

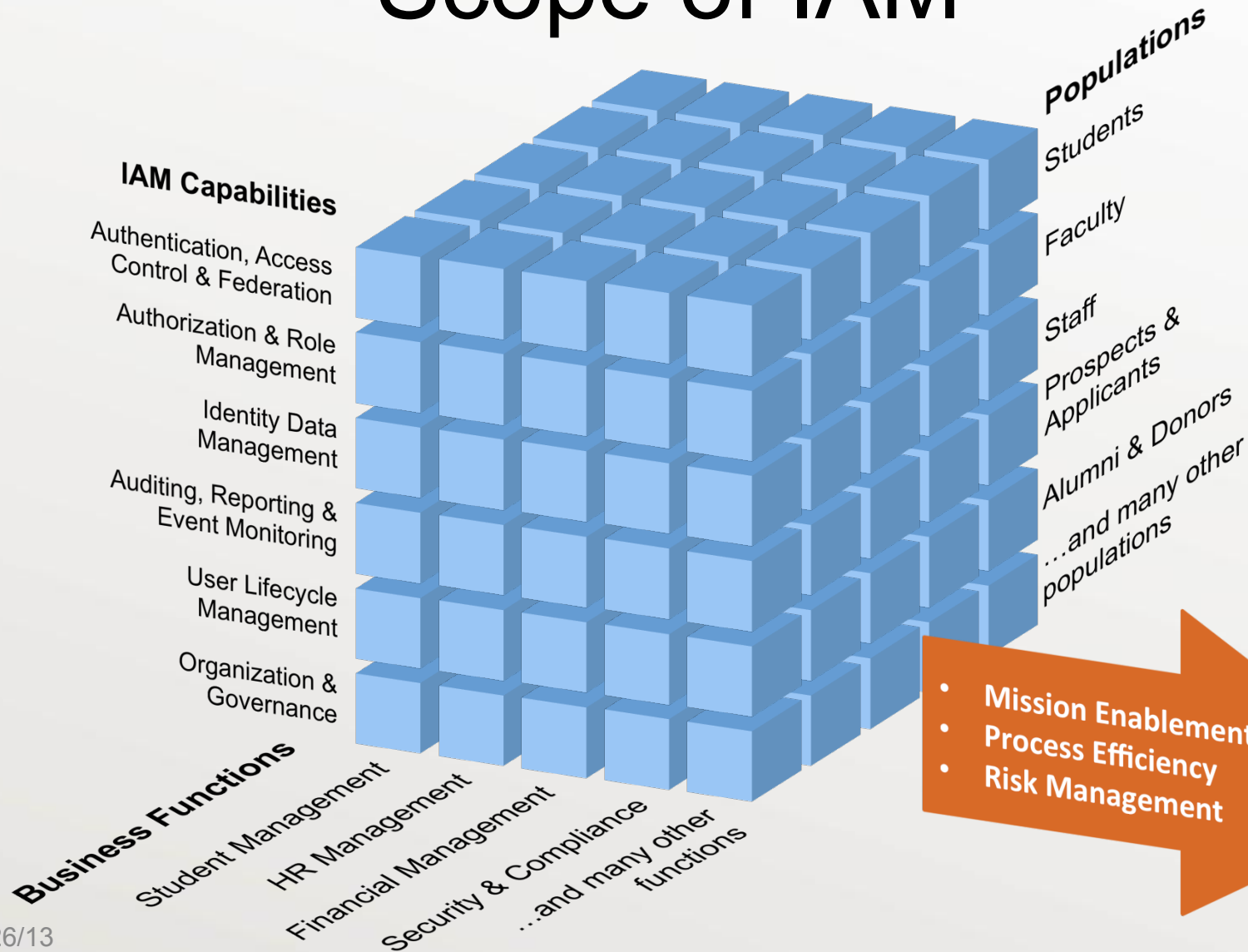
Identity & Access Management: Strategic Roadmap

April 2013

What is IAM?

