The Educause Toolkit for Developing an Identity and Access Management Program

David Sherry, CISO
Brown University

July 16-17, 2013
Standard disclaimer, and some polls
About the IAM Program Project Team
IAM Program Project Team

Team members:

- Matthew Dalton, Ohio University
- Erik Decker, Columbia U. Medical Center
- Jacob Farmer, Indiana University
- Shirley Payne, Univ. of Virginia
- David Sherry, Brown University
- Miguel Soldi, Univ. of Texas System
- Stephen Vieira, Comm. College of RI
- Don Volz, Texas State University, San Marcos
IAM Program Project Team History

- Discussions on the need held in early 2012
- The group was assembled and started meeting in March 2012
- Charter was brainstormed and approved
- Program outline was drafted
- BOF held at Security Professionals Conference in May
- Monthly meetings, with a goal of completion and publication in December of 2012
- IAM Online presentation in October of 2012
- Team disbanded in March 2013
- Published by Educause in May 2013
IAM Program Project Team Methodology

- Put together the project team, looking for breadth of missions and focus
- Perform an environmental scan of current resources
- Establish a direction of the final result
- Begin the framework
- Utilize feedback at every opportunity
- Finalize and publicize the result
IAM Program Project Team Charter

Mission/Purpose:
The Identity and Access Management (IAM) Program Project Team is focused on creating a roadmap for institutions to use in developing an IAM program (or to address gaps in their current offerings).

Goals:
- Provide structure or guidance for those starting IAM.
- Identify a policy framework that institutions may need to consider.
- Develop a policy template (or set of policy templates) that other campuses can use. (*note: changed to provide examples*)
- Provide guidance or awareness about IAM governance.
- Identify existing IAM policies or programs and provide use cases.
- Strengthen the business side of the IAM program.
IAM Program Project Team Charter

Target Audience:
- Those responsible for IAM policy development.
- Those who have IAM policies in place that need to be updated.
- People or functions impacted by regulatory requirements regarding access control (e.g., GLBA, HIPAA).
- Institutions developing an IAM program or set of policies for the first time.

In scope:
- Actionable steps
- Preparation tasks
- Foundation
- Policy
- Technology *needs* (Note: tools and technologies are NOT in scope)
IAM Program Project Team Assumptions

- Organizations are complex to a point that simple traditional access and authorization to information assets is not scalable.
- A regulatory pressures are pressuring the organizations to better manage its access control and authorization.
- There must be policies and organizational structure in place to support any successful IAM Program.
- We also feel that a “potential assumption” is that the context of an IAM program may be useful for creating or validating context around other technologies, such as monitoring, DLP and SIEM.
IAM Program Toolkit – how is it laid out?

Each of the outline sections contains:

- High level overview of the section
- Key questions to ask
- Case studies, and/or use cases
- Other resources

As this is a living document, additional resources will continue to be added.
Outline of the toolkit......
Section 1: The Big Picture
The IAM Program – *The Big Picture*
The IAM Program – *The Reality*

How do I get from *HERE* to *THERE*?
The IAM Program – An Outline

So, where are we heading?

Destination: Understand where you are starting from, and what you are trying to accomplish.

Why are we heading there?

Business and Regulatory Drivers:
- Increase / improve security
- Compliance with Federal and State Rules
- Inter / Intra institutional collaboration
- Operational efficiencies and cost control

What is the landscape like?

- Single Campus or University System?
- Homogeneous or Diverse environments?
- Consistent governance policies?
- Significant differences in campus size and budgets?
- Significant differences in culture?
- Multiple constituency affiliations?
- Affiliation life-cycles?
- Expertise and skill sets availability?
- Information technology roadmap?

Why is this important?

Institutional Strategic Direction / Policy Says So:
- Examples:
  - Elimination of SSNs as identifiers
  - Deployment of a robust and secure interoperable infrastructure for support of inter-institutional collaboration is a strategic goal

State Policy Says So:
- Example:
  - Texas Administrative Code (TAC-202) Authentication / Authorization
  - “Identification shall be authenticated before the information resource system may grant access.”

The Feds Says So:
- New regulations require more stringent IAM processes:
  - HIPAA
  - FERPA
  - Sarbanes-Oxley
  - Graham-Leach-Bliley

Who is on board?

Stakeholders:
- IT Management
- Data Stewards
- Policy Stewards
- Application Sponsors
- Resource Users:
  - Staff
  - Faculty
  - Students
  - Residents
  - Applicants
  - Guests and Collaborators

How do we get there?

