Regulatory reform & security continue to play critical roles in education as K-12 School Districts discover new ways to integrate technology in their departments. Modern School Districts have taken advantage of the Information Technology (IT) explosion, and have deployed a large number of systems to support school administrators, teachers, parents, and students. While access to these new sophisticated systems have resulted in increased productivity, Access Management for districts has become an unmanageable problem in education.

The challenge in identifying how to streamline users’ access to disparate resourcing systems & applications is testing academic IT professionals in areas of Security, Operational Efficiency, Cloud Service and Regulatory Compliance. Although these challenges aren’t entirely new to education, improved recognition of Identity Management (IdM) is one of the fastest growing trends in helping to address them. Having a common set of policies, practices, and protocols to manage the identity of users is imperative in today’s K-12 School Districts for the following reasons:

- Security
- Cloud Services
- Operational Efficiency
- Regulatory Compliance
SECURITY
As education institutions continuously embrace the Internet for on-line learning, student services, administrative systems, and self-services security becomes a high-risk indicator. Identification plays a significant role in controlling security and streamlining methods to address threats to student information systems & applications.

CLOUD SERVICES
There’s a lot of examination today in how the cloud can impact K-12; a natural progression to enterprise services, like Google Applications or Office 365, has been mounting. Without appropriate solution roadmaps this cost-saving effort quickly turns into an expensive development effort integrating systems and managing users.

OPERATIONAL EFFICIENCY
Account management for all users within a school district (e.g. login names, passwords, etc.) is becoming increasingly complex. Individual accounts must be created at the beginning of each school year, security and permission levels are constantly changing and the frequency of account maintenance during the year continues to increase. On average, 40% of educators change roles on an annual basis leading to increased maintenance & compliancy risks.

REGULATORY COMPLIANCE (E.G., HIPPA, FERPA, GLD ACT)
Federal law protects the privacy of student education records while requiring access to increased amounts of data reported to the general public on America’s students and their schools and school districts. This creates challenges for IT in identifying practices that protect information about individual students, while at the same time minimizing the negative impact on the utility of reported data. Thus, creating a goal to maximize the amount of information that can be released while protecting personally identifiable student information through a relatively straightforward set of policies that can be easily implemented…and we can help.

“As our District’s technology needs grow, we need our limited technical staff to focus on innovation in our learning environment instead of the repetitive, tedious and mundane tasks of managing user accounts.”
– Dwight Humphrey, Executive Director of IT at DCSD
THE PROBLEM

What happens when thousands of users are changing every year?

This question might be one your department is facing; it was for Jenny McGurk from Douglas County School District (DCSD) in Castle Rock, Colorado. DCSD is like most medium-sized school districts throughout the United States. The District experienced a rapid increase in numbers of students (over 61,000), employees (over 6,000), and parents (around 60,000 households) in Douglas County School District over the last decade. With frequent movement, addition, and termination of employees and students at schools and other sites, it became increasingly difficult to administer access to over 25 major enterprise applications run by the District.

Growth and the introduction of cloud-based Learning Management System (LMS) initiatives caused clear tactical challenges that the district was forced to address. Compounding issues; the proliferation of manual processes for on-boarding and access control, integration issues and other tactical challenges lead to consequential challenges:

- System Access Retained after Role/Department Change
- High Help-Desk Cost
- Sensitive Employee or Student Data at Risk
- Incorrect Access Level Assignment

A centralized, scalable and automated solution was a must. A few years ago Oracle® and Arisant partnered to deliver one of the first Identity Management solutions in Education saving approximately $1M in IT and other Departments personnel’s time.
THE SOLUTION

The DCSD Identity Management System consists of two main components. One automatically provisions (or generates and activates) user accounts and synchronize passwords across District-managed applications. User accounts are generated in various district applications based on position that the employee occupies or the grade and school that the student is enrolled in.

Rules have been automated so that accounts can be activated as soon as the employee begins work.

