Developing an Identity and Access Management System for

North Carolina Education Cloud

A Race To The Top Initiative

Friday, August 26, 2011
Version 2.0
Prepared by:

Sammie Carter, Phil Emer, Lee Sartain, James Robinson
Friday Institute
(swcarter, paemer, rlsartai,jerobins)@ncsu.edu

Steve Thorpe
MCNC
thorpe@mcnc.org

http://cloud.fi.ncsu.edu
cloudhelp@ncsu.edu
Developing an Identity and Access Management System

This page is left blank intentionally
Table of Contents

EXECUTIVE SUMMARY .................................................................................................................. 7

PROJECT BACKGROUND ................................................................................................................. 8

OVERVIEW OF PURPOSE ............................................................................................................... 10

IDENTITY MANAGEMENT OVERVIEW ......................................................................................... 11

POLICY AND GOVERNANCE ......................................................................................................... 13

Business Operations ..................................................................................................................... 15

Consume User Identity Information from Authoritative Data Sources ........................................ 16

Managing Identities ...................................................................................................................... 17

Managing Access .......................................................................................................................... 18

Centralized Reporting and Auditing .............................................................................................. 19

REQUIREMENTS AND SPECIFICATIONS .................................................................................... 20

FR1 Consume User Identity Data from Authoritative Data Sources ........................................... 21
 FR1.1 Connect & Monitor Authoritative Data Sources for New User Identity Data Files ............... 21
 FR1.1.1 Support Various Connection Interfaces ............................................................................ 22
 FR1.1.2 Support various connection interfaces specification ......................................................... 22
 FR1.2 Consume User Identity Data for Processing ....................................................................... 22
 FR1.2.1 Consume User Identity Data for Processing Specifications ............................................. 23
 FR1.3 User Identity Data Transformations, Processing, and Maintenance ..................................... 23
 FR1.3.1 Validate User Identity Data Specifications ........................................................................ 24
 FR1.3.2 Inspection/detection of duplicate records ........................................................................... 24
 FR1.3.3 Consuming only required User Identity Data fields .............................................................. 24
 FR1.3.4 Detect and handle changes in data between updates/consumptions (differentials) ........... 25
 FR1.3.4.1 Detect and handle changes in data between updates specification .................................. 25
 FR1.3.5 Identity Matching / Joining .............................................................................................. 25
 FR1.3.5.1 Identity Matching / Joining Specifications ..................................................................... 26
 FR1.4 User Data Loading ............................................................................................................... 26
 FR1.4.1 User Data Loading Specifications .................................................................................... 26
 FR1.5 General Notifications and Alerts ......................................................................................... 26

FR2 Manage Identities .................................................................................................................. 29
 FR2.1 Central Identity Manager ..................................................................................................... 29
 FR2.1.1 Central Identity Manager Specification ............................................................................. 29
 FR2.2 Central Directory Provisioning ............................................................................................ 30
 FR2.2.1 Central Directory Provisioning Specification ...................................................................... 30
 FR2.3 Central to Local Directory Syncing ...................................................................................... 30
Developing an Identity and Access Management System

FRS2.3 Central to Local Directory Syncing Specification ................................................................. 30
FR2.4 Consistent User Naming Convention ....................................................................................... 30
FRS2.4 Consistent User Naming Convention Specification .............................................................. 31
FR2.5 Automated Assignment of Roles, Groups Memberships, Entitlements .................................... 31
FRS2.5 Automated Assignment of Roles, Groups Memberships, Entitlements Specification ................ 31
FR2.6 Password Management ........................................................................................................... 32
FRS2.6 Password Management Specification ................................................................................... 32
FR2.7 Self-Service Capabilities ......................................................................................................... 32
FRS2.7 Self Service Capabilities Specification .................................................................................. 33
FR2.8 Service Provider User Identity Provisioning and De-provisioning .......................................... 33
FRS2.8 Service Provider User Identity Provisioning and De-provisioning Specification ..................... 34
FRS2.9 Delegation of Administrative Functions for Identity Management ....................................... 34
FRS2.9 Delegation of Administrative Functions for Identity Management Specification .................... 35
FR2.9.1 Group, role, membership, entitlement and policy management .......................................... 35
FR2.9.2 Reset user passwords ........................................................................................................... 35
FR2.9.3 Disable accounts ................................................................................................................... 35
FR2.9.4 Create system usage reports ................................................................................................ 36
FR2.9.5 Download LEA-specific data ................................................................................................ 36
FR2.9.6 Add and delete accounts ....................................................................................................... 36
FR2.10 Workflow Support .................................................................................................................. 36
FRS2.10 Workflow Support Specification .......................................................................................... 36
FR2.11 Guest User Self Registration .................................................................................................. 36
FRS2.11 Guest User Self Registration Specification .......................................................................... 37
FR2.12 Account Reconciliation ......................................................................................................... 37
FRS2.12 Account Reconciliation Specification .................................................................................. 37
FR2.13 Attestation ............................................................................................................................. 38
FRS2.13 Attestation Specification ....................................................................................................... 38
FR2.14 Identity Deactivation ............................................................................................................. 38
FRS2.14 Identity Deactivation Specification ....................................................................................... 38

