

IAM Roadmap Quarterly Review (Q4, FY21-22)

IAM Committee

Updated: August 31, 2022

Key Roadmap Priorities

- Identity Governance & Administration (IGA):
Modernize tools, reduce technical debt
- Authentication: Continuous improvement
- Directory Services: Unify platforms
- NEW: Audit findings

IGA Initiatives

| FY2021-2022 | Q3 | Q4 | FY2022-2023 Q1 |
|---|---|--|--|
| Initiative 1: Improve password security with new hash | <i>(Reduced scope due to resource constraints.)</i> | <i>(Reduced scope due to resource constraints.)</i> | <i>(Reduced scope due to resource constraints.)</i> |
| Initiative 2: Reduce technical debt by modernizing tools (IGA Modernization Program) | <ul style="list-style-type: none"> ✓ Stand up the Sandbox TAP environments. ✓ Begin design for EID Portal. ✓ Begin configuration of TAP solution to meet password management requirements. | <ul style="list-style-type: none"> ✓ Stand up the Test and Qual TAP environments. ✓ Complete configuration of TAP solution to meet group and role management requirements. ✓ Begin functional testing of TAP solution and remediate issues. ✓ Continue configuration of TAP solution to meet password management requirements. | <ul style="list-style-type: none"> <input type="checkbox"/> Complete security, functional, and non-functional testing of TAP solution and remediate issues. <input type="checkbox"/> Stand up the Production TAP environments. <input type="checkbox"/> Complete configuration of TAP solution to meet Phase 1 requirements. <input type="checkbox"/> Complete midPoint Service Planning. <input type="checkbox"/> Complete Phase 1 Go Live. <p style="text-align: right;"><i>(Reduced scope due to resourcing limits.)</i></p> |
| Initiative 3: Rightsize data retention with identity lifecycles | <i>(Reduced scope due to resource constraints.)</i> | <i>(Reduced scope due to resource constraints.)</i> | <ul style="list-style-type: none"> <input type="checkbox"/> Develop and test Sponsored Affiliates and Youth Protection Program affiliations. |
| Initiative 4: Group and role management strategy | <ul style="list-style-type: none"> ✓ Refine use cases. ✓ Plan implementation strategy. ✓ Implement use cases | <ul style="list-style-type: none"> ✓ Test use cases in Test. ✓ Finalize implementation strategy. | <ul style="list-style-type: none"> <input type="checkbox"/> Complete testing of use cases. <input type="checkbox"/> Complete Grouper Service Planning. |

IGA Initiatives

| FY2022-2023 | Q2 | Q3 | Q4 and beyond |
|---|---|--|---|
| Initiative 1: Improve password security with new hash | <i>(Reduced scope due to resource constraints.)</i> | <input type="checkbox"/> Complete analysis and determine approach for transition of TED & FI/ST mainframe authentication to new hash. | <input type="checkbox"/> Complete transition of TED & FI/ST mainframe authentication to new hash. <input type="checkbox"/> Retire old hashes and purge hash history. |
| Initiative 2: Reduce technical debt by modernizing tools (IGA Modernization Program) | <input type="checkbox"/> Define charter for Password Management focus for Phase 2. <input type="checkbox"/> Finalize Phase 2 project schedule. <input type="checkbox"/> Complete design for EID Portal. <input type="checkbox"/> Begin development of EID Portal. <input type="checkbox"/> Continue configuration of TAP solution to meet password management requirements. <input type="checkbox"/> Plan functional and non-functional testing of TAP solution for Phase 2. | <input type="checkbox"/> Complete midPoint upgrade to incorporate requested password management functionality (vendor dependency). <input type="checkbox"/> Complete configuration of TAP solution to meet password management requirements. <input type="checkbox"/> Continue development of EID Portal. <input type="checkbox"/> Begin functional and non-functional testing of TAP solution. | <input type="checkbox"/> Complete development of EID Portal. <input type="checkbox"/> Complete security, functional, and non-functional testing of TAP solution and remediate issues, including UAT. <input type="checkbox"/> Plan and complete external communications about upcoming changes. <input type="checkbox"/> Complete Phase 2 Go Live. <input type="checkbox"/> Define and finalize Phase 3 scope and project schedule. |
| Initiative 3: Rightsize data retention with identity lifecycles | <input type="checkbox"/> Deploy Sponsored Affiliates and Youth Protection Program affiliations. | <i>Completed in Q2.</i> | <i>Completed in Q2.</i> |
| Initiative 4: Group and role management strategy | <i>Completed in Q1.</i> | <i>Completed in Q1.</i> | <i>Completed in Q1.</i> |



