

# IAM Overview and Self-assessment Exercise

Keith Hazelton, UW-Madison & Internet2 MACE  
Renee Shuey, Penn State & InCommon TAC Co-chair  
InCommon CAMP, Columbus, 22 June 2011

# Who is IAM?

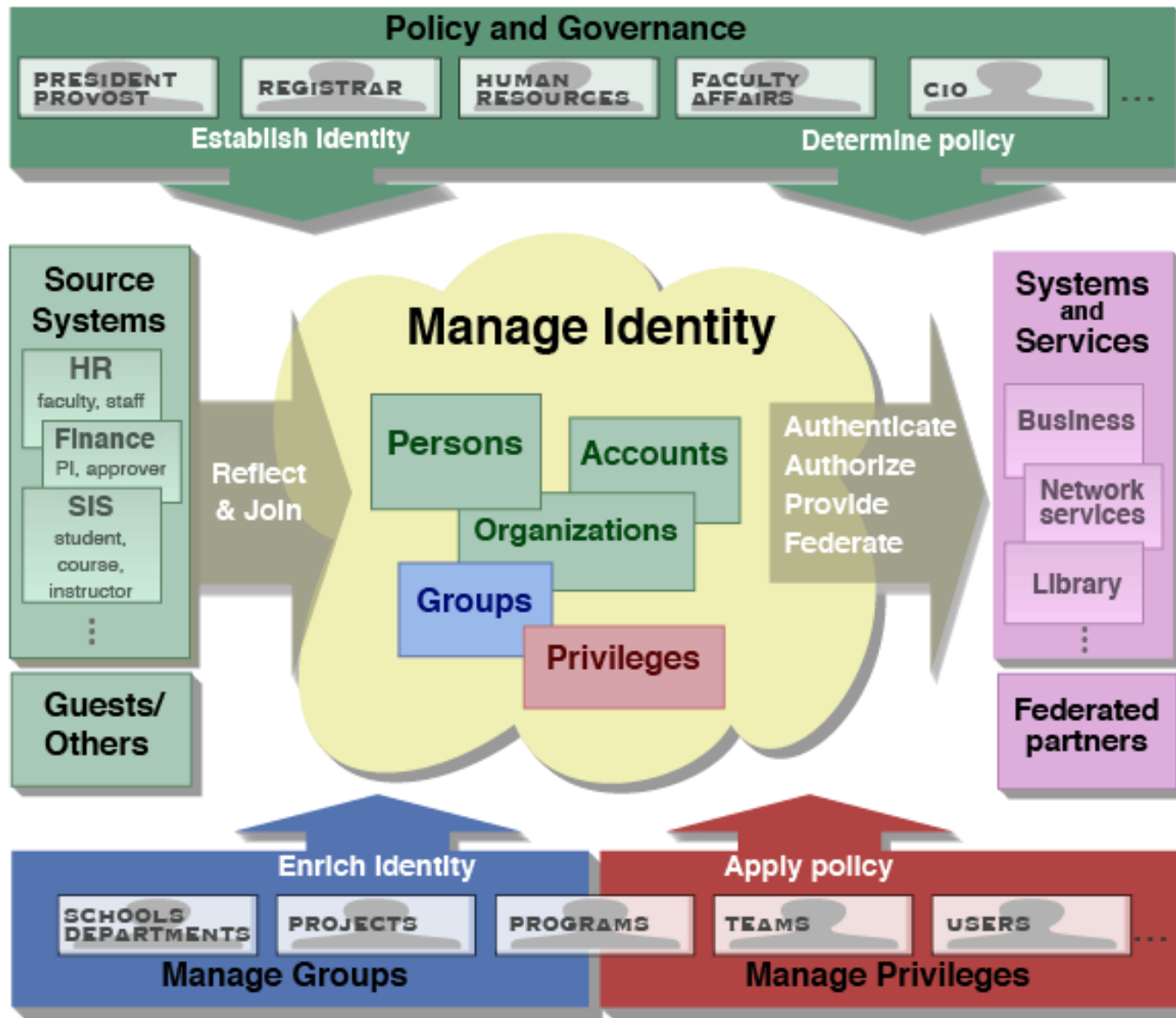
- Access to Protected Library Resources
- Library Staff Access to Integrated Library System
- Access to Library Public Workstations
- HMC Affiliate
- Access to Library Resources
- Access to Alumni Library Resources
- Access to Electronic Theses and Dissertations Web Site
- Graduate School Exit Survey
- Federating to blogging hosted Services
- Prospective students applying for financial aid
- Employee Confidentiality
- Provisioning of an employee's digital Identity
- Student early access to residence hall requests and immunization records submissions
- Grouper Auditing Use Case
- Continuing Education and Adult Students
- New Students Applying for Admissions and Oncampus Housing
- Prospective Students Visiting Penn State New Kensington
- New Faculty and Access to ANGEL and Other Class Resources
- Adjunct Faculty Activating Access Account
- New Faculty & Staff
- Selecting Benefits
- Terminated Faculty Member Maintains Access
- Physicians at the Hershey Medical Center and Access to Library Resources
- Patients, Family Members, and Visitors at the Penn State Hershey Medical Center
- Alumni Donors
- Alumni Association
- Local Community Member and Short Term Access Accounts
- Registrar Relationships
- Student Lifecycle
- New Students Applying for Undergraduate Admissions
- Provision of Access to Course Work For Students at a Distance
- Library Resources
- ITS Computer Store Access
- CIC CourseShare
- Deprovision User content after graduation or resignation
- Google Cache Updates
- Access to user content after graduation and or resignation
- Access to directory data
- Emergency Rehire
- Multiple IDs
- Deceased Employee Outreach Registration process
- Updating ISIS Security Profile
- Multiple Security Realms, Same Userids but Different Passwords
- ROTC Instructor Affiliation
- Instructor with Independent Contractor Status
- Name change switching in the directory
- Special Affiliates (for example Religious Affiliates)
- Father and son who is a JR
- Cloning ISIS Security Profiles
- New PSUid assigned for new PSU affiliation
- Student Football Tickets
- Department Identity
- DSL Use Case Interview
- Police Services Use Case Interview
- Police Services Use Case
- Police Log

