INTRODUCTION TO
IDENTITY MANAGEMENT

INTERNET2 TECHNOLOGY EXCHANGE
OCTOBER 28, 2014

Nathan Dors
Assistant Director, Identity & Access Management
University of Washington
PURPOSE

QUESTIONS

> What are the purposes behind developing and deploying an identity management system?
> What problems does it solve?
> What are the benefits?
> What’s the value?
> Why now?
AGENDA

TOPICS

> 1:30pm – Welcome
> 1:40pm – What is IAM? (Nathan)
> 1:45pm – Why Do We Care? (Dennis, Mark)
> 2:30pm – Walk-through (Nathan)
> 3:00pm – Adjourn
WHAT IS IAM?

IDENTITY & ACCESS MANAGEMENT

> An acronym?
> A set of related processes?
> A complex undertaking?
> A project... or a program?
> A discipline?
WHAT IS IAM?

DEFINITION

“Identity and access management is a security, risk management, and business discipline that ensures the right individuals have the right access to the right resources at the right time for the right reasons.”

(Source: Gartner, Inc.)
WHAT IS IAM?

IDENTITY MANAGEMENT

WHO YOU ARE

- name
- image
- identifiers
- contact info
- address, location
- biographical sketch, tagline
- belongings (nationality, groups, affiliations, demographics)
- other indicators of identity (biometrics)
- privacy and data sharing preferences
- interests, intentions
- activities, responsibilities, projects
- reputation
WHAT IS IAM?

ACCESS MANAGEMENT

WHAT YOU CAN DO

– authority
– delegation
– roles
– groups
– permissions
– entitlements
– limits, constraints
– as they relate to access to resources
WHAT IS IAM?

A team.

At the UW, IAM is an organizational unit with these responsibilities:

- Identity registration & administration
- Account & password management
- Access management
- Authentication & Authorization
- Non-person identity management
- Federation & trust
WHAT IS IAM?

A set of services.

We offer these IAM services through the central IT service catalog:

- UW NetID
- Access Management
- Authentication
- Directory Services
- UW Windows Infrastructure
WHAT IS IAM?

A set of capabilities.

The essential work of our IAM team is coordinating these IAM processes and activities with our diverse customers and stakeholders.
IDENTITY REGISTRATION & ADMINISTRATION

CUSTOMER ASKS:

“Help me register people affiliated with the university to participate in online activities.”
ACCOUNT & CREDENTIAL MANAGEMENT

CUSTOMER ASKS:

“Give me and my users trustworthy identification to use online.”
ACCESS GOVERNANCE & ADMINISTRATION

CUSTOMER ASKS:

“Help me manage how I enable and disable access to my resources.”
PROVISIONING & INTEGRATION

CUSTOMER ASKS:

“Help me integrate with identity services and orchestrate processes to provision data and access.”
ACCESS CONTROL

CUSTOMER ASKS:

“Help me authenticate and authorize users as they access my resources and make online transactions.”
REPORTING & ANALYTICS

CUSTOMER ASKS:

“Give me reports and activity data I can analyze to make decisions and manage risk.”
WHAT IS IAM?

IDENTITY & ACCESS MANAGEMENT

> More than an acronym
> A set of related processes
> A set of related services
> An enabler of solutions to complex problems
> A way to deliver value to customers

IAM is a means of delivering value to customers by helping them manage their users (who they are, what they can do) without the burden of operating the related IT services.
NEXT UP

WHY CAMPUS ADMINISTRATORS CARE

> Dennis Cromwell
  Associate Vice President, Client Services and Support
  Indiana University

> Mark McConahay
  Associate Vice Provost and Registrar
  Indiana University

Duration: 30min
NEXT UP: WALK-THROUGH

PURPOSE

- Demonstrate IAM functions
- Simulate IAM processes
- Discuss benefits
  - who?
  - how?
  - why?
- Discover themes & variations

Duration: 20-30min
SERVICE PROVIDER

- offers a service valuable to end users
- understands the value of the assets
- decides access control policy
- uses access controls to enforce policy
ACCESS CONTROL

- authenticates users – establishes user identity or externalizes this function to an authentication service
- authorizes actions – allow/deny access decisions based on user’s access roles and permissions; can be externalized to an access management service
ACCESS MANAGEMENT

> define roles and permissions
> add users to roles
> remove users from roles
> review a user’s access
> access request and approval workflows
> provide data for access control decisions
ACCOUNTS & CREDENTIALS

- issue credentials to registered users
- manage credential lifecycle
- help users recover account (resent password)
IDENTITY REGISTRATION

- issue credentials to registered users
- manage credential lifecycle
- help users recover account (resent password)
IDENTITY PROVIDER

- authenticates users – establishes user identity by verifying credentials issued to user
- can be used by a service provider to externalize user authentication
- provides identity assertions to service providers – username, attributes, etc.
POLICY & OVERSIGHT

- oversees decisions
- responsible for institutional risk
- decides investments