Terminology - Glossary

Access Management (AM)	Part of Identity and Access Management, it deals specifically with how users (identities) are authorized to access resources, frequently through the use of groups, roles and entitlements that are established through policies. Privilege Management is a related area and tends to be more granular in nature.
Affiliation	Describes an individual's *relationship* with an institution. Slightly different than *role*, which describes the job function performed or responsibilities of the job, rather than the relationship.
Authentication	The "act" of proving you are the owner of an identity (e.g. username, credential, account, etc.), usually consists of providing a password or other factor (token, PIN, digital certificate, fingerprint scan, etc.)
Cloud	Cloud services or applications are those that are not run locally, but are hosted at a vendor location and accessed through the internet.
eduPerson	eduPerson is an LDAP schema designed to include widely-used person attributes in higher education. It was developed, and is maintained, by the Internet2 MACE-Directories Working Group (MACE-dir), a project of the Internet2 Middleware Initiative. The eduPerson object class provides a common list of attributes and definitions. Attributes are used to communicate information about an individual accessing an online resource.
Federated Identity Management(FIM)	The management and use of identity information between members of a federation.
Federation	A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.
Identity	A unique, electronic representation of a physical person (usually) used to interact with online resources.
Identity Data	Attributes about an individual that uniquely identify them. Usually consists of bio-demo data such as Name, Address, Phone number, email, Employee/Student Number, DOB, etc.
Identity Management (I dM)	Identity management refers to the policies, processes, and technologies that establish (provision) user identities and enforce rules about access to digital resources.
Identity and Access Management (IAM)	Identity and Access Management is the current discipline, which combines the creation and management of Identities and how they are enabled to access resources. Formerly referred to as Identity Management (IdM), it was expanded to include Access Management in the last few years.
Provisioning	The act of creating an electronic identity or record for a user. May also refer to the creation of accounts or the *provisioning* of services (access to applications).
Role-Based Access Control, Group-Based Access Control(RBAC & GBAC)	Provisioning access (to resources) for a user based on what roles they have (e.g. teacher, guidance counselor, student, etc.), or based on their membership in a group of like individuals (e.g. All fifth graders, Data Coordinators, Coaches, principals, etc.)
Shibboleth	Shibboleth is an open-source software that allows sites to make informed authorization decisions for individual access to protected online resources in a privacy-preserving manner. The Shibboleth software implements widely used federated identity standards, principally OASIS' Security Assertion Markup Language (SAML), to provide a federated single sign-on and attribute exchange framework.
Single Sign-On (SSO)	The act of a user logging in *once* to gain access to multiple applications, services, etc., without being prompted to log in again at each of them.
Source Systems	The authoritative Systems of Record (SoR) that are the source of identity data in an Identity and Access Management system.
Target Systems	The applications, services, resources, etc. that users access with their accounts/credentials. Service accounts may be provisioned directly into the target system via a vendor's API (e.g. Google Apps), or target systems may be enabled to use federated access via a SAML assertion (e.g. Shibboleth).