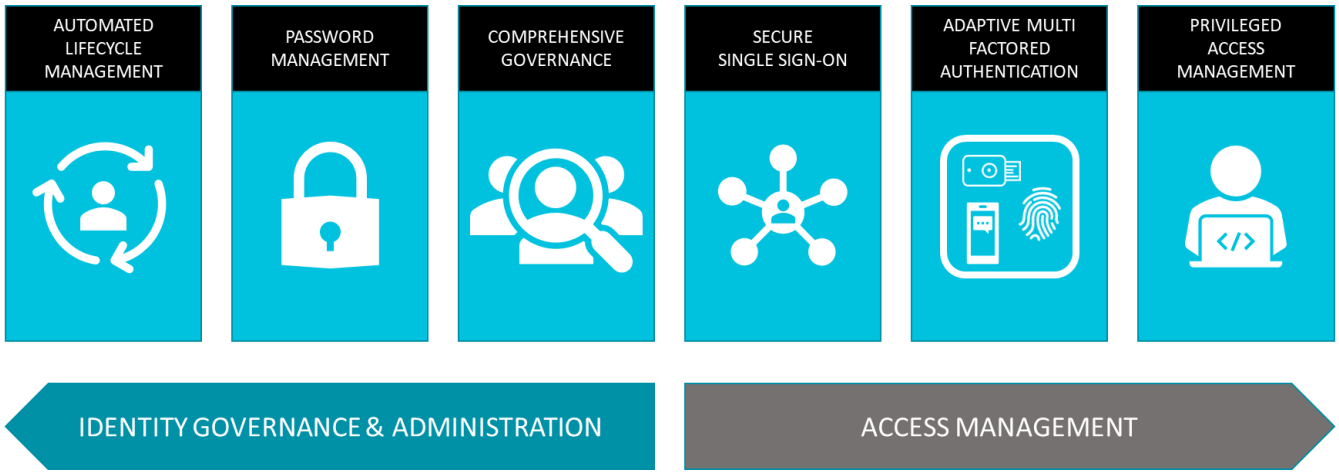
IAM CHECKLIST FOR HIGHER EDUCATION

CONCENSUS TECHNOLOGIES

TABLE OF CONTENTS

IAM PROGRAM FOR HIGHER EDUCATION INTRODUCTION

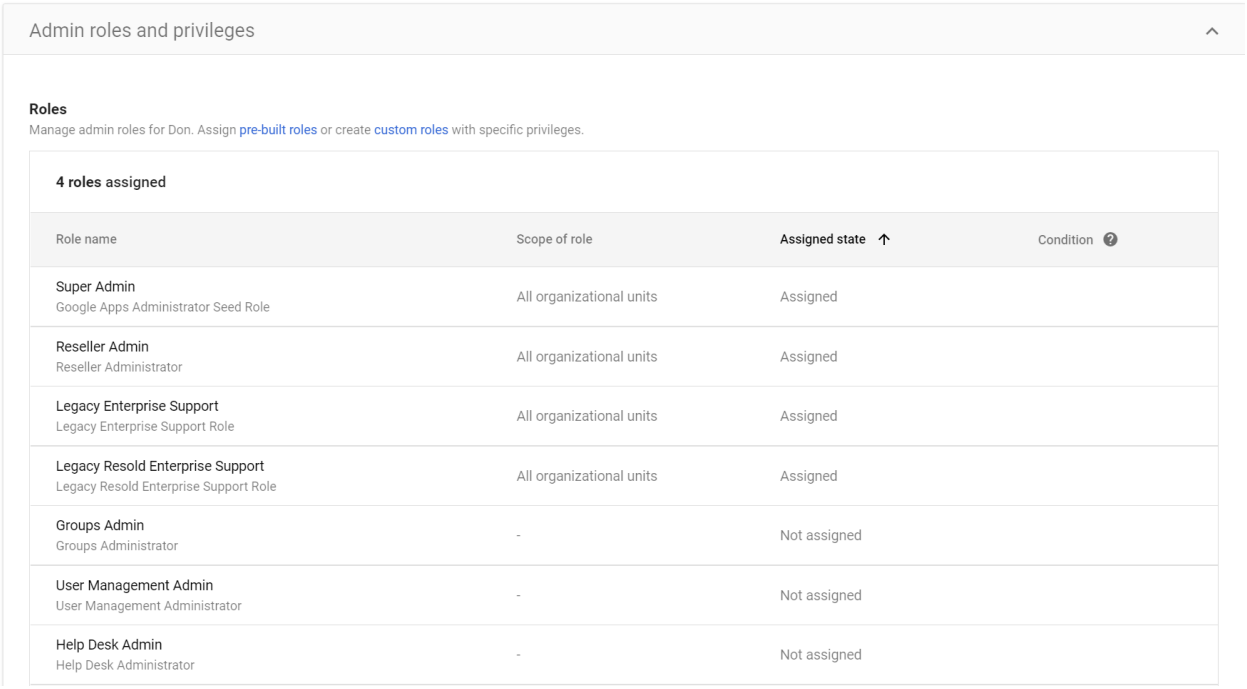
A modern Identity and Access Management (IAM) program can be summed up in the following graphic.