- Identity & Access Management is the set of policies, process, and technologies used to manage digital identities and their access to resources
- Includes digital identity (EID) creation, password management, authentication, authorization, and related services

Scope of IAM







Current State of IAM





- UT's current IAM infrastructure is an aging mix of components, implemented in a piecemeal manner
- Existing infrastructure is unable to keep up with campus IAM needs, for example:
 - Easy-to-use services for returning and loosely affiliated populations (former students, applicants)
 - Seamless integration with hosted “cloud” services
 - Efficient provisioning of application access as well as deprovisioning when no longer needed
- Upcoming implementation of new administrative systems will introduce new requirements for IAM

Approach to Strategy Development

- Established project steering committee
- Engaged IAM strategy consultant (Identropy) to help us:
 - Interview campus stakeholders and peer institutions
 - Assess current IAM capabilities
 - Develop strategic recommendations and roadmap

What We Heard from Campus Stakeholders

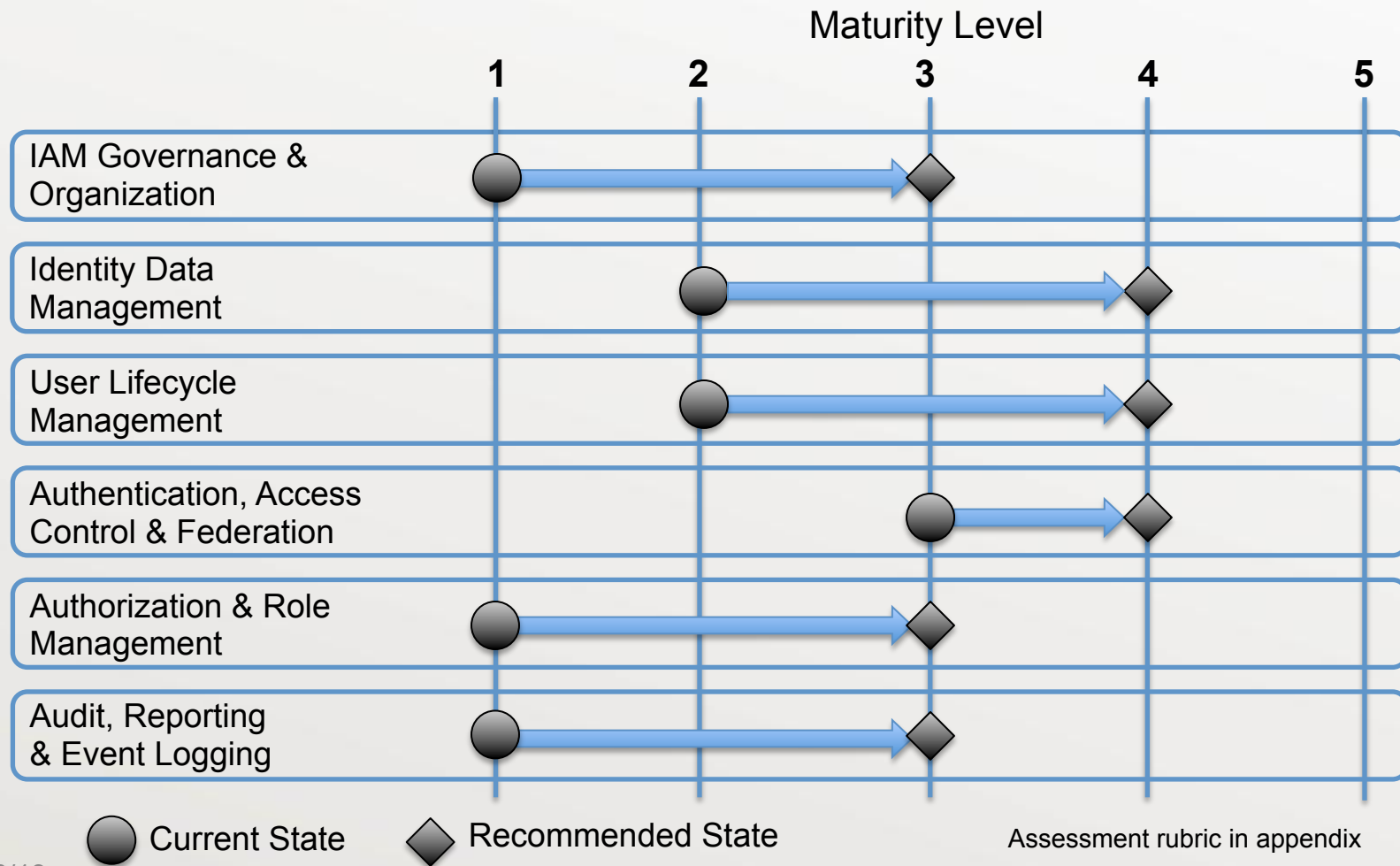
-  *“The colleges need to solve IAM problems themselves if there is not a Central IAM solution.”*
-  *“Our federated structure is core to how we operate. The departments and colleges can implement their own solutions if we are not filling their need centrally.”*
-  *“We tried to get students at another university access to our resources for a joint class, but it was too difficult, so we used their site.”*
-  *“We need to ability to easily group users for applications. For example, a list of people registered in a given class.”*