# What is IAM?

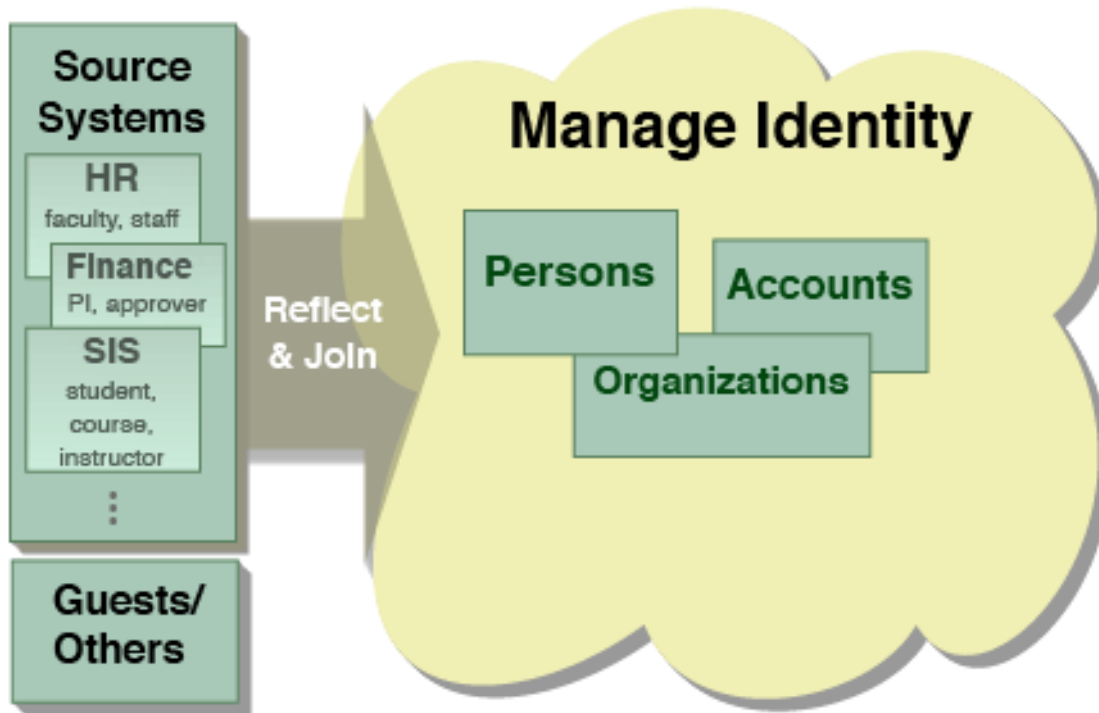
“....it is the **alignment of University business processes, policies, and technologies** that manage identities to support the delivery of rich and diverse array of online services for faculty, staff, and students....”