FR3 Manage Access ........................................................................................................................... 39
FR3.1 Reduced Sign On (minimal requirement) ................................................................................... 39
FRS3.1 Reduced Sign On Specification ................................................................................................. 39
FR3.2 Single Sign On ........................................................................................................................... 40
FRS3.2 Single Sign On Specification ..................................................................................................... 40
FR3.3 Enterprise Single Sign On (future work) .................................................................................. 40
FRS3.3 Enterprise Single Sign On Specification .................................................................................... 40
FR3.4 Authentication Protocols .......................................................................................................... 40
FRS3.4 Authentication Protocols Specification ................................................................................... 40
FR3.5 Delegation of Administrative Functions for Access Management ........................................... 40
FRS3.5 Delegation of Administrative Functions for Access Management Specification .................... 41
FR3.6 Access Limited to Authorized Users ......................................................................................... 41
FRS3.6 Access Limited to Authorized Users Specification ................................................................ 41
FR3.7 Identity Federation Support ..................................................................................................... 41
FRS3.7 Identity Federation Support Specification ................................................................................ 42

FR4 Provide Centralized Reporting and Auditing ............................................................................. 43

FR5 IAMS Administrative Functions .................................................................................................. 44

NFR1 Identity Data Design .................................................................................................................. 45
NFRS1 Identity Data Design Specification ............................................................................................ 45

NFR2 Scale and Scope .......................................................................................................................... 46
## Developing an Identity and Access Management System

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFR3 Flexibility, Modularity, and Minimum Dependencies</td>
<td>47</td>
</tr>
<tr>
<td>NFR4 High-Availability Design</td>
<td>48</td>
</tr>
<tr>
<td>NFRS4 High-availability Design Specification</td>
<td>48</td>
</tr>
<tr>
<td>NFR5 Policy Support</td>
<td>49</td>
</tr>
<tr>
<td>NFR6 Simple, clean, easy user interfaces</td>
<td>50</td>
</tr>
<tr>
<td>NFR7 End-to-end Monitoring</td>
<td>51</td>
</tr>
<tr>
<td>DESIGN</td>
<td>52</td>
</tr>
<tr>
<td>IMPLEMENTATION</td>
<td>59</td>
</tr>
<tr>
<td>Strategies</td>
<td>59</td>
</tr>
<tr>
<td>Tentative RFP Process Timeline</td>
<td>59</td>
</tr>
<tr>
<td>Tentative Phases</td>
<td>59</td>
</tr>
<tr>
<td>Phase 0: Vendor Design/Planning Period</td>
<td>59</td>
</tr>
<tr>
<td>Phase 1: Data Consumption / Populate Identity Store</td>
<td>60</td>
</tr>
<tr>
<td>Phase 2: Basic Identity and Access Management Pilot</td>
<td>60</td>
</tr>
<tr>
<td>Phase 3: Federation Services</td>
<td>60</td>
</tr>
<tr>
<td>Phase 4: Expanding to Production</td>
<td>60</td>
</tr>
<tr>
<td>DEPLOYMENT</td>
<td>61</td>
</tr>
<tr>
<td>Strategies</td>
<td>61</td>
</tr>
<tr>
<td>Policy / Governance</td>
<td>61</td>
</tr>
<tr>
<td>Migration of LEAs</td>
<td>61</td>
</tr>
<tr>
<td>Pilots</td>
<td>61</td>
</tr>
<tr>
<td>Onboarding of Service Providers</td>
<td>61</td>
</tr>
<tr>
<td>PRODUCTION</td>
<td>62</td>
</tr>
<tr>
<td>Support / Help Desk Model</td>
<td>62</td>
</tr>
<tr>
<td>Outreach</td>
<td>62</td>
</tr>
<tr>
<td>Communication Model</td>
<td>62</td>
</tr>
<tr>
<td>Training and Professional Development</td>
<td>62</td>
</tr>
<tr>
<td>CURRENT WORK</td>
<td>63</td>
</tr>
<tr>
<td>FREQUENTLY ASKED QUESTIONS</td>
<td>64</td>
</tr>
<tr>
<td>POTENTIAL FUTURE WORK</td>
<td>67</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>69</td>
</tr>
</tbody>
</table>
Executive Summary

The NC Education Cloud Identity and Access Management System (IAM) shall provide every K-12 student, teacher, staff member, parent/guardian, and school community member in North Carolina an account, with a single username and password that will enable access to cloud-based learning resources. The IAM system will have three major components: a centralized data repository with all user information, a central directory service that provides a master authentication and authorization resource, and federation software that enables Single Sign-On functionality for users.

