October 7, 2015
CAMP at Internet2 Technology Exchange 2015

The State of the Program:
Identity and Access Management Self-Assessment

Instructions

Each item below describes an aspect of Identity and Access Management and provides four choices that roughly equate to the maturity level for that process or function. Choose the answer that best describes what your institution currently does today. Enter the number associated with your choice in the last column, calculate the subtotal for each section, and then tally your final total at the end.

This assessment is not a test that you can pass or fail but, instead, is a tool meant to help you identify the maturity of your IdM processes and infrastructure. It defines the characteristics of each maturity level in order to help you develop your IdM program with federation as the goal. It is likely that your institution may be at different maturity levels for the process or infrastructure of any given function. If you fall in between levels, you may use half points in your totals.

Maturity Levels

Practices are ad hoc and immature. There is no planning or processes for infrastructure or functions. Tasks are manual – not automated or connected – leading to inconsistent results.	Some tasks are repeatable, but results still vary. There is minimal planning, process definition, and documentation.	Policies, processes, and infrastructure are standardized across the enterprise. Some processes are automated. Identity data is standardized.	Processes are defined, automated, and measured. Policies are audited, enforced, and updated based on business risk. Identity data is standardized, integrated, and shared using standards.
Ad Hoc	Defined	Standardized	Optimized

This assessment is based on a tool first developed by Lynn McRae, Stanford University, updated by John O'Keefe, Lafayette College, further tailored for the TIER Workshops, and revised by Nathan Dors, University of Washington; Susan Neitsch, Texas A&M University; and Janemarie Duh, Lafayette College, for CAMP at Technology Exchange 2015.

1. Identity Data

1.1 Coverage

Our identity management system covers just the core community – faculty, staff and students – as defined by source systems.	Our identity management system includes faculty, staff, and students, plus secondary sources like library patrons, hospital staff, etc.	We collect information about all people of interest to schools, departments, research collaborators, central offices, libraries, guests, etc.	We collect information about all people of interest and have standard processes and system interfaces for adding new sources and managing the lifecycle of existing sources.	
1 point	2 points	3 points	4 points	Score

1.2 Integrity

We get information from many sources. It is possible that someone can be represented multiple times and it is difficult for us to detect except in reaction to service incidents.	We have good central identity matching processes, but work to resolve identity issues mostly as needed.	We have strong partners and practices across campus. Defined processes and systems aid in detecting, avoiding, and resolving identity issues.	We work with our partners to define data quality standards and continually improve processes to reduce error rates and improve auditability. Analytics are applied to issues.	
1 point	2 points	3 points	4 points	Score

1.3 Freshness

We periodically gather information from sources on cycles that can vary from daily, to weekly, or longer.	We regularly gather information from sources, generally no less than daily.	We have real-time or near-real-time connections to source systems, but there are delays propagating changes into services and access decisions.	Identity data is gathered real-time or near-real-time. Changes propagate to services and access decisions without significant delay.	
1 point	2 points	3 points	4 points	Score

Section Subtotal _____

2. Current State of Identity Infrastructure

2.1 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 real-time access to data, e.g., through LDAP or APIs.	We have real-time access to data, e.g., through LDAP or APIs, as well as an enterprise, message-based integration infrastructure.	
1 point	2 points	3 points	4 points	Score

2.2 Identifiers

We reuse our identifiers.	We support reused but persistent identifiers in our infrastructure.	We support non-reassignable persistent identifiers in our infrastructure.	We support non-reassignable persistent identifiers, and exception processes are defined and auditable.	
1 point	2 points	3 points	4 points	Score

2.3 Change Management

We have little connection or control over changes in external systems, so we mostly react to changing business rules or data definitions about faculty, staff, and students.	We have development, test, and user-acceptance environments, but inconsistent processes for coordinating changes with source systems.	We have standard, cooperative change management processes and use end-to-end test, development, and user-acceptance environments with all sources and consumers.	Our change management processes have auditable approval trails, and are analyzed for continual improvement.	
1 point	2 points	3 points	4 points	Score

2.4 Staffing

We are stretched thin on staffing, especially with respect to Identity Management (IdM).	We have some staffing efforts partly dedicated to IdM, but it is a best effort and often they are pulled away to other projects.	We have staff dedicated to managing and growing our IdM infrastructure.	We have dedicated IdM staff with organizational development efforts to manage IdM positions, skill development, and succession planning.	
1 point	2 points	3 points	4 points	Score