# Why IAM?

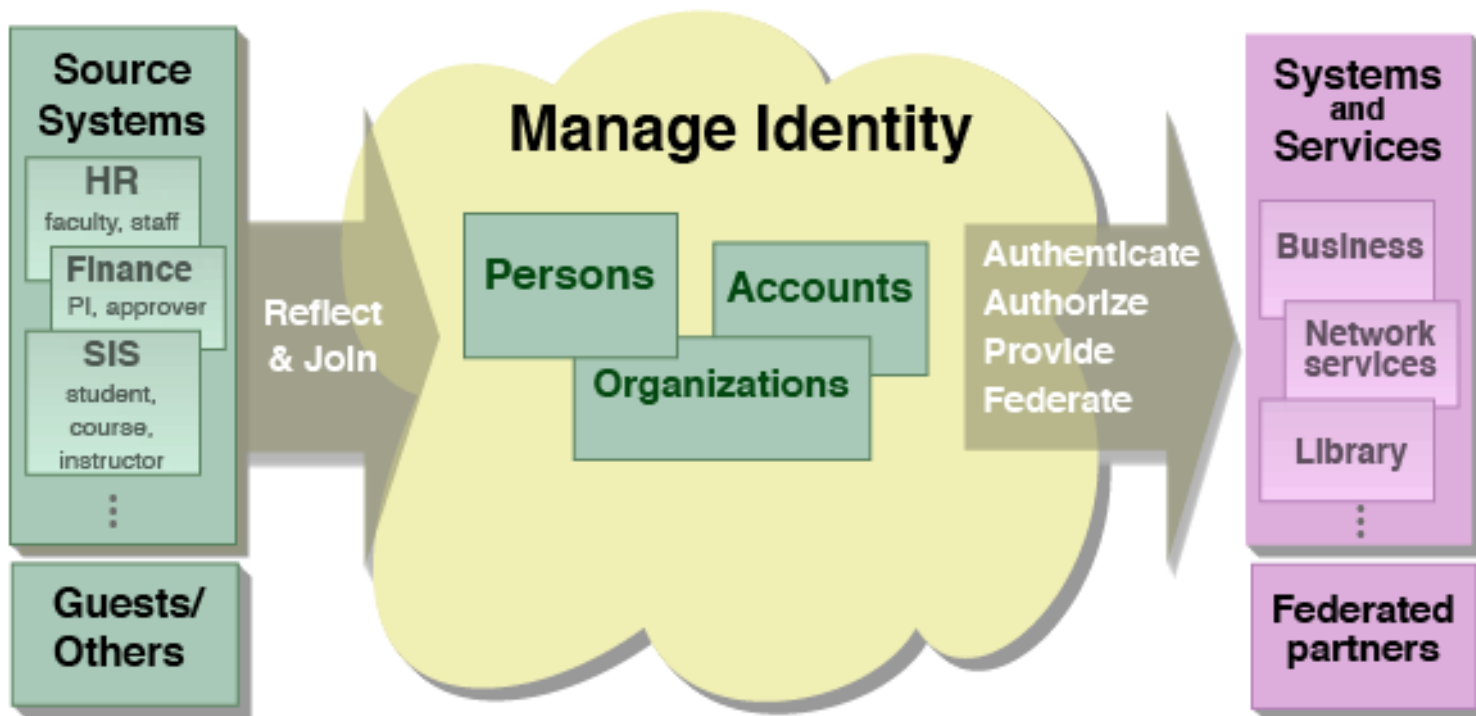
- Consolidation of multiple identity stores
- Simplify process for user's to manage identity information
- Mitigate Risk
- Provide flexibility to move to a more user centric IdM



