IAM CHECKLIST FOR K-12 DISTRICTS

CONCENSUS TECHNOLOGIES

TABLE OF CONTENTS

ABOUT CONCENSUS TECHNOLOGIES

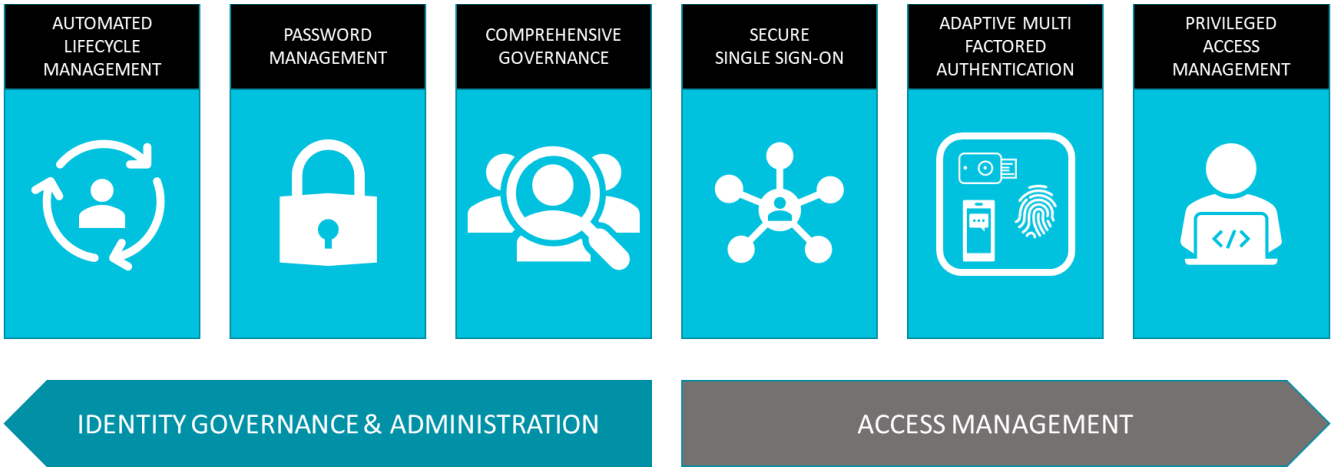
With 20 years of experience, Concensus Technologies provides educational clients with the protection they need for their sensitive data. Their comprehensive solutions let organizations access a variety of features and control protocols that make it easier for IT professionals to monitor and defend against malicious activities.

Our cutting-edge technology ensures that your organization is always ahead of the curve when it comes to security threats, providing you with peace of mind knowing your system is always appropriately defended from cyber-attacks. With unbeatable customer service and up-to-date security solutions, Concensus Technologies is the perfect choice for educational clients looking to ensure their data remains safe and secure.

Concensus is everything you need us to be, but we're at our best when you see us as your trusted partner in identifying and implementing top-notch solutions to your top business, security, and IT challenges.