Authentication Initiatives

| FY2021-2022 | Q3 | Q4 | FY 2022-FY2023 Q1 |
|---|--|--|---|
| Initiative 1: Separate Guest and Enterprise SSO | <ul style="list-style-type: none"> ✓ Investigate additional Guest Authentication early adopter(s) and determine next steps. | <ul style="list-style-type: none"> ✓ Investigate additional Guest Authentication early adopter(s) and determine next steps. | <ul style="list-style-type: none"> <input type="checkbox"/> Investigate additional Guest Authentication early adopter(s) and determine next steps <input type="checkbox"/> Produce Guest Authentication service plan and implement early adopter use cases. |
| Initiative 2: Continuous improvement | <p><i>(Reduced scope due to resource allocation for IGA Modernization.)</i></p> | <ul style="list-style-type: none"> ✓ Transition to GitHub actions. ✓ Investigate authn integration enhancements. <p><i>(Reduced scope due to resource allocation for IGA Modernization.)</i></p> | <ul style="list-style-type: none"> <input type="checkbox"/> Investigate Kubernetes implementation. <p><i>(Reduced scope due to resource allocation for IGA Modernization.)</i></p> |
| Initiative 3: Multi-factor authentication enhancements | <ul style="list-style-type: none"> ✓ Complete required changes to MFA registration portal for Duo Universal Prompt. | <ul style="list-style-type: none"> ✓ Coordinate externally to complete required changes for Duo Universal Prompt. ✓ Draft communication plan and update ServiceNow documentation. | <ul style="list-style-type: none"> <input type="checkbox"/> Execute communication plan and finalize ServiceNow documentation. <input type="checkbox"/> Deployment of required changes for Duo Universal Prompt (scheduled for October 19, 2022). |



Authentication Initiatives

| FY2022-2023 | Q2 | Q3 | Q4 and beyond |
|---|---|--|---|
| Initiative 1: Separate Guest and Enterprise SSO | <input type="checkbox"/> Deploy Guest Authentication for general availability. | <input type="checkbox"/> Begin transitioning customers to Guest Authentication. | <input type="checkbox"/> Continue transitioning customers to Guest Authentication. |
| Initiative 2: Continuous improvement | <input type="checkbox"/> Begin Kubernetes implementation. <i>(Reduced scope due to resource allocation for IGA Modernization.)</i> | <input type="checkbox"/> Continue Kubernetes implementation. <i>(Reduced scope due to resource allocation for IGA Modernization.)</i> | <input type="checkbox"/> Complete Kubernetes implementation. <input type="checkbox"/> Implement OpenID Connect. |
| Initiative 3: Multi-factor authentication enhancements | <input type="checkbox"/> Investigate disabling SMS functionality for certain affiliations. <input type="checkbox"/> Investigate approaches to reducing telephony credit usage. | <i>(Additional work to be determined based on investigations and Audit Finding 3.)</i> | <input type="checkbox"/> Investigate potential transition to Azure MFA. <i>(Additional work to be determined based on investigations.)</i> |

Directory Services Initiatives

| FY2021-2022 | Q3  | | Q4  | FY2022-2023 Q1 |
|--|--|--|--|----------------|
| Initiative 1: Retire WHIPS | <i>Customer transition from WHIPS to uTexas Enterprise Directory (TED) put on hold due to resource allocation for IGA Modernization.</i> | | | |
| Initiative 2: TED Cloud Resiliency | ✓ Evaluate and create a TED cloud resiliency strategy. | <i>(Reduced scope due to resource allocation for IGA Modernization and Authentication Initiative 2.)</i> | <i>(Reduced scope due to resource allocation for IGA Modernization and Authentication Initiative 2.)</i> | |