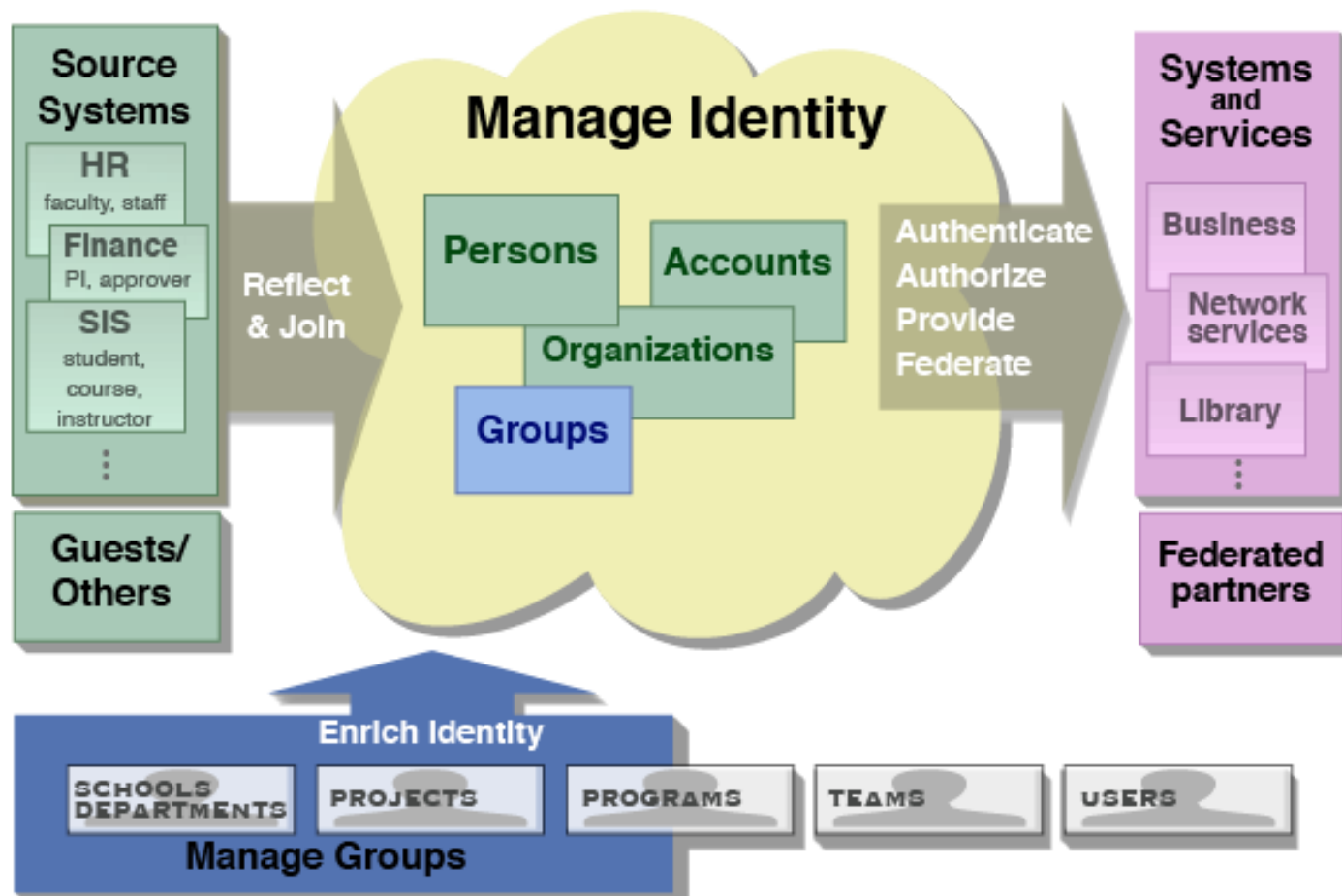
# Identity and Access Management Infrastructure Big Picture