-  *“The process for creating a new password is especially difficult. It really affects our international students.”*
-  *“The ASMP will replace our legacy ERP platform. We haven’t selected the new platforms so IAM will need to accommodate all the likely scenarios.”*
-  *“We need guidelines, standards, and polices for selecting cloud solutions that will work with our IAM setup.”*
-  *“The current IAM infrastructure is very maintenance heavy. We would welcome a software package if it would reduce maintenance overhead.”*

What We Learned from Peer Universities

- All strive for one identity per person
- Most have mix of vendor and custom IAM solutions. Some investigating CIFER
- Existing group and role management solutions are custom-developed – moving to vendor and open-source
- Downstream provisioning interfaces are custom-developed – moving to ESB and Connector-based
- Struggles with cloud integration are common
- Some have an authorization repository. For others it's a goal
- Uneven IAM governance maturity but most have an IAM steering committee
- Most have an IAM roadmap but formality of update process is inconsistent

Identropy's Assessment of our IAM Capabilities



Key Takeaways from Assessment

- We have significant gaps between current and recommended maturity levels across all IAM capability areas
- Gaps are in both technology and adoption
- The Authentication area had a higher maturity level due to wide use of EID authentication and the upcoming transition to UTLogin

Identropy's Key Recommendations

To Enable the Mission...

- Employ an IAM shared service delivery model and deploy enabling technologies

To Drive Greater Adoption...

- Implement an inclusive IAM governance framework

To Balance Security with Usability...

- Establish a risk assessment and level of assurance framework

IAM Shared Services Model

IAM Shared Service

Providing a common set of IAM services for consumption by multiple organizations within the university

Design Principles

- Standardization
- Visibility
- Reusability
- Platform Independence
- Extensibility
- Location Transparency
- Reliability

Success Factors

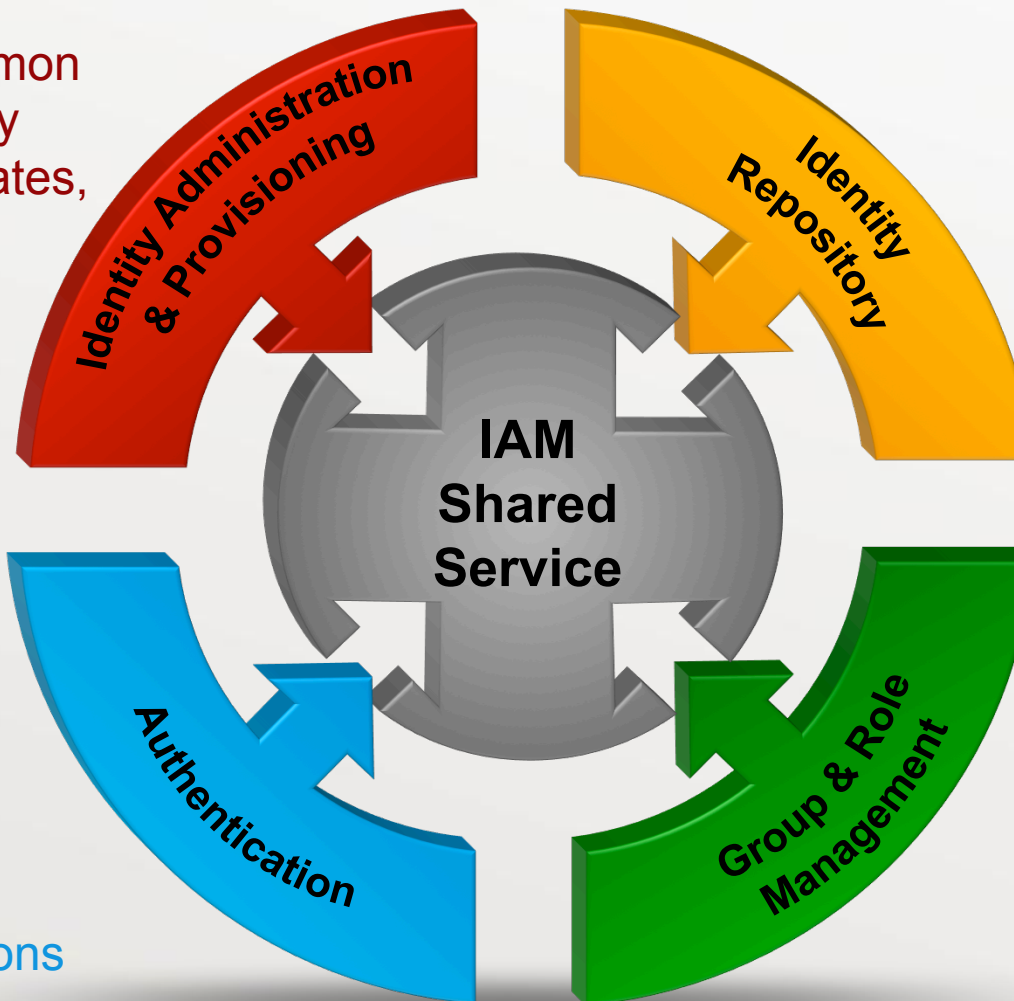
- Executive Support
- Cultural Change
- Business Process Reengineering
- Technology Enablement
- Resource Realignment
- Adoption Strategy
- Continuous Improvement