IAM CHECKLIST FOR K-12 SCHOOLS INTRODUCTION

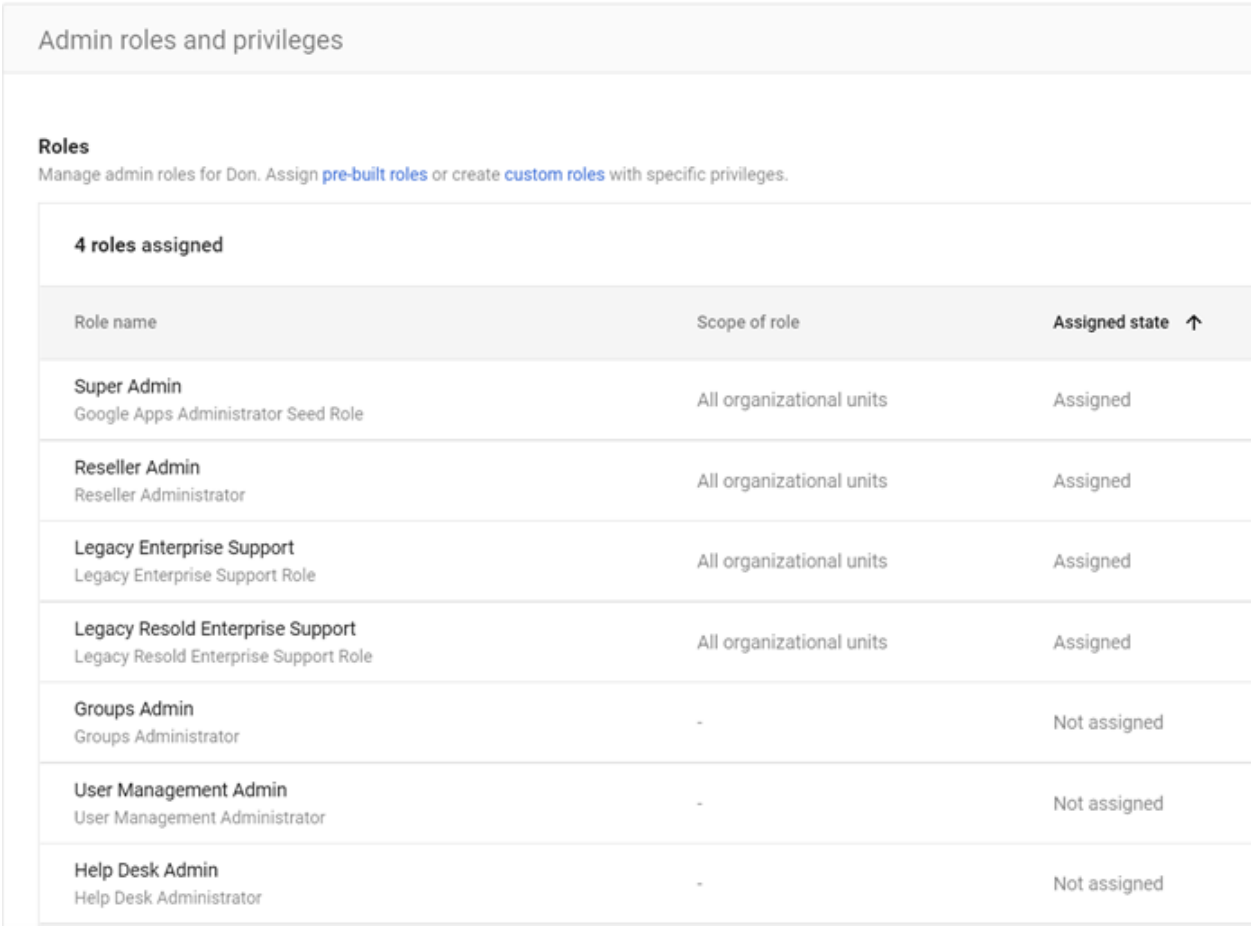
A modern Identity and Access Management (IAM) program can be summed up in the following graphic.



For K-12 districts IAM is the foundation of implementing a zero-trust network. Students 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 K-12 districts.

ROLES

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



In many schools this is a very simple process. You are either staff, teacher, or student. In large districts with many employee's role definitions in the HR system will need to be mapped to technical roles. This can be accomplished manually by using a top down (or a top up approach) or IaM software can be used to help mine roles from different applications. This is an enterprise level feature that most districts can get by with basic roles.

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. IdM systems fall under the overarching umbrellas of IT security and data management.