Section Subtotal _____

3. Authentication

3.1 Single Sign On and Authentication

We have separate authentication credentials and methods for access to different institutional services.	We leverage a consistent set of credentials for authentication for access to different institutional services.	We have implemented a standard single sign-on solution for access to different institutional services.	Our single sign-on solution includes multi-factor authentication (MFA), and policies for SSO and MFA are defined based on asset classification and risk.	
1 point	2 points	3 points	4 points	Score

3.2 Credential Provisioning

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 self-service and some are not. We have some policy around who can request an account.	Our processes are established, automated, and documented.	Automated processes are also defined for credential revocation, integrated with security incident response efforts.	
1 point	2 points	3 points	4 points	Score

3.3 Identity Assurance

We use the same userid and password for all our services regardless of business domain or asset classification (finance, email, etc.). Our identity and security teams have little interaction.	We require stronger credentials for some services, but still support questionable practices for accessing some legacy systems. The identity and security teams understand their interdependence.	We have classified our services according to risk levels and implemented analogous credential-related requirements. For legacy systems, we have developed strategies to reduce our exposure. We have a strong relationship between identity and security staff.	We additionally include identity proofing in our identity assurance framework and practices. Our identity and security staff work with the audit community to improve awareness and assessment against standard assurance profiles.	
1 point	2 points	3 points	4 points	Score

Section Subtotal _____

4. Authorization and Access Management

4.1 Separation of Authentication and Authorization

The act of authenticating provides some simple access rights.	In general, we have enabled the separation of authentication from access, but users can still access some services, especially in legacy systems, without explicit granting of it.	We have nearly complete separation of authentication from access rights. We feel comfortable allowing people to authenticate who no longer are members of our campus. Risk is being managed effectively at the service or system level.	We have policies and practices that enforce the separation of authentication from access rights. Exceptions are rare, and service or system owner are responsible for risk management plans.	
1 point	2 points	3 points	4 points	Score

4.2 Group Strategy and Deployment

We currently do not have any "groups" management strategy or system beyond, perhaps, system-specific "roles" as defined by local application security.	We have groups and a model for distributed maintenance of membership, but limited integration with or leveraging of this information across the infrastructure.	We support groups at a high level, integrating institutional roles (e.g., faculty, student) with ad hoc groups, easily leveraged across campus-wide systems.	We manage the full lifecycle and wide integration of roles and ad hoc groups, with a consistent approach to membership privacy (confidentiality and unwanted communication). Memberships can include federated IDs and non-person entities.	
1 point	2 points	3 points	4 points	Score

4.3 Putting Access Right Controls in the Hands of Those Making Decisions

Access rights are generally managed internally by IT through a variety of online methods, including email or help ticket requests.	Departments and users can manage access rights, but across multiple systems in a variety of interfaces. Some is still done by IT as well.	Users have a common interface to manage access rights, for both assigning and review. We support delegated assignment of access rights.	We additionally measure and support reporting and analysis of access rights, to streamline approval processes and to manage institutional risk.	
1 point	2 points	3 points	4 points	Score

4.4 Provisioning and Lifecycle: Business Process

Each new faculty or staff position must be incrementally enabled or disabled for access as needed. This can take days, weeks, or months to get it all set up.	Good processes are in place to identify and to facilitate the many steps in establishing access rights.	Access rights for new individuals can be quickly established based on role or transferred from the last holder of that position. Standard approval workflows support ad hoc access requests.	Access rights for non-person entities are managed by business processes with similar rigor.	
1 point	2 points	3 points	4 points	Score

4.5 Provisioning and Lifecycle: Technology

Access rights need to be granted and revoked manually by the responsible managers or administrators. Too often we rely on one's login being turned off to cut off services.	Basic computing services – login, email, web – are automatically tied to affiliation and status, but richer forms of authorization require manual control or custom integration.	Access rights of all kinds – infrastructure services, business systems authority, resource access – are tied to affiliation and status using standardized means of integration.	Access rights of all kinds are additionally subject to common date and status controls for automated lifecycle management. Selection of new technologies includes evaluation and alignment with provisioning.	
1 point	2 points	3 points	4 points	Score