Common Metrics

- Usage
- Uptake
- Satisfaction
- Efficiency
- Effectiveness

IAM Enabling Technologies

Leverage common tools for identity creations, updates, and removals

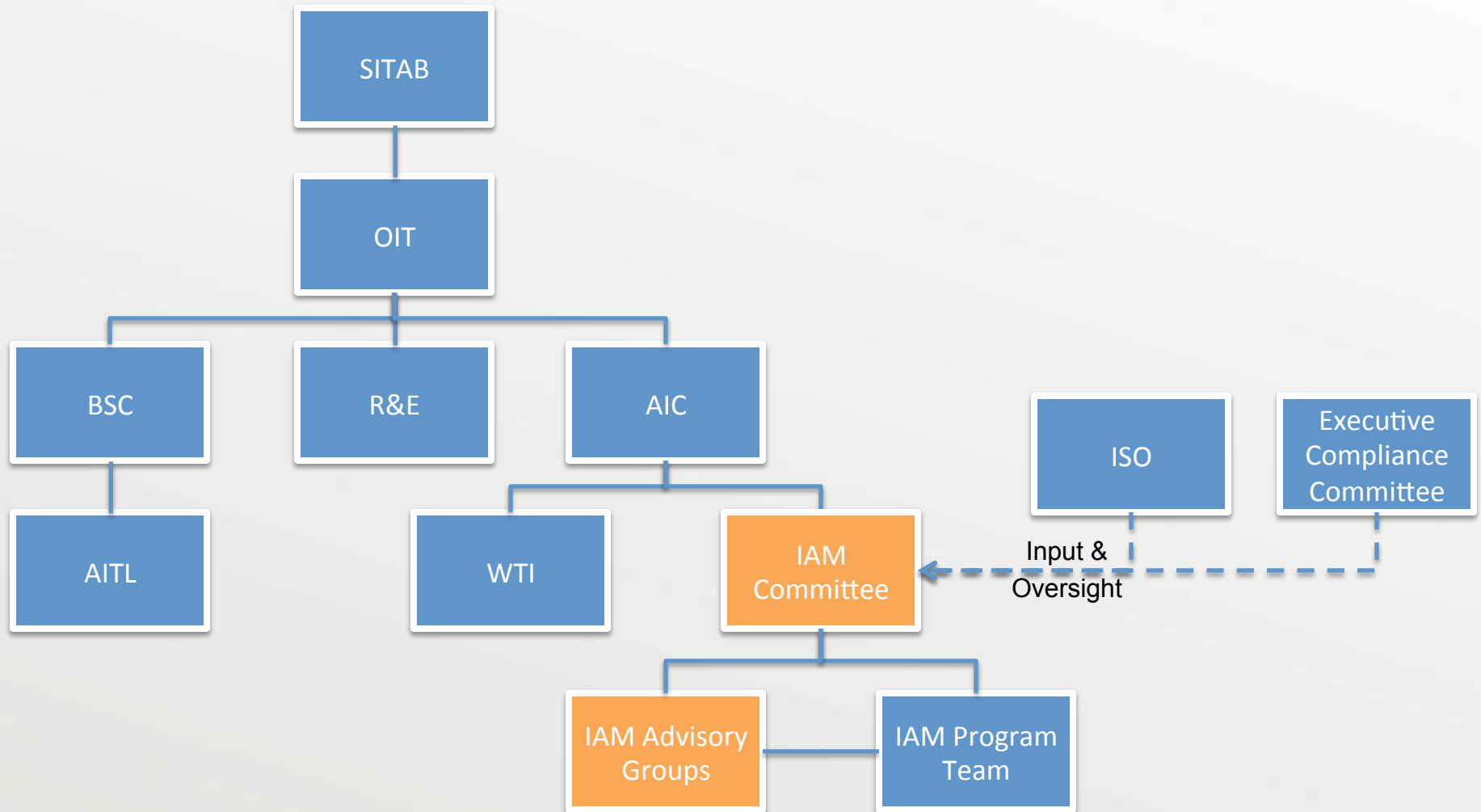


Single source to know “who has access to what”

Authentication services for enterprise and cloud applications

Delegated management of dynamic and static groups

Recommended IAM Governance Structure



New IAM Governance Groups

- IAM Committee
 - Permanent subcommittee of AIC
 - Includes business and technical representation from across campus
- IAM Advisory Groups
 - Business and technical advisory groups established for particular initiatives or projects
 - Allows in-depth stakeholder participation in specific areas of interest

Risk Assessment and Levels of Assurance Framework

Conduct Application Function Risk Assessment

- Use objective assessment rubric to quantify application risks

Determine Required Levels of Assurance

- Map risk levels to level of assurance framework

Select Authentication Mechanisms

- Choose authentication tools to meet required level of assurance – balancing security with usability