For higher education institutions, IAM is the foundation of implementing a zero-trust network. Students, faculty, and staff must have the right level of access to the correct resources with as little friction as possible. The following checklist shows the core components necessary for higher ed.

ROLES

Roles are used in many IAM software for Roles Based Access Controls. Roles are assigned different permissions and application access. If you have logged into Google Workplace you will see many different roles available in the admin roles and privileges.



For many, this seems to be a simple decision. An individual is exclusively faculty, staff, or student. However, the reality of higher education is that affiliated persons may be in one or more of these roles, perhaps even in additional roles not yet defined in the simple model. An institution may have a need for roles for research faculty, adjunct faculty, graduate or undergraduate student, and many others. A role system for managing account access and permissions will need to have flexibility to address the needs of many higher education institutions. Assigning people to the appropriate roles can be done manually, an often time consuming and error prone process. Alternatively, enterprise IaM software can help mine roles from different applications such as human resources and student information systems.

This checklist is dedicated to the main features necessary for a higher education environment.

	AUTOMATED USER LIFECYCLE MANAGEMENT
	PASSWORD MANAGEMENT
	ROSTERING
	LM Integration
	SINGLE SIGN-ON
	MULTI-FACTOR AUTHENTICATION
	PRIVILEGED ACCESS MANAGEMENT