POLICY
- Roles
- Standards
- Procedures
- Responsibilities

TECHNOLOGY
- Registry
- Standards
- Provisioning
- Access Control

FOUNDATION
- Scope
- Budget
- Governance
- Staff

WHAT IS NEEDED MOST? ENABLERS?
- MONEY!!!
Section 2: What Comprises an IAM Program
The IAM Program - Outline

- Section 2: What comprises an IAM Program?
  - Three essential components:
    - A resource and governance foundation
    - A policy body
    - Technology
Section 3: Starting an IAM Program
The IAM Program - Outline

Section 3: Starting an IAM Program

3.1 Scope the Program
- Where are you starting from?
- What are you trying to accomplish?
- What key strategies / initiatives are you trying to support?

Key Questions to Ask (Some examples)
- At what stage of managing identity are we in (e.g., beginning, have something already in place, mature)?
- How important is flexibility, convenience and ease of use?
- How would the IAM Program align with the Institution’s Strategic Objectives?
- Policy work is very slow, but critical - how early should we start?
- How difficulty would be application integration with new or legacy infrastructure?
- How important is Federation? Build our Own or join InCommon?
3.2 Organizational Landscape

- Single campus? University System? It’s a Jungle out there?
- Homogeneous or Diverse environments?
- Consistent governance policies?
- Significant differences in campus size and budgets?
- Significant differences in culture?
- Multiple constituency affiliations? (Some Examples)
  - Formal and Casual
  - Dependent and Exclusive
    - Administrators with Faculty appointments
    - Student Staff
- Affiliation Life-Cycles? (Some Examples)
  - Applicant → Employee/Staff/Faculty → [Departmental Affiliation Change] -> Former employee
  - Prospective/Expected User → Active User → Deactivated User → Deleted User
The IAM Program - Outline

Section 3: Starting an IAM Program

3.3 Identifying Stakeholders

- IT Management,
- Data and Policy Stewards
- Subject (a/k/a user, principal, or customer)
- Identity Provider (a/k/a credential service provider, CA)
- Relying Party (a/k/a service provider, vendor)
- Service Consumers:
  - Staff and retirees,
  - Faculty and researchers,
  - Students and alumni
  - Guests,
  - Applicants, and members of the community
- Service providers
- Role Provider

Source: Thomas J. Smedinghoff, Chair of ABA Identity management Legal Task Force
The IAM Program - Outline

- Section 3: Starting an IAM Program

  - 3.4 Defining Program Ownership / Governance
    - Ownership / funding
      - Ramp up and on-going
    - Staff Roles and Responsibilities
      - Ramping Up
        - SME’s, HR, registrar, CIO, CISO, programmers, etc
      - Ongoing
        - Functional and technical staff, oversight, etc
    - Strategies for Procuring Talent
      - Skill set inventory
      - What to grow, what to buy, and what to outsource?
      - Institutional Subject Matter Experts?
      - Job Descriptions
Section 4: Developing a Policy Framework
The IAM Program - Outline

Section 4: Developing a Policy Framework

- What body of polices should be considered for an IAM Program?
  - Data Inventory and Classification Policy
  - Access Management Policy
    - Identity Lifecycle
    - Issuing and Revoking Credentials
    - Least Access / Business Need Based
    - Role-Based Access
    - Standard schema definitions (eduPerson?)
  - Federated Access Policy
    - Federation Operating Procedures
    - Attribute Release Policies
  - Acceptable Use Policy
  - Eligible Affiliations
  - Remote Access

- Use Cases and Resources of Model Policies
The IAM Program - Outline

- Section 5: A helpful glossary
  - Alphabetical list of regulations, acronyms, and definitions
  - There’s no way I’m going to list (or read) them all for you
Your thoughts?
The IAM Program - Outline

- Would your institution find this helpful?
- What are we missing?
- What areas need work?
- What do you think is most helpful?
Summary

• There is a need for IAM supporting materials, no matter what the size or affiliation of each institution

• Educause saw the need for a toolkit, and volunteers delivered

• There is much still to do, and much still to learn from each other
Where to find the program toolkit:


• Or, simply go to educause.edu and search for “IAM toolkit”
Feel free to contact me to follow up on any of the IAM Program:

David Sherry, CISSP CISM
Chief Information Security Officer
Brown University
Campus Box 1885
Providence, RI 02912
401-863-7266
david_sherry@brown.edu