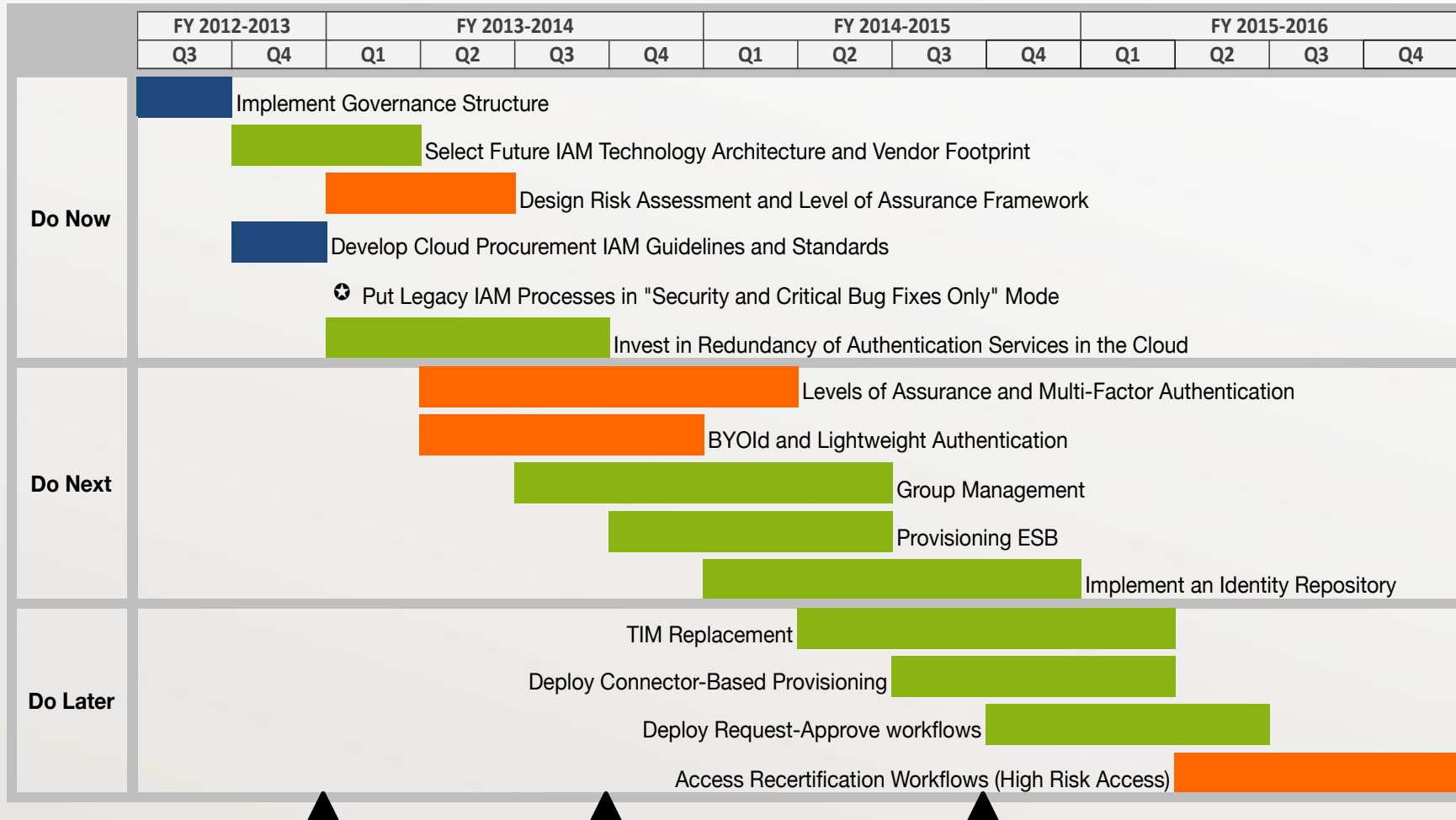
Risk Assessment Framework Example

Potential Impact of Authentication Errors	Level 1	Level 2	Level 3	Level 4
Inconvenience, distress, or damage to university standing or reputation	Low risk	Moderate risk	High risk	High risk
Financial loss or university liability	Low risk	Moderate risk	High risk	High risk
Harm to university programs or public interest	n/a	Low risk	Moderate risk	High risk
Unauthorized release of sensitive information	n/a	Low risk	Moderate risk	High risk
Personal safety	n/a	n/a	Low risk	Moderate or high risk
Civil or criminal violations	n/a	Low risk	Moderate risk	High risk

Roadmapping Approach

- *Do Now:* Implement building blocks
 - Establish governance structure
 - Select IAM architecture and vendor footprint
 - Design risk assessment and assurance level framework
- *Do Next:* Address key functional gaps
- *Do Later:* Replace existing infrastructure (TIM) and build out new capabilities

IAM Roadmap



Appendix: IAM Capability Assessment Rubric

Capability	Scoring Rubric
IAM Governance & Organization	<ul style="list-style-type: none"> • 5 = Formal IAM Governance is serving the needs for visibility for all stakeholders • 4 = IAM Governance is part of a larger IT governance framework and manages with metrics and SLAs • 3 = IAM Governance is part of a larger IT Governance framework and includes formal subcommittees • 2 = IAM Governance is formal but is not part of a larger IT governance framework • 1 = IAM Governance is informal
Identity Data Management	<ul style="list-style-type: none"> • 5 = All accounts & roles centrally provisioned and reconciled • 4 = Centralized account & role provisioning processes in use • 3 = Internal accounts provisioned, roles local in applications • 2 = Single registry exists, some provisioning is automated • 1 = No single registry of users
