# The State of Our Identity and Access Management

### Self-Assessment Questionnaire

# To get a sense of where your workshop cohort falls on the IAM maturity continuum, please work with your campus colleagues to complete this questionnaire.

# Each entry below describes an aspect of identity and access management and provides three choices that roughly equate to maturity level for that function. For each item, choose the answer that best describes what your institution does today. Enter the score associated with your choice in the empty box to the right of each entry, subtotal each section, then compute your final total at the end.

# This questionnaire is based on an identity management assessment tool first developed by Lynn McRae, Stanford University,

# updated by John O’Keefe, Lafayette College and further tailored for the TIER Workshops.

##### Current State of Identity Data Section Subtotal

Coverage

|  |  |  |
| --- | --- | --- |
| Our identity management covers just the core community—faculty, staff and students—as defined by source systems. | Our identity management includes faculty, staff and students, plus secondary sources like library patrons, hospital staff, etc. | We capture information about all people of interest to schools, departments, research collaborators, central offices, libraries, guests, etc. |
| 1 point | 2 points | 3 points | |  |  |

Matching and Uniqueness

|  |  |  |
| --- | --- | --- |
| We get information from many sources; it’s possible someone can be represented multiple times. It is difficult for us to detect except in reaction to service issues. | We have good central identity matching processes, but work to resolve identity issues mostly as needed. | We have strong partners and practices across campus and multiple systems that participate in detecting, avoiding and resolving identity issues. |
| 1 point | 2 points | 3 points | |  |  |

How Fresh Is Your Data?

|  |  |  |  |
| --- | --- | --- | --- |
| 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 and client systems that allow service and access changes to take effect in minutes -- on or off -- when data changes. | |
| 1 point | 2 points | 3 points |  | |  |

##### Current State of Identity Infrastructure Section Subtotal

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, as well as an enterprise, message-based integration infrastructure. | |
| 1 point | 2 points | 3 points |  | |  |

Identifiers

|  |  |  |  |
| --- | --- | --- | --- |
| We reuse our identifiers. | We support reused but persistent identifiers in our infrastructure. | We support non-reassignable persistent identifiers in our infrastructure. | |
| 1 point | 2 points | 3 points |  | |  |

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 source system involvement, and problems with authentication/SSO. | We have end-to-end test, development, and user-acceptance environments with all sources and consumers, and cooperative processes for planning change. |
| 1 point | 2 points | 3 points | |  |  |

Staffing

|  |  |  |
| --- | --- | --- |
| We are stretched thin on staffing, especially with respect to Identity Management | We have some staffing efforts partly dedicated to IdM, but it is a best-effort and often these staff are pulled away to other projects. | We have staff dedicated to managing and growing our IdM infrastructure. |
| 1 point | 2 points | Advanced (3) | |  |  |

##### Authentication Section Subtotal

Single Sign On and Authentication

|  |  |  |
| --- | --- | --- |
| We have separate authentication credentials for access to different institutional services. | We leverage unified authentication for access to different institutional services. | We have implemented a single sign-on solution for access to different institutional services. |
| 1 point | 2 points | 3 points | |  |  |

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. |
| 1 point | 2 points | 3 points | |  |  |

Identity Assurance

|  |  |  |
| --- | --- | --- |
| We use the same userid and password for all our services from financial system access to email. Our identity and security groups have little interaction. | We require stronger credentials for some services, but still support questionable practices for accessing some legacy systems. The identity and security groups 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. |
| 1 point | 2 points | 3 points | |  |  |

##### Authorization and Access Management Section Subtotal

Separation of Authentication and Authorization

|  |  |  |
| --- | --- | --- |
| The act of authenticating provides some simple access rights. | In general, we have separated authentication from access, but users can still access services, especially in certain systems, without explicit granting of it. | We have complete separation of authentication from access rights. We feel comfortable allowing people to authenticate who no longer are members of our campus. They can’t access any resource. |
| 1 point | 2 points | 3 points | |  |  |

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. |
| 1 point | 2 points | 3 points | |  |  |

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. |
| 1 point | 2 points | 3 points | |  |  |

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. |
| 1 point | 2 points | 3 points | |  |  |

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 other forms of authorization require manual control. | Access rights of all kinds – infrastructure services, business systems authority, resource access – are subject to common date and status controls for automated life-cycle management. |
| 1 point | 2 points | 3 points | |  |  |

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. |
| 1 point | 2 points | 3 points | |  |  |

##### Planning and Governance Section Subtotal

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. |
| 1 point | 2 points | 3 points | |  |  |

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. |
| 1 point | 2 points | 3 points | |  |  |

##### Federation Perspectives Section Subtotal

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. | Leveraging as many cloud resources as fits our technology and business goals is a key component of our IT strategy to service the institutional mission. |
| 1 point | 2 points | 3 points | |  |  |

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. |
| 1 point | 2 points | 3 points | |  |  |

Cloud Provider Access to Identity and Credential Information

|  |  |  |  |
| --- | --- | --- | --- |
| We are comfortable permitting corporate service providers to access BOTH our identity information AND authentication information. | We are comfortable permitting some corporate service providers to access our identity and/or authentication information. We allow this for services that are really important to our stakeholders and the company is being difficult. | We are not comfortable releasing any authentication information and only releasing minimal identity information to external corporate partners. | |
| 1 point | 2 points | 3 points |  | |  |

eduPerson

|  |  |  |
| --- | --- | --- |
| We don’t have it or are not sure what it is. | We have partially implemented it, but don’t have the data available for most of the attributes types. | We have fully implemented and leveraged eduPerson on our campus. |
| 1 point | 2 points | 3 points | |  |  |

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 with institutions and entities beyond or own. | Collaboration beyond our institution is a key component to our educational and research missions. |
| 1 point | 2 points | 3 points | |  |  |

Attribute Release

|  |  |  |
| --- | --- | --- |
| We set up a new attribute release policy upon request and have an ad hoc process for doing this | We have a process for campus review of Attribute Release Requests. We support the Research and Scholarship Category Tag. | We release public directory information to all SPs in InCommon. We have a process for campus review of Attribute Release Requests for information beyond the public set. We support the Research and Scholarship Category Tag. |
| 1 point | 2 points | Advanced (3) | |  |  |

**Final Total**