancement	0.55
ID Card System Replacement Phase 1	1.06
Directory Services Roadmap Implementation	0.95
UTLogin RPM Update (ssoadm to REST)	0.15
…and many others	1.75
Total	**12.7**

Identity and Access Management Modernization Program (IAMMP)

Phase 1 Status

Monday, October 17, 2016

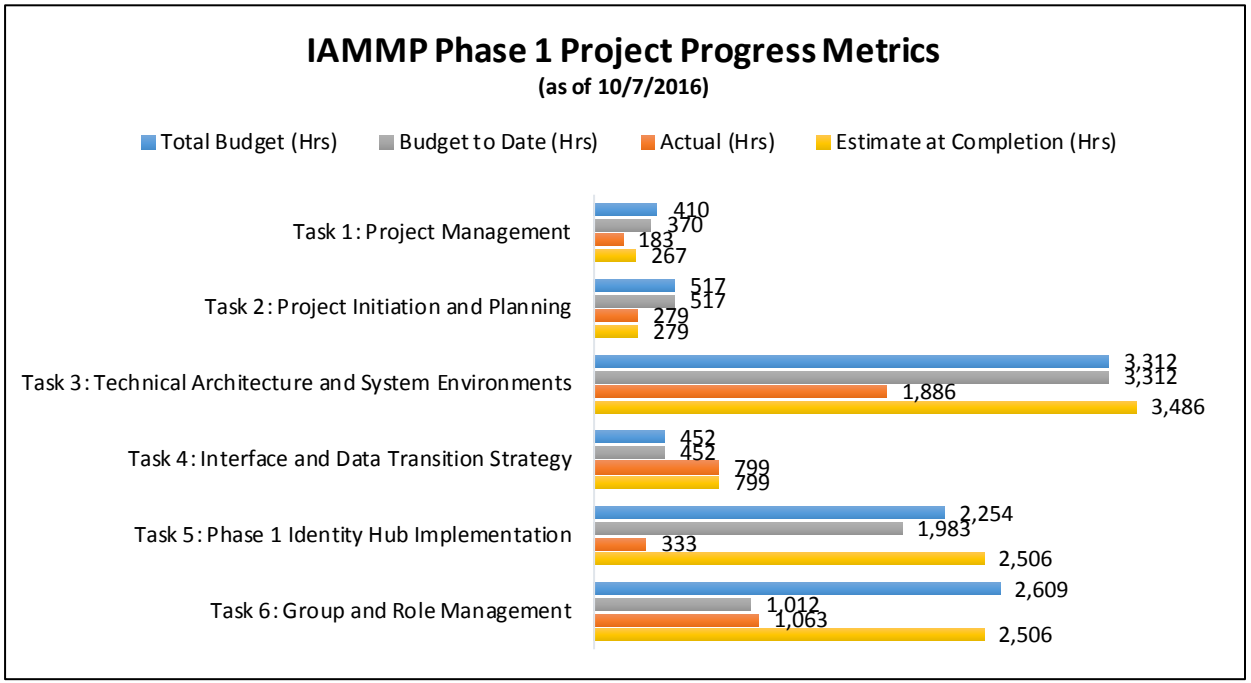
Items for Management Attention

- Corrective measures are continually monitored to address issues with KPMG's performance, with a focus on overcoming resource challenges and improving the delivery of quality and value. Weekly project management issue reviews are continuing until issues are addressed accordingly.
- The project schedule is being revisited with discussions about changes to the project delivery approach to be able to assess more realistic delivery dates.

Executive Summary

The following four tasks are in progress:

- Task 1: Project Management – UT Austin and KPMG management are discussing the rebaseline approach. The Communication Plan is in Executive Sponsor review. The next quarterly status report is being drafted.
- Task 3: Technical Architecture and System Environments – The Technical Architecture Build deliverables are in Executive Sponsor review. The team has begun building automated test scripts and executing testing. The remaining deliverables, including the Playbook, Deployment, and Operations and Maintenance Plan, are underway.
- Task 5: Phase 1 Identity Hub Implementation – The Phase 1 Identity Hub Design Blueprint deliverable is in development. The team is working to define dependencies between Task 5 and Task 6 to address design challenges. The team is working with the Workday team to execute the initial round of integrations verification.
- Task 6: Group and Role (G&R) Management – The G&R Management Use Cases are in Project Management review. The G&R Requirements deliverable is in progress.



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	Behind	10/24/2016	EC: TBD
	D1.2.4	Q4 Quarterly Status Report		1/30/2017	
	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	Behind	7/18/2016	EC: 10/21/2016
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	Behind	8/8/2016	EC: 10/21/2016
	D3.6	Technical Architecture Testing	Behind	8/22/2016	EC: 12/16/2016
	D3.7	Technical Architecture Training	Behind	8/29/2016	EC: 11/18/2016
	D3.8	Technical Architecture Deployment Playbook	Behind	8/22/2016	EC: 11/18/2016
	D3.9	Technical Architecture Deployment	Behind	9/12/2016	EC: 11/18/2016
	D3.10	Technical Architecture Operations and Maintenance Plan	Behind	9/26/2016	EC: TBD
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	Behind	8/1/2016	EC: 12/9/2016
	D5.2	Phase 1 Identity Hub Build		9/6/2016	
	D5.3	Phase 1 Identity Hub Test	Behind	10/24/2016	EC: TBD
	D5.4	Phase 1 Identity Hub Training	Behind	10/31/2016	EC: TBD
	D5.5	Phase 1 Identity Hub Deployment Playbook		10/10/2016	
	D5.6	Phase 1 Identity Hub Deployment		10/31/2016	
	D5.7	Phase 1 Identity Hub Operations and Maintenance Plan		11/14/2016	
Task 6: Group and Role Management	D6.1	Group and Role Management Use Cases	Behind	8/22/2016	EC: 11/18/2016
	D6.2	Group and Role Management Requirements	Behind	9/6/2016	EC: 11/28/2016
	D6.3	Group and Role Management Design Blueprint		9/26/2016	
	D6.4	Group and Role Management Adoption Plan		11/7/2016	
	D6.5	Group and Role Management Build		10/24/2016	
	D6.6	Group and Role Management Testing	On Hold	11/21/2016	EC: TBD
	D6.7	Group and Role Management Training	On Hold	12/12/2016	EC: TBD
	D6.8	Group and Role Management Deployment Playbook		10/24/2016	
	D6.9	Group and Role Management Deployment		12/12/2016	
	D6.10	Group and Role Management Operations and Maintenance Plan		12/19/2016	