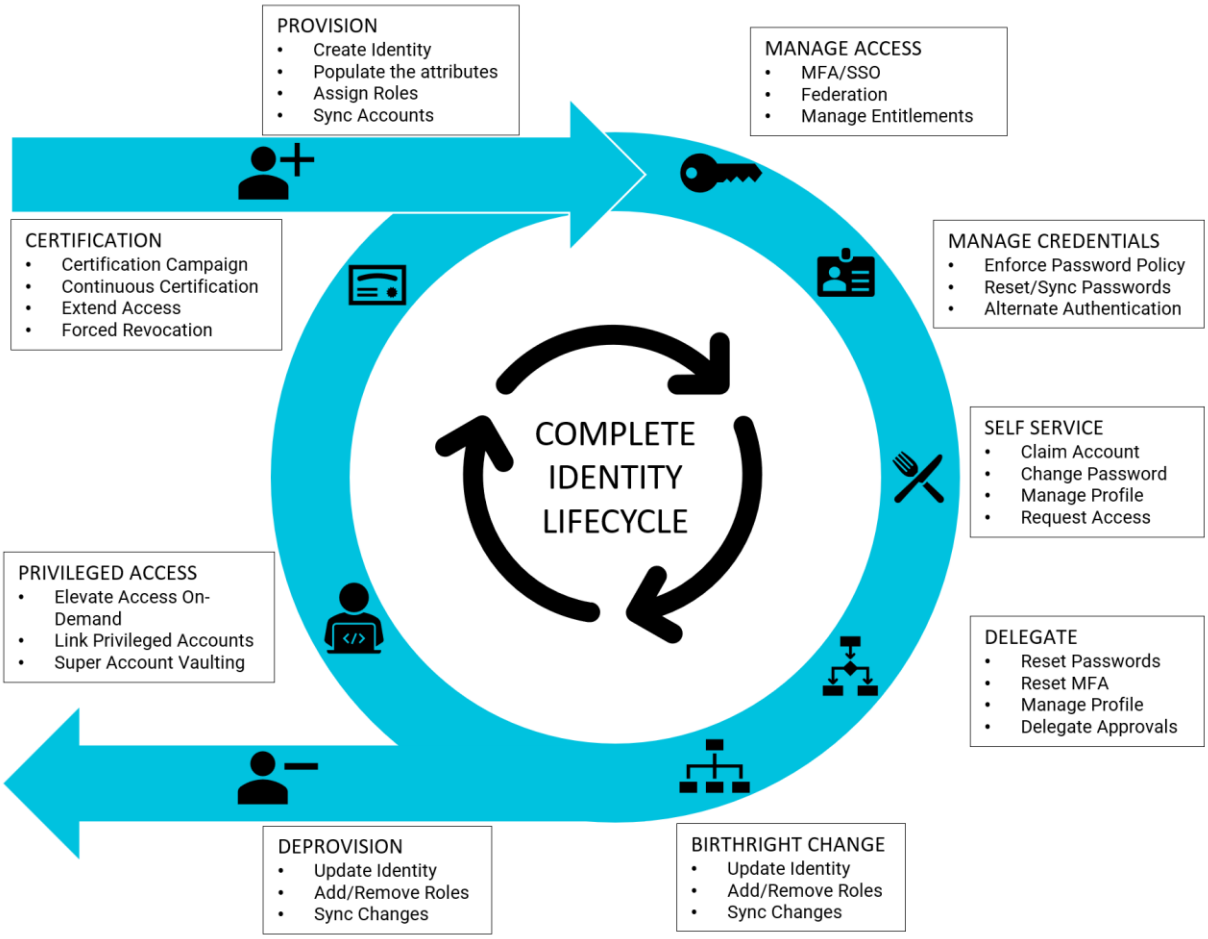
This checklist is dedicated to the main features necessary for a K-12 environment.

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

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 student, staff member, or even contractor.



This is the automation of a zero-trust network. Automated Lifecycle Management (ALM) integrates with your student information system and HR system 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 Substitutes
- Account Claiming – For parents and guardians
- 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 students and staff 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 schools have a password change policy (one for staff and one for students). Even students may have multiple password rules and change policy. 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 cannot support a web based single sign-on solution.

ROSTERING

Rostering is at the core of curriculum and not only does a learning management platform need this information but also many applications need this important information.

Enabling automated rostering will not only accelerate digital learning within the district but also can keep third parties up to date with the latest classroom information throughout the year. This will ensure that students and educators have the right access to digital textbooks and resources they need.

Another benefit of automated rostering will help eliminate the sprawl of PII by providing a granular level of control.

This works by implementing software that consumes course information either in real-time (via a trigger or webhook) or on a scheduled query to your student information system (SIS). Then the data is evaluated, transformed, and filtered into formats required by your third-party target systems.