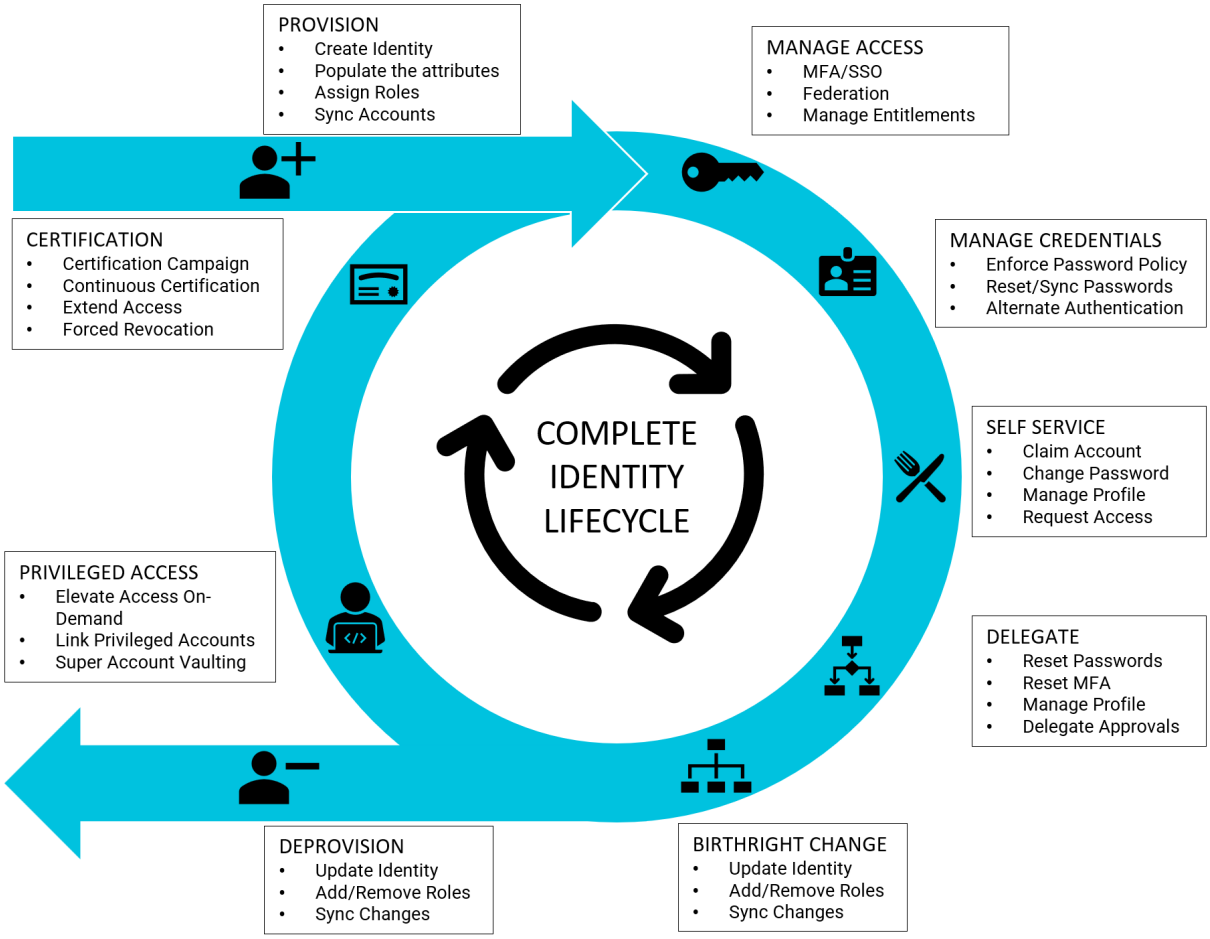
IDENTITY MANAGEMENT AND GOVERNANCE

Identity management, also known as identity and access management, is a framework of policies and technologies to ensure that the right users have the appropriate access to technology resources. IaM systems fall under the overarching umbrellas of IT security and data management.

This section is dedicated to the main features necessary for a higher education environment.

AUTOMATED LIFECYCLE MANAGEMENT

This is the process of managing your student and staff accounts access to applications on premise or in the cloud. The following graphic sums up the automated lifecycle of a faculty, staff, student, or other associated person with the institution.



This is the automation of a zero-trust network. Automated Lifecycle Management (ALM) integrates with your human resources and student information systems so you can automatically provision, manage access and ultimately de-provision any digital accounts within the internal network or within the cloud.

Features that are specific to look for that add to the value of ALM are:

- Account Sponsorship – Great for Contractor and temporary accounts
- Account Claiming – Sponsors and faculty facilitators
- Workflows – Delegation of Approvals

This should not be confused with Single Sign-On's just in time provisioning features, as they do not manage anything other than initial account creation and authorization (i.e. logins). They do not manage items like licensing, birthright changes or complete de-provisioning.

Products that fit this role:

- Rapid Identity by Identity Automation – www.identityautomation.com
- Okta Workforce Identity – https://www.okta.com/products/lifecycle-management/
- Micro Focus Identity Manager – https://www.microfocus.com/en-us/cyberres/identity-access-management/identity-manager

Our end users benefit from self-service as part of their experience with ALM but the account creation, updates and removal of accounts is a security and back of the office benefit. The time benefits and automation are great and necessary due to the increased applications being deployed every year and the high turnover rate of user accounts every year.

This sometimes makes it difficult to get funding for this feature as there is typically a lack of end user interaction with these features.

PASSWORD MANAGEMENT

Password management can be broken down into several categories but for the purposes of this document we will discuss password management in terms of how it fits into Identity Management and Self-Service. Other forms of password management include password managers like LastPass that can store passwords and perform form fill for applications that are not enabled with Single Sign-On.

Most institutions have a password change policy (often one for faculty/staff and one for students). Many institutions may have several policies for different roles and subsets of roles. Centrally managing password management is a difficult task but can be accomplished with ALM and SSO.

Most IAM platforms come with a self-service portal where end users can:

- Change their password
- Set challenge response questions
- Modify their profile – Add cell phone number and/or configure multi-factor authentication
- Perform a workflow request – (request to be added to a group or even request a device)
- Sponsor an account
- Perform basic helpdesk requests

When combined with an ALM platform, passwords can be synchronized to supported systems securely so that they may operate independently without an SSO solution. This is very useful if there are multiple active directory domains that do not have a trust relationship or to systems or databases that do not support a web based single sign-on solution.

LMS INTEGRATION

Increasingly, higher education has embraced various Learning Management Systems to enhance the experience of both faculty and students. These systems, which leverage student, instructor, and course enrollment data, benefit greatly from integration with an enterprise IaM solution.

IaM can connect identity and account data, provisioning person account data into the LMS in a role-focused manner. This can allow the LMS solution to accommodate users in many capacities, instructor, instructional assistant (Graduate TA/GA roles), adjunct faculty, and students, in many combinations, at the same time. All driven from institutional data and policies.