4.6 Reporting and Audit

We have no good way to determine all the access rights a person has or all the holders of a certain access type; this information is scattered across many systems and accessible only to the maintainers of those systems.	Processes are in place to answer questions about access types and holders of access rights to central offices and auditing.	Access information is available on demand to individuals in offices or departments who are responsible for managing them.	Additionally, access information is proactively analyzed to continually improve processes and to effectively manage institutional risk.	
1 point	2 points	3 poin	4 points	Score

Section Subtotal _____

5. Planning and Governance

5.1 Identity Management Roadmap

Identity Management Roadmap? We don't have one.	An Identity Management roadmap is under development.	An Identity Management roadmap is in place and being actively maintained.	Our roadmap is integrated into and informed by strategic planning processes.	
1 point	2 points	3 points	4 points	Score

5.2 Governance - Who Gets to Say Who Gets to Say?

IT staff may find themselves making decisions where business rules don't exist and no decision-making body exists.	We have general workplace guidelines that designate who can use identity data and stewardship of it.	We have policies around identity data and stewardship as well as chain of authority for group and access management.	Our policies additionally maintain accountability in the methods used by and between systems and other non-person entities for delegated access to identity data on behalf of individuals.	
1 point	2 points	3 points	4 points	Score

Section Subtotal _____

6. Federation Perspectives

6.1 Cloud Strategy

We rarely if ever look to the cloud to provide resources and services to the institution.	Some external applications and resources are of interest to us.	We have standard approaches to leveraging the cloud for central IT, including some awareness of Internet2 NET+ services. However, schools, departments, and other business units are on their own.	We leverage as many cloud resources as fits our technology and business goals, including strategic sourcing of Internet2 NET+ services. Cloud is a key component of our IT strategy to service our institutional mission.	
1 point	2 points	3 points	4 points	Score

6.2 Federating Methodology

We use multiple methods to connect to cloud services such as credential syncing and provider access to our campus LDAP service.	We are members of InCommon, but do not require it of our cloud service providers.	We are members of InCommon and require its use by our cloud providers, with rare exceptions.	We additionally manage our exceptions, ensuring our cloud providers implement federation compatible with InCommon.	
1 point	2 points	3 points	4 points	Score

6.3 Third-party Service Provider Access to Identity and Credential Information

We are comfortable permitting third-party service providers to access both our identity information and credential information used for authentication.	We are comfortable permitting some third-party service providers to access our identity and/or credential information. We allow this for services with a business need and for companies that offer no other options.	We are generally not comfortable releasing credential information, but it happens occasionally. We only release minimal identity information to third-party service providers.	We are very uncomfortable releasing credential information, and monitor known and potential cases, taking action to remediate all cases. We only release minimal identity information, based on a signed data sharing agreement and/or user consent for discretionary cases.	
1 point	2 points	3 points	4 points	Score

6.4 eduPerson

We don't have it or are not sure what it is.	We have partially implemented it with lots of local customizations to the specification.	We have partially implemented it, adhering to the standard, but don't have the data available for some of the attributes.	We have fully implemented and leveraged eduPerson on our campus.	
1 point	2 points	3 points	4 points	Score

6.5 External Collaboration

Faculty collaboration with other institutions and entities beyond our own is rare or non-existent.	There is some ad hoc research and scholarly collaboration, mostly individuals and small teams working with others at other institutions and entities beyond our own.	We enable ad hoc research as well as some large-scale scholarly collaboration with other institutions and entities beyond our own. Some methods of collaboration must be standardized and streamlined.	Collaboration beyond our institution is a key component to our educational and research missions. We enable collaboration at many scales, using a mix of experimental and standardized processes.	
1 point	2 points	3 points	4 points	Score

6.6 Attribute Release

We set up a new attribute release policy upon request and use an ad hoc approval process each time.	We have a process for campus review of requests for attribute release, but decisions aren't always consistent. We support the Research and Scholarship Entity Category.	We release public directory information to all SPs in InCommon. We have a consistent process for campus review of requests for attribute release beyond the public set. We support the Research & Scholarship (R&S) Entity Category.	We leverage and require user consent when attribute release isn't required. We have a holistic process for campus review of requests for attribute release and consent management. We support the Research & Scholarship (R&S) Entity Category.	
1 point	2 points	3 points	4 points	Score

Section Subtotal _____

Final Total _____