It is important that rostering data be synchronized in lock step with your user ALM. Many applications require a user account to be present prior to rostering assignments. ALM manages the login while rostering provides the correct access to classroom resources within an application.

Many applications support OneRoster (https:// www.imsglobal.org/activity/onerosterlis). This standard helps schools securely and reliably exchange roster information, course material and grades between connected systems.

Concensus has worked with several vendors who provide these types of rostering capabilities.

- Clever – https://clever.com/products/rostering
- Identity Automation - https://www.identityautomation.com/iam-platform/rapididentityidentity-access-management/rostering-for-k12/

GOVERNANCE

Identity management systems have evolved and multiplied to address the rise of governance regulations (going back to HIPAA, Sarbanes-Oxley Act, and even PCI). The digital landscape was further complicated by the rapid introduction of cloud and software-as-a-service (SaaS). User identities moved from the relative safety of inside the walls of the organization to anywhere in the world.

The result of these shifts is a tangled mess of access for staff, students, consumers, and 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.

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

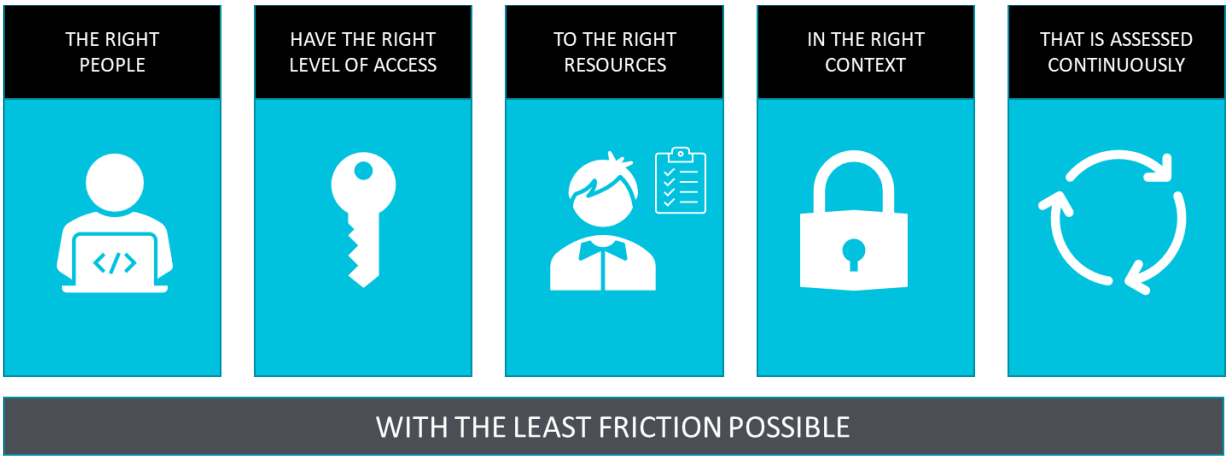
K-12's are now managing distance learning, partnering with organizations that provide cyber-schooling, and now must balance that access with regulations like FERPA. This means not only managing access from a user perspective but monitoring third-party API access to student or staff information.

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. This is of enormous importance, not only for regulatory compliance but for simple due diligence: PII data is a prime target of cybercriminals.

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 K-12's has taken off since Google introduced Google G-Suite for education. The explosion of applications available to classrooms 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

K-12's in particular need to look at authentication from a broader lens due to the age differences 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 students, teachers, and staff. 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 K-12 the last few years. 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 K-12. 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 students will naturally change personas based upon age/grade. 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 K-12. Kindergarten students are not going to be able to use the same methods that seniors or even teachers utilize. Also the types of devices will change year to year or grade to grade.

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? and 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 especially important to schools is Endpoint Privilege Management. This can help you eliminate unnecessary privileges on your endpoints (Windows, Mac, Linux systems for instance.)

SUMMARY

Many districts 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 (including k12 and higher education). K12s' have different needs than corporations and even other academic systems.

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 K-12's 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.