Directory Services Initiatives

| FY2022-2023 | Q2  | Q3  | Q4 and beyond |
|--|--|--|--|
| Initiative 1: Retire WHIPS | <i>(Customer transition from WHIPS to uTexas Enterprise Directory (TED) put on hold due to resource allocation for IGA Modernization.)</i> | | <ul style="list-style-type: none"> <input type="checkbox"/> Remove WHIPS dependency from directory.utexas.edu web application. <input type="checkbox"/> Complete customer transition from WHIPS to uTexas Enterprise Directory (TED). <input type="checkbox"/> Retire and decommission WHIPS. |
| Initiative 2: TED Cloud Resiliency | <i>(Reduced scope due to resource allocation for IGA Modernization and Authentication Initiative 2 dependency.)</i> | | <ul style="list-style-type: none"> <input type="checkbox"/> Begin and complete TED cloud resiliency implementation. |

Audit Findings

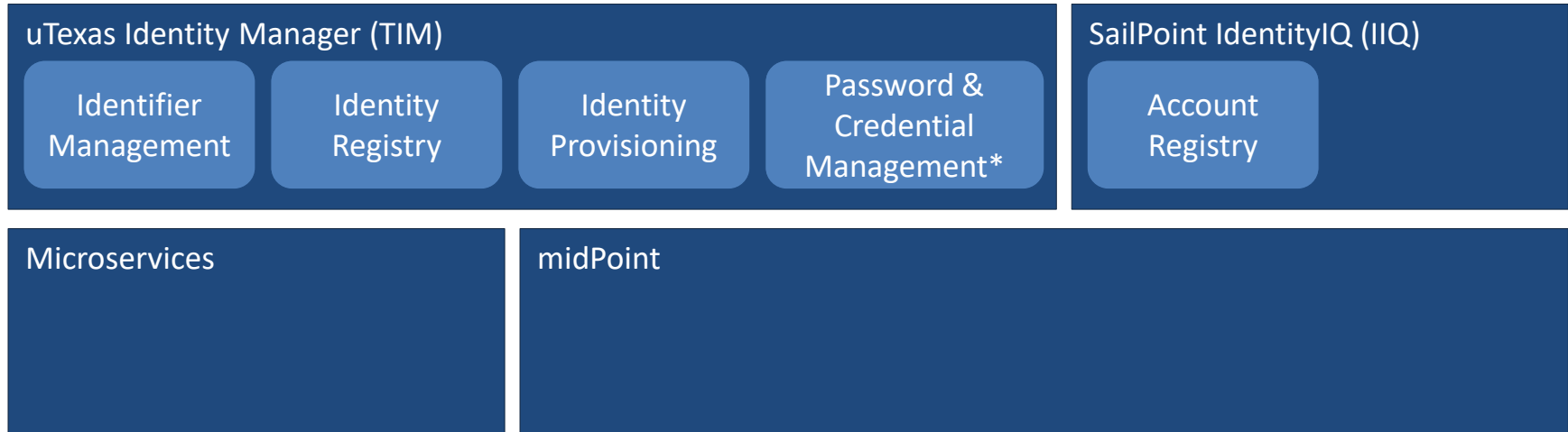
| FY2021-2022 | Q3 | Q4 | FY2022-2023 Q1 |
|---|---|---|---|
| Audit Finding 1: Standardized Account Management Due Date: August 2023 | <i>Audit report finalized May 2022.</i> | <i>(Reduced scope due to resource allocation for IGA Modernization.)</i> | <ul style="list-style-type: none"> <input type="checkbox"/> Plan approach to communicate and identify devices to apply device entitlement and/or transition to device EIDs. <input type="checkbox"/> Create a project plan. |
| Audit Finding 2: Privileged Access Management (PAM) solution Due Date: December 2023 | <i>Audit report finalized May 2022.</i> | <i>(Dependency on IGA Modernization Phase 2 Password Management functionality. EC: FY2022-2023 Q4)</i> | <i>(Dependency on IGA Modernization Phase 2 Password Management functionality. EC: FY2022-2023 Q4)</i> |
| Audit Finding 3: Length of Duo Trusted Sessions Due Date: August 2023 | <i>Audit report finalized May 2022.</i> | <ul style="list-style-type: none"> ✓ Complete implementation analysis and approach. <i>(Dependency on IGA Modernization Phase 1 Group and Role Management functionality. EC: FY2022-2023 Q1)</i> | <ul style="list-style-type: none"> <input type="checkbox"/> Finalize deployment plan of Duo Authentication Proxy. <input type="checkbox"/> Begin testing Duo Authentication Proxy. <i>(Dependency on IGA Modernization Phase 1 Group and Role Management functionality. EC: FY2022-2023 Q1)</i> |