User Lifecycle Management	<ul style="list-style-type: none"> • 5 = User lifecycle is managed centrally, request and approval processes are segregated and captured • 4 = Most lifecycle processes are centralized, approvals are generally captured • 3 = Most lifecycle processes are centralized, approvals are generally out-of-band • 2 = Identity is created centrally, but remaining lifecycle processes decentralized • 1 = Identity Management processes are tribal knowledge
Authentication, Access Control & Federation	<ul style="list-style-type: none"> • 5 = Federated single sign-on • 4 = Single sign-on with strong authentication • 3 = Single sign-on, static password • 2 = LDAP directory authentication, static password • 1 = Local username, local static password
Authorization & Role Management	<ul style="list-style-type: none"> • 5 = Business roles are defined and leveraged for (de)provisioning and transfers • 4 = Business roles are defined and leveraged for (de)provisioning • 3 = Centralized group management processes exist and are widely leveraged • 2 = Centralized group management processes exist but are not widely leveraged • 1 = Authorization processes are decentralized and not coordinated
Audit, Reporting, & Event Monitoring	<ul style="list-style-type: none"> • 5 = Risk-based access recertification cycles exist with quality control measures in place • 4 = Risk management framework used to establish appropriate recertification cycles • 3 = High-risk access is periodically recertified in an automated system • 2 = Access recertification tools exist but are not widely used • 1 = Access is not routinely audited or recertified