Student Information Systems (SIS) and registrar data can be used to drive course enrollment status into the LMS. In many cases, these integrations can significantly ease the workload of term enrollment and drop/add course changes at the start of each term.

Accurate, up to date student, instructor, and course enrollment data, when integrated into a campus LMS system, can bring high visibility, significant value to the end users of your systems and further the goals of an instructional higher education institution. This end user value brings with it additional savings in reduced workload on IT and instructional staff.

GOVERNANCE

During the rise of governance regulations (going back to HIPAA, Sarbanes-Oxley Act, FERPA, and even PCI) the rise of identity management systems began to grow. Then when the digital landscape started to change and the rapid introduction of cloud and software-as-a-service (SaaS) took hold and user identities were now inside and now outside of an organization. The result was a tangled mess of access for staff, students, consumers, partners across multiple environments.

New solutions had to be developed (as people were going back to spreadsheets of user accounts to review user access for review and approval. On top of that costs for SaaS applications were beginning to rise.

This is where identity management and identity governance merged into Identity Governance and Administration. Today, IGA helps organizations be compliant through certifying the appropriate level of users' access and providing the access to the right resources at the right time. Policy-based controls now allow organizations to govern user access.

Higher education institutions are now managing distance learning, partnering with organizations that provide cyber-schooling and now must balance that access with regulations such as FERPA compliance.

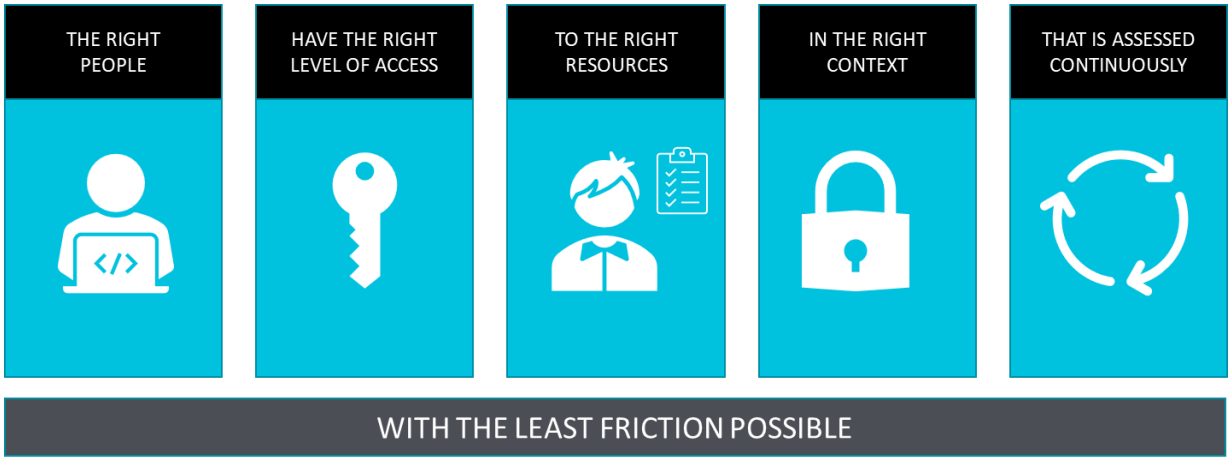
This means not only managing access from a user perspective but when allowing third parties API access to student or staff information this access must be monitored.

Continuously monitoring access requires ensuring that no identities maintain excess access. IT departments must also terminate access in a timely manner to mitigate risks arising from orphaned accounts and excess access.

While not necessarily a part of identity management, Data Access Governance (usually part of IGA software solutions) can enable schools to identify, risk/rate and categorize their data (for PII) to enforce least privilege. One of the most coveted things a cyber criminal wants is PII data.

ACCESS MANAGEMENT

The Right People Have the right level of access to the right resources in the right context that is assessed continuously.



SINGLE SIGN-ON

Single Sign-On for higher education has taken off since Google introduced Google G-Suite for education. The explosion of applications available to educational institutions has required the integration of our directories and many different identity providers over the years. Many applications focused on education customers have integrated with Security Assertion Markup Language (SAML) to provide SSO. There are other important protocols to consider including OAuth, Central Authentication Service (CAS) and Shibboleth. Mainstream providers of SSO will include these protocols within their stack.