The second component validates user login attempts and provides Single Sign-On capability for a subset of those applications. It essentially asks the question “Who are you?” and then determines what the user should be allowed to access.

THE RESULTS

IdM was a part of the technological foundation that enabled security for a collaborative online environment and scalability for the unpredictable growth of tomorrow. Because the system is able to uniquely identify a user, the district is now in a position to provide user, school & department-specific web content and collaboration tools…and save time doing it.

Savings over the initial 5 years are calculated at roughly $5 Million; the first 18 months included provisioning time and assumed only 50% of DSDC’s 20 applications would be integrated the first year. The ROI calculations (Figure 1) are comprised of actual salaries of programmers, system administrators, and teachers that are administrating all access. Cost per year over the initial 5 years included licensing, consulting, and annual support costs.

Having a common set of policies, practices, and protocols in place to manage the identity of users allowed the DCSD IT Department to keep pace with District growth, provide better service, and significantly reduce the cost of administration.
Oracle® Identity Management

Oracle® Identity Management enables K-12 School Districts to efficiently comply with regulatory requirements, secure critical applications and sensitive data, and lower operational costs. Oracle® Identity Management helps address these pressures by:

- Centralizing application access control.
- Providing strong, multi-factor authentication.
- Providing sophisticated real-time risk analysis and access prevention based on events and rules.
- Automating routine account management activities.
- Meeting regulatory requirements for reporting and verification.
- Enabling new modes of inter-campus communications.
- Protecting user identity data with a secure, scalable and highly available infrastructure.
- Bridging islands of user identity information across a variety of infrastructures.

“The Colorado Department of Education (CDE) has experienced rapid application growth, especially as online systems continue to mature and develop. Arisant consulting services and the Oracle Identity Management product suite have become our primary drivers for enabling CDE in delivering secure information services to our school districts. We’re helping school districts by enabling them to help themselves.”

– Chris Edmundson, Information Security Officer at the Colorado Department of Education
The Oracle® Identity Management Suite, a fully automated, standards-based, and integrated software solution, can address all major Identity and Provisioning challenges in a cost-effective manner.

**ORACLE® IDENTITY MANAGER (OIM)**

OIM is a rules and workflow driven provisioning engine that integrates with enterprise directory services like Microsoft® Active Directory and third party software applications such as Microsoft® Exchange, PeopleSoft® and Infinite Campus. OIM offers automated provisioning as well as history and audit compliance reporting.

**ORACLE® ACCESS MANAGER (OAM)**

OAM provides user authorization and Single Sign-On (SSO) functionality. Meaning, once the user has logged in through OAM, there is no further authentication needed to access other applications. OAM maintains access and security policies relating to access control.

**ORACLE® VIRTUAL DIRECTORY (OVD)**

OVD combines information from multiple directories and presents a single view of a user’s identity. This unified view simplifies application access control and provides a platform on which a comprehensive white pages search function can be built.

**ORACLE® ENTERPRISE SINGLE SIGN-ON (eSSO)**

eSSO provides sign-on access across enterprise resources. It extends SSO on the Microsoft® Windows desktop, where primary authentication occurs through the Microsoft® logon for third-party software such as VPN applications and external portals. eSSO integrates with OIM for automated provisioning. It also integrates with existing IT and authentication infrastructures.
Conclusion

Arisant is enabling a shift in Education to promote a comprehensive approach to “identity management”. By taking a holistic approach by which identity attributes are abstracted and standardized for seamless and secure exchange throughout the online environment, School Districts are able to promote more efficient academic policy. The following chart shows the challenges, capabilities, and the value of IdM for student lifecycle management:

Arisant’s Identity Management offers solutions that educational institutions need to address the unique challenges they face with an integrated, standards-based and open set of Oracle® products that fit into existing infrastructures. The results equals less time spent integrating disparate components, the backing of the world’s largest enterprise software company, and the proven experience of a true partner.

We encourage you to contact us today for a free consultation or visit our website at www.arisant.com for more information.