## Foundational **Identity** Management

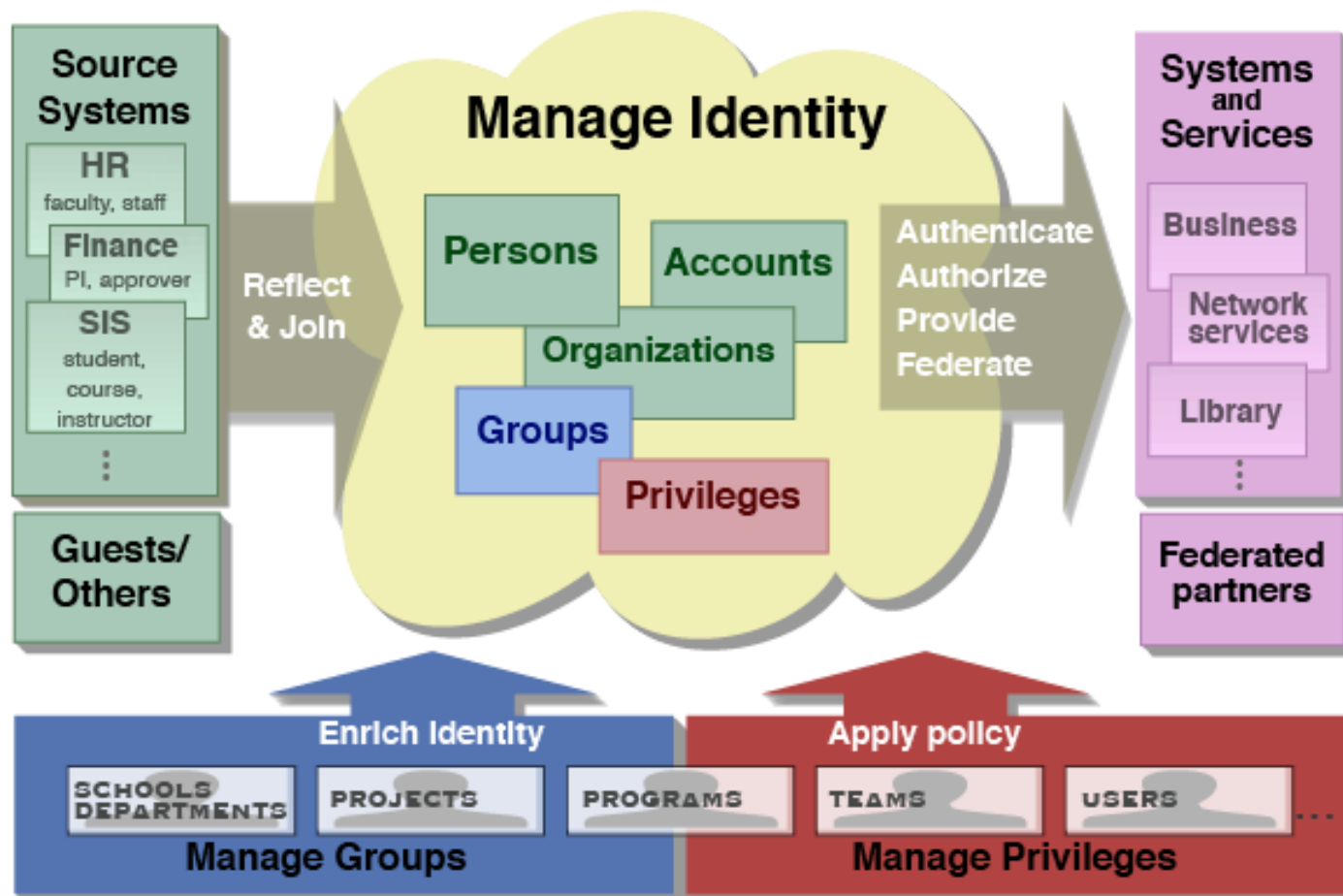


## **Identity *and Access* Management**

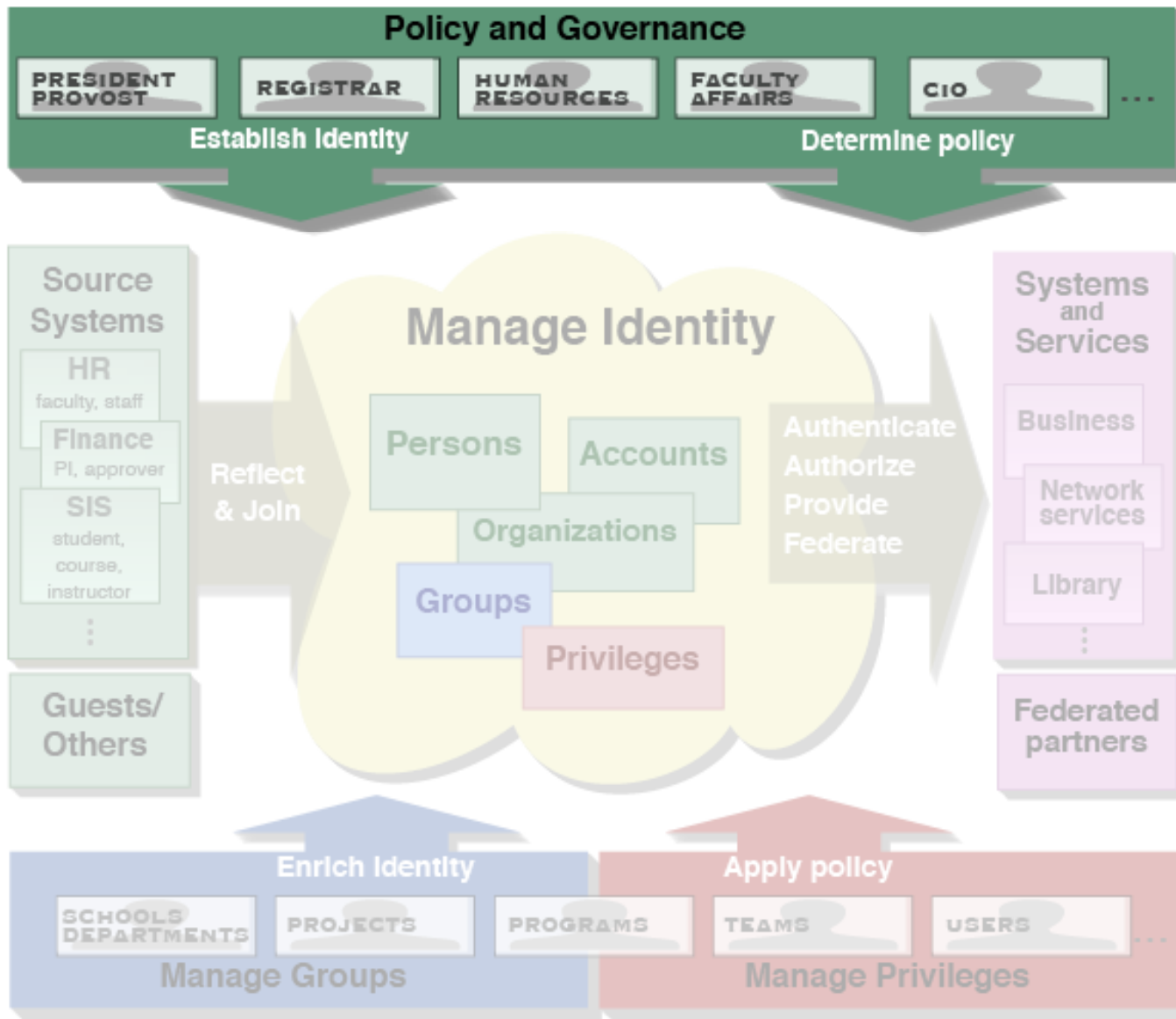


## Group and Role Management





## Privilege Management



# Identity and Access Management The Rest of the Story

# Governance

- Resolve conflicts, make decisions at the institutional level
- Attributes for Success:
  - Sustained lateral awareness of needs, challenges for the purposes of anticipating collisions before they happen
  - Recognizing what is possible and what we're striving for
  - Processes to make decisions when conflicts arise

# Governance

- People own their identity
- Within the institution, units/executives are stewards for a context
- Those contexts overlap in complicated, significant ways

# Governance

- What Kinds of Decisions
  - Methods, processes to resolve conflicts
  - Policy recommendations, changes, development
  - Set direction for process and technology requirements

