Business Services Committee
1:30-3:00 p.m., April 7, 2016, FAC 228D

I. 1:30-1:50 Sailpoint - Update (CW Belcher)

II. 1:50-2:15 Business Continuity and Disaster Recovery Plan (Dana Cook)

III. 2:10-2:45 ASMP – UBC Update (Renee Wallace)

IV. 2:45 -3:00 WorkDay Demo (Renee Wallace and Team)

On tap for 1:30 – 3:00 p.m. on May 6, 2016 in FAC 228D

*Next meeting falls on UT Remembers
**Open call for agenda items
SailPoint IdentityIQ Overview

Business Services Committee
April 1, 2016
The IAM Roadmap: 3 Main Goals

• Implement inclusive **IAM governance** framework
  – *IAM Committee in place and reports up through IT governance structure*

• Deploy **enabling technologies** to improve IAM service capabilities
  – *SailPoint IdentityIQ selected as new IAM software foundation*

• Establish risk-based **level of assurance framework**
  – *In progress now*
IAM Enabling Technologies

Central directories and repositories of identity information

Identity Repository

Authentication services for enterprise and cloud applications

Authentication

Role-, rule-, and attribute-based authorization management

Authorization & Access Governance

Identity Administration & Provisioning

Digital identity management, password management, & identity data provisioning

IAM Services
IAM Enabling Technologies

Central directories and repositories of identity information

Identity Repository

Authentication services for enterprise and cloud applications

Authentication

Role-, rule-, and attribute-based authorization management

Authorization & Access Governance

Digital identity management, password management, & identity data provisioning

Identity Administration & Provisioning

SailPoint

SailPoint

IAM Services
Identity Administration & Provisioning

Features (in a Nutshell)

• Identity Store & Resource Connectors
  – Consolidated identity store to track “all things identity” – users, accounts, entitlements, etc.
  – Extensive connector library to integrate out-of-the-box with many on-premise and cloud applications

• Password Management
  – Support risk-based password policies
  – Provide mobile device friendly self-service user interface
Identity Administration & Provisioning Features (in a Nutshell) – Part 2!

• Automated Provisioning
  – Detect identity lifecycle events and automatically trigger identity attribute and access changes (“joiners, movers, leavers”)
  – Orchestrate automated and manual provisioning tasks

• IT Service Management Integration
  – Integrates with ServiceNow for a unified service request experience
Authorization & Access Governance Features

• Flexible Role Management Model, supporting:
  – Both enterprise-level roles and CSU-level roles
  – Both attribute-/rule-based roles and “requestable” roles
  – Multiple role types (could be tied to job type, resources needed, user characteristics, etc.)

• Access Requests
  – Easy-to-use access request wizard
  – Configurable request approval workflow
More Authorization & Access Governance Features

• Access Policy Management
  – Define *separation-of-duties* or other access policies
  – Automatically *detect, report, and remediate* violations (if desired)

• Access Certifications
  – Facilitate *regular reviews of access*, time-based or event-based (such as an employee changing jobs)

• Authorization Reporting and Analytics
  – View “*who has access to what*” across multiple applications
  – Analyze authorization data for *role mining*
Even More Authorization & Access Governance Features

• Change Control
  – Role changes go through approval & impact analysis process

• Role Versioning
  – Roles have version control and changes can be rolled back, if needed

• Role Certifications
  – Periodic reviews of both role composition and role membership
Multiple Role Models are Supported

- **Birthright** roles
  - Assigned automatically based on attributes or business rules
  - Typically of interest across the enterprise
- **Use case** roles – geared to meet a specific business need, for example:
  - Streamline on-boarding/off-boarding in a department using position-based authorizations
  - Allow one system to “see” and leverage role information from another system
- **Simple** roles
  - Groupings of commonly requested entitlements
  - Usually assigned through a request/approval process
Sample Role Approaches: “Entitlement” Focus

- Role
  - Application
- Role
  - Application
- Role
  - VPN
- Role
  - Email
- Role
  - ID Card
Sample Role Approaches: “Entitlement” Focus
Sample Role Approaches:
“Entitlement” Focus
Sample Role Approaches: “IT Role” Focus

- Role
  - Application
- Role
  - Application
- Role
  - VPN
- Role
  - Email
- Role
  - ID Card
Sample Role Approaches: “Business Role” Focus
How does it fit together?

- Identity Source Systems
  - Identity Data
  - Application ("Unconnected")
  - Application ("Connected")
  - Application ("Indirectly connected")

- SailPoint IdentityIQ
  - Identity Data
  - Authorization Data
  - Identity & Group Data

- ServiceNow
  - Requests & Provisioning
  - Identity & Group Data
  - Directory Services (TED, AD, etc.)
  - Group data
How does it fit together?

Identity Source Systems

Identity Data

SailPoint IdentityIQ

Requests & Provisioning

ServiceNow

Directory Services (TED, AD, etc.)

Group data

Identity & Group Data

Authorization Data

Authorization Data

Application ("Unconnected")

Application ("Connected")

Application ("Indirectly connected")

Identity Data

Requests & Provisioning

Identity & Group Data

Authorization Data

Authorization Data

Application ("Unconnected")

Application ("Connected")

Application ("Indirectly connected")
How does it fit together?

- Identity Source Systems
- SailPoint IdentityIQ
- Application (“Unconnected”)
- Application (“Connected”)
- Application (“Indirectly connected”)
- ServiceNow
- Directory Services (TED, AD, etc.)

Connections:
- Identity Data
- Authorization Data
- Requests & Provisioning
- Identity & Group Data

Applications:
- Identity Data
- Authorization Data
How does it fit together?

1. **Identity Source Systems**
   - Identity Data
   - Authorization Data

2. **Application ("Unconnected")**

3. **Application ("Connected")**
   - Identity Data

4. **Application ("Indirectly connected")**
   - Identity & Group Data
   - Authorization Data

5. **SailPoint IdentityIQ**
   - Requests & Provisioning
   - Identity & Group Data
   - Authorization Data

6. **ServiceNow**
   - Directory Services (TED, AD, etc.)
   - Group Data
SailPoint IdentityIQ will be implemented in 3 phases

• Phase 1 (Feb 2016 – Feb 2017):
  – Technical Architecture
  – Group & Role Management

• Phase 2 (~Sep 2016 – ~Sep 2017):
  – Identity Administration & Provisioning
  – Password Management

• Phase 3 (mid 2017 – mid 2018):
  – Access Requests & Certification
  – Enterprise Authorization Reporting
Priorities for Initial Role Management Rollout

• Establish **basic functionality** and **role governance model/process**

• Implement **initial set of roles:**
  – Birthright roles: EID affiliations (current employee, current student, etc.)
  – Use case roles: Early adopter use case roles, such as reflecting Workday roles for use by other systems
  – Simple roles: Implement simple roles to address specific pain points

• Coordinate with **ServiceNow project** on service request process improvements

• Develop a **role adoption plan** to guide next steps
Rome wasn’t built in a day…

…and neither are roles

• Expansion and enhancement of role management will follow an iterative process:
  – Evaluate and prioritize role management needs and opportunities
  – Implement new roles or enhance use of existing roles
  – Repeat the process
Questions?

CW Belcher

cbelcher@austin.utexas.edu

512-232-6519
SailPoint IdentityIQ Overview

Business Services Committee

April 1, 2016