Audit Findings

| FY2022-2023 | Q2 | Q3 | Q4 and beyond |
|---|---|---|--|
| Audit Finding 1: Standardized Account Management Due Date: August 2023 | <input type="checkbox"/> Begin process of transitioning devices to device entitlement and/or device EID. | <input type="checkbox"/> Continue process of transitioning devices to device entitlement and/or device EID. | <input type="checkbox"/> Complete process of transitioning devices to device entitlement and/or device EID. |
| Audit Finding 2: Privileged Access Management (PAM) solution Due Date: December 2023 | <input type="checkbox"/> Complete analysis and determine implementation approach. <i>(Dependency on IGA Modernization Phase 2 Password Management functionality. EC: FY2022-2023 Q4)</i> | <input type="checkbox"/> Create project plan. <input type="checkbox"/> Define and finalize requirements. <input type="checkbox"/> Create and finalize design. <i>(Dependency on IGA Modernization Phase 2 Password Management functionality. EC: FY2022-2023 Q4)</i> | <input type="checkbox"/> Create and execute communication plan. <input type="checkbox"/> Complete development of Stache connector. <input type="checkbox"/> Establish and enable Privileged Access Management (PAM) process. <input type="checkbox"/> Transition accounts to PAM process. |
| Audit Finding 3: Length of Duo Trusted Sessions Due Date: August 2023 | <input type="checkbox"/> Complete verifications of Duo security policies. <input type="checkbox"/> Build manageable group of campus IT community members to link to the custom Duo policy. <input type="checkbox"/> Create communication plan to share implementation plan with IT community. <input type="checkbox"/> Begin communication plan execution. | <input type="checkbox"/> Continue execution of communication plan. | <input type="checkbox"/> Enable new Duo security policy for identified IT community. This Duo policy will reduce the “Remember Me” feature from 30-days to 1-day and require staff to use Yubikeys. |

Identity Governance & Administration (IGA)

Identity Management: Current State



* TIM & Duo

Identity Governance & Administration (IGA)

Identity Management: Planned Future State

uTexas Identity Manager (TIM)

Retired

SailPoint IdentityIQ (IIQ)

Retired

Microservices

Identifier
Management

midPoint

Identity
Registry

Identity
Provisioning

Account
Registry

Password &
Credential
Management*

* midPoint or Azure Tool & Duo

Identity Governance & Administration (IGA)

Authorization Services: Current State

SailPoint IdentityIQ (IIQ)

Group & Role
Management

Authorization
Reporting and Review

Legacy Authorization Management

Apollo

*DPUSER

OHSC

Custom

Grouper

Identity Governance & Administration (IGA)

Authorization Services: Planned Future State

SailPoint IdentityIQ (IIQ)

Retired

Legacy Authorization Management

Apollo

*DPUSER

OHSC

Custom

Grouper

Group & Role
Management

Authorization
Reporting and Review

Authentication

Current State

Enterprise Authentication

Web SSO
(Shibboleth)

O365 Authentication

AD FS

Multifactor Authentication

Duo

Microsoft
2FA

Guest Authentication / Social ID

Cirrus
Identity

Network Authentication

FreeRADIUS

Cisco ACS

Directory Services

Current State

Enterprise Directory - LDAP

TED (OpenLDAP)

Windows Management & AD Groups

(Active Directory)

Public Directory

WPS (OpenLDAP)

Enterprise Directory - Mainframe

TOM (Adabas)

Directory Services

Planned Future State

Enterprise Directory - LDAP

TED (OpenLDAP)

Windows Management & AD Groups

(Active Directory)

Public Directory

Retired

Enterprise Directory - Mainframe

TOM (Adabas)