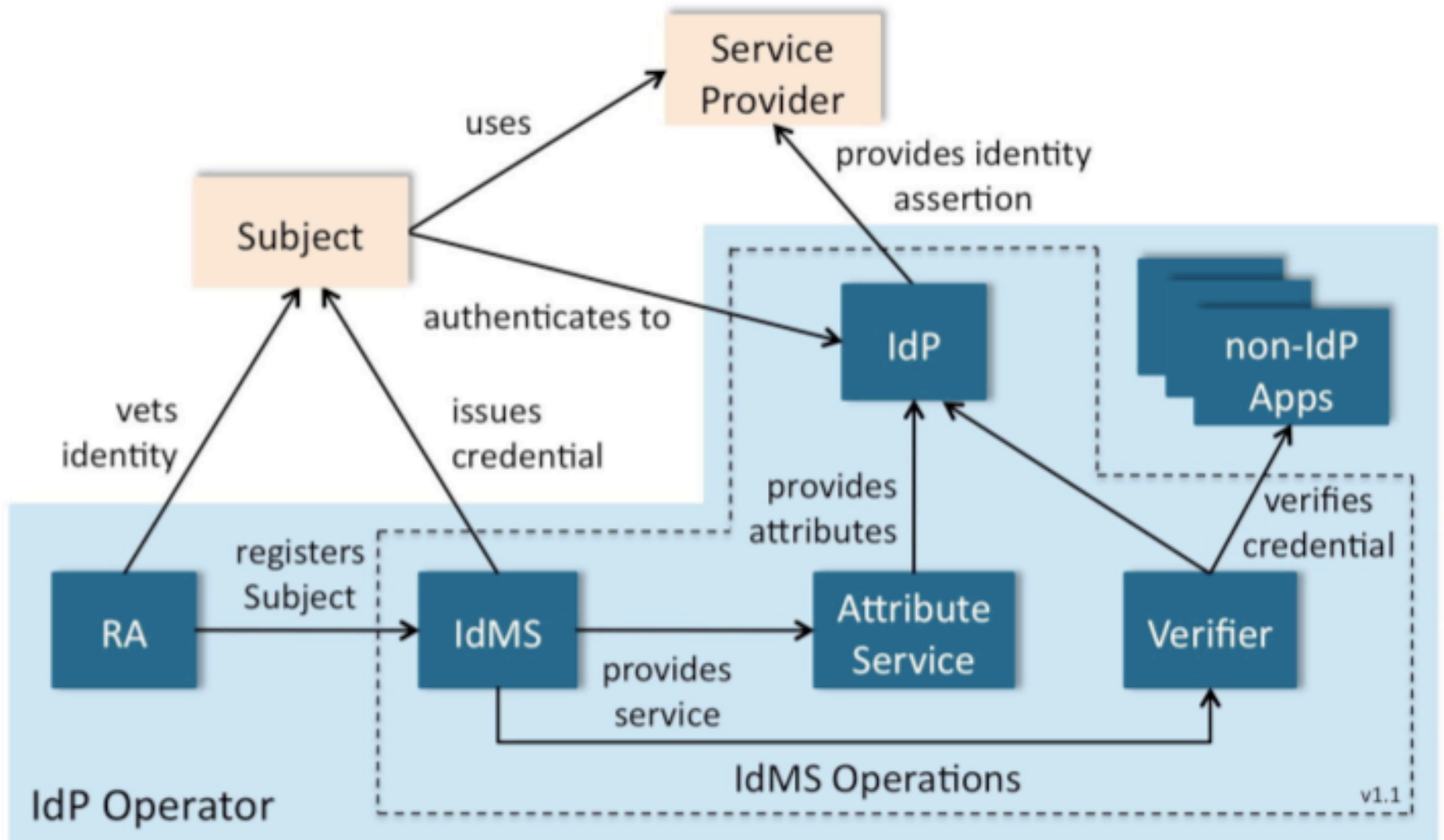
# Policy

- The establishment and adoption of policy is a key component to the success of an Identity and Access Management (IAM) implementation.
- “P”olicy vs. “p”olicy

# Policy - One Approach

Policy statement	Business Decisions	Business Rules	Guidelines	TAG(S)
<p>A principle or rule setting out desired outcome</p>	<p>The results of a deliberation regarding how to implement policy in practice.</p>	<p>a yes/no, left/right, up/down, split/join juncture on a flow chart.</p>	<p>A set of procedural "bridges" between existing systems and the CPR in Pilot (and applicable procedures - even some of what is currently in policy). Experience with these guidelines will inform refining of procedures and / or policies.</p>	
<p>The Central Person Registry is the authoritative source for the capture and storage of identity information.</p>	<p>The Central Person Registry will provide processes for other systems to add or update identity information.</p>		<p>Systems will pull informational identity data changes from the Central Person Registry via an electronic messaging service.</p>	<p>authoritative, source, cardinal</p>

# InCommon Identity Assurance Program Identity Management Functional Model





**The State of Identity  
Management  
Self-assessment  
Questionnaire**

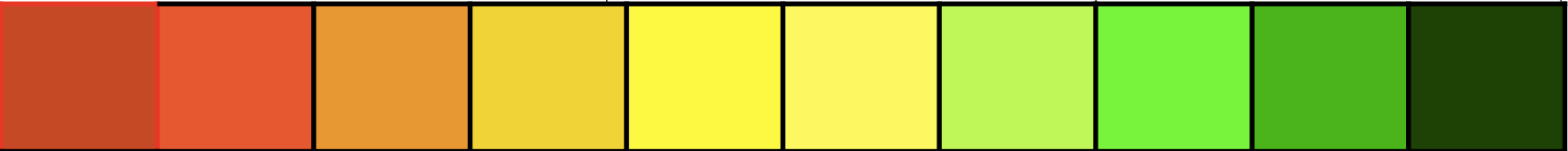
# External Collaboration

Collaboration with other institutions and entities beyond our own is rare or non-existent.		There is some ad-hoc collaboration with institutions and entities beyond or own.			Collaboration beyond our institution is a key component to our educational and research missions.				
1	2	3	4	5	6	7	8	9	10

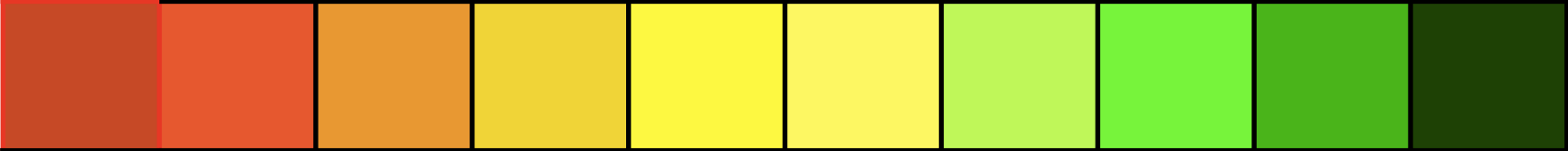
# Security of Identities and Authentication