The components of a SSO Solution are:

- Directory – Usually AD or other LDAP compliant directory
- Identity Provider – performs the authentication request and verifies identities
- Access Gateway – Access Gateways are a component of a SSO solution and can provide proxy access to gated systems
- Secure Portal

Higher-Ed in particular need to look at authentication from a broader lens due to the diversity of persons seeking access to institutional resources and the different type systems in use (Chromebooks, windows devices, iPads etc.). Universal Authentication has become necessary to deal with the unique persona-based needs of faculty, staff, students, and other affiliated people. This will be discussed more in the Multi-Factor authentication section as the two go hand in hand.

There are many vendors that support SSO but do not provide an identity provider. Some of the ones we have worked with:

- Rapid Identity by Identity Automation – www.identityautomation.com
- Okta Workforce Identity – https://www.okta.com/products/single-sign-on/
- Micro Focus Access Manager - https://www.microfocus.com/en-us/cyberres/identity-access-management/access-manager
- Onelogin - https://www.onelogin.com/product/sso
- Google Workplace for Education
- Microsoft Azure AD (Part of Azure AD premium P1 and P2)

MULTI-FACTOR AUTHENTICATION

Multi-Factor Authentication (MFA) has been on the "hot" list for Higher-Ed for some time. Driven by cybersecurity insurance and driven by breaches in general this element of Access Management is now one of the most critical for our schools.

There are many challenges to overcome with MFA in Higher-Ed. First and foremost, who needs it? As mentioned earlier in this book there is a real need for MFA and SSO to support persona-based access. This means that your users' needs will naturally change during their time with the institution, changes in major or field of study, employment status, affiliated institutions and collaborative partnerships. MFA, while secure, is usually perceived as a burden to teachers and staff. Most MFA services require you to first register a "thing" (method). This can be a device, an application on a smartphone, an sms message, or even just a PIN code. Not only that, but they want you to do this organization wide.

This introduces the real struggle for adoption in Higher-Ed. Remote students, students over traditional age, research faculty, adjunct and guest faculty, temporary workers, high school student programs, and many others, present a variety of barriers to enroll devices and methods to support MFA.

MFA can be achieved through integration with your Identity Management system and a robust MFA platform. By using Identity-Driven policy enforcement you will enable flexible (and automated) authentication across all your users, applications, and devices.

There are a lot of features that come with MFA software that can make your district more secure. They include:

- Location Based MFA – Utilizes their GEO location
- Risk Based Authentication (adaptive authentication) - These systems ask not only where you are trying to authenticate but what device? What are you trying to gain access to? What type of network are you on?

We have worked with systems from:

- Identity Automation
- Micro Focus
- Microsoft
- Google
- Duo (Cisco)
- OneLogin
- Okta

Balancing security with your educators' needs for simplicity and speed are the key to implementing MFA.

PRIVILEGED ACCESS MANAGEMENT

In cybersecurity the most dangerous accounts are your administrative accounts. Once these accounts are compromised, access for attackers is difficult to stop. Privileged Access Management (PAM) started out as who is watching our admins and what are they accessing?

Today PAM is defined as strategies and technologies for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment.

By gaining control of all privileged accounts (local admin, domain admin, service, and application accounts) you can start to implement least privileged access.

Within the IAM framework PAM can be enabled via workflows where someone requests temporary access to a system, it is approved and granted. This is usually connected directly to the ALM system to ensure that access is elevated properly and removed once complete.

PAM components include:

- Shared access password management
- Privileged Session Management
- Vendor Privileged Access Management
- Application Access Management

PAM can be enabled for on-premises applications and systems as well as for SaaS based applications.

We have worked with systems from:

- Identity Automation
- Micro Focus
- Microsoft
- Google
- Beyond Trust
- OneLogin
- Okta

One other area of Privileged access management that is important to higher education is Endpoint Privilege Management. This can help you eliminate unnecessary privileges on your endpoints (Windows, Mac, Linux systems for instance).

SUMMARY

Many higher educational institutions have pieces of an IaM program but do not have a fully working or integrated system. The question is always where do we start? The journey to an IaM program is not accomplished in one year for most organizations. Higher educational institutions have different needs than corporations and even K-12 school districts.

This checklist was just the beginning of understanding where you are in your program lifecycle. You may be strong in certain areas and need guidance in other areas.

Developing your strategy starts with:

- Current state assessment
- Identifying your future state and vision based upon your needs
- Prioritization and budgeting of those needs
- Creating an actionable roadmap

Concensus has been working with higher education across the country for over 20 years. We help you by providing the right people, the right processes, and the right technology to succeed.

Contact us today to see how you can get started with an Identity and Access Management Assessment.