We are comfortable permitting vendor access to BOTH our identity information AND authentication information.		We are comfortable permitting vendor access to EITHER identity information OR authentication information.		We are not comfortable releasing ANY authentication information and only releasing MINIMAL identity information to the vendor.															
1		2		3		4		5		6		7		8		9		10	

# Guests or weakly identified entities

<p>We do not have a centrally supported guest login. This brings weakly identified people into our identity management system that are poorly tracked and managed over time.</p>				<p>There is some ad-hoc collaboration with institutions and entities beyond our own.</p>			<p>Collaboration beyond our institution is a key component to our educational and research missions.</p>		
									
1	2	3	4	5	6	7	8	9	10

# INTEGRATION TECHNOLOGIES





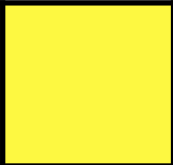
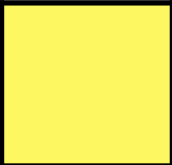
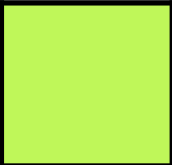
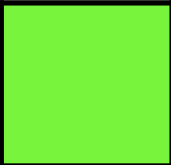


We gather information from sources with a mix of flat file transfer, reports, direct SQL access, and/or email.			We rely on batch processes but use consistent techniques with our clients and a common secured infrastructure.			We have realtime access to data, e.g., through LDAP, as well as an enterprise, message-based integration infrastructure.			
									
1	2	3	4	5	6	7	8	9	10





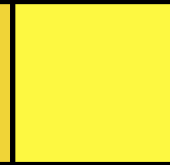
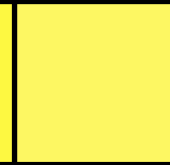
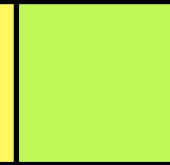
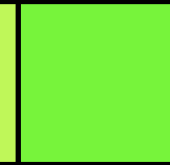
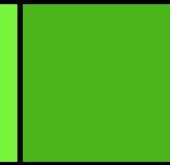

# Account Provisioning Process

Our processes are manual, ad-hoc, and not documented or well understood.			We have a mix of formal processes and those created on an as-needed basis. Some are automated and some are not.			Our processes are established, automated, and documented.			
1	2	3	4	5	6	7	8	9	10

# Account de-Provisioning



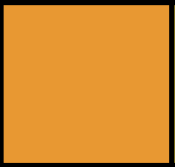

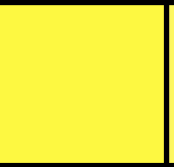

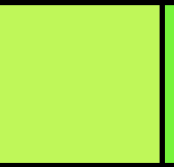
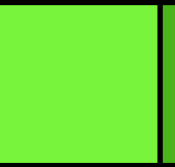


## process

<p>There is little connection between central IT support for core infrastructure and business systems, and distributed school or departments system. There means many independently maintained shadow systems with poor data sharing and little automated updates from common sources.</p>	<p>We can make data available, through reports or directory lookups to more directly enable local systems, but actual reuse is inconsistent across campus.</p>	<p>We support collaborative work in schools and departments by enabling them to define and share information and privileges on their own. It is easy to access common enterprise data, either for realtime reference or for ongoing synchronization.</p>							
									
1	2	3	4	5	6	7	8	9	10

<p>IT staff may find themselves making access management decisions where business rules don't exist and no decision-making body exists.</p>	<p>Policies providing a framework for consistent access management decisions are in development or in place.</p>	<p>Business units base access management decisions on policies and the classification of the data being protected.</p>							
									
<p>1</p>	<p>2</p>	<p>3</p>	<p>4</p>	<p>5</p>	<p>6</p>	<p>7</p>	<p>8</p>	<p>9</p>	<p>10</p>



# Practices

Our practices are ad-hoc at best.	We have a mix of formal practices and those created on an as-needed basis	Our practices are established and publicly posted.							
									
1	2	3	4	5	6	7	8	9	10

**Self Assessment -  
Group Exercise  
~30 Minutes**

# Additional Resources

- InCommon
  - <http://www.incommonfederation.org/>
- EDUCAUSE IdM
  - <http://www.educause.edu/iam>
- Grouper
  - <http://www.internet2.edu/grouper/>
- PACCMAN
  - <http://middleware.internet2.edu/paccman/>