The data repository will be a centralized collection of all relevant user information from disparate data sources. The centralization of this data creates an opportunity for better reporting capabilities, data analytics generation, and access control management. The central directory service will also bring new options to local school district personnel by providing an automated mechanism for synchronizing global user information from the centralized directory service to local directory services. Finally, the federation software will give the end users a new experience of Single Sign-On. That is, a single username and password that grants access to all his or her relevant cloud services.

Overall, the IAM system can bring new options and opportunities to the local school districts. It has the potential to reduce support costs through more effective account life-cycle management and create a better, more productive user experience.
Project Background

In 2010, North Carolina was awarded a 4-year, $400M Race to the Top (“RttT”) award\(^1\) through the federal stimulus program. Receipt of this grant, designed to spur public school innovation, is a key component of North Carolina’s work to continue its momentum for school improvement. The NC RttT program includes five pillars: Statewide Standards and Assessments, Great Teachers and Leaders, Data Systems to Support Instruction, Turnaround of Lowest Achieving Schools, and State Success Factors.

An important element of the State Success Factors pillar is an NC Education Cloud with infrastructure, tools, and resources to support all NC RttT initiatives. This will be a service delivery platform for modern instructional and administration support systems. It will establish a K-12 education technology infrastructure to provide cost-effective and robust services for the LEAs, and provide digital tools and resources to support all RttT initiatives. The idea is to facilitate shared services through collaborative procurements, buying rather than building services where appropriate, using pay-for-use statewide licensing arrangements, and shared support models.

Expected benefits of the NC Educational Cloud include\(^2\):

- Cost savings for the LEAs through participation in a buyer’s consortium
- Increased IT efficiency through fewer servers that are utilized at a higher capacity
- Shift in emphasis from technology support to instructional support
- Improved reliability from servers hosted and managed in data centers with regular backups, formal disaster recovery plans, and stringent service level guarantees

The two foundational components of the NC Education Cloud include:

- Shared Infrastructure Services
  - X-as-a-Service
- Service Delivery Platforms
  - Learning Management Systems
  - Identity Management
  - Collaborative Tools
  - Learning Object Repository

Initially targeted shared services may include\(^3\):

- Email migrations into the cloud (e.g. Google, Microsoft)
- Web collaboration tools
- Central hosting of administrative applications
- Statewide Directory for services delivery

---

\(^1\) “NC Race to the Top”, http://www.ncpublicschools.org/rttt/


• Virtual desktops inside a web browser on an old PC or on a new netbook
• Unified Learning Management System and Learning Object Repository
• Managed/shared wireless services
• Network dashboards using statewide directory
• Content filtering as a service provided by the network controlled in the LEA
• Other Network services such as security, firewall, backup, and disaster recovery

The NC Education Cloud will provide a highly reliable, highly available, server infrastructure supporting the K-12 education enterprise statewide. Specifically, it will facilitate migration from LEA-hosted server infrastructure to cloud-hosted infrastructure as a service. The primary objective of the cloud is to provide a world-class IT infrastructure as a foundational component of the NC education enterprise. Moreover, the NC Education Cloud will provide for:

• Equity of access to compute and storage resources;
• Efficient scaling according to aggregate NC K-12 usage requirements;
• Consistently high availability, reliability and performance;
• A common infrastructure platform to support emerging instructional and data systems;
• Sustainable and predictable operational cost.

Robust technology infrastructure will support data-driven decision-making, for the development of and access to online instructional resources, and to transition the focus of district technical resources from infrastructure to users and instruction. Furthermore, prudent one-time investments in technology infrastructure service platforms buy down long-term IT costs, providing sustainable funding for new instructional and leadership programs.

A centralized identity and access management system is a foundational component for this shift in the IT paradigm. As more services move to the cloud, a centralized and standard way to manage accounts, roles, and permissions to these services is required for a successful cloud model.
Overview of Purpose

This document provides a snapshot of the proposed Identity and Access Management architecture and system. The purpose of the Identity Management project is to address the following challenges that K-12 stakeholders face:

1. **K-12 users have too many accounts for current services**
   The average student in NC currently has 4-6 accounts for accessing their learning resources, whether it is local LEA systems or cloud-based services. Teachers and other administrators on average have double that amount of accounts. Most of these accounts have different usernames and passwords. As these numbers increase, it has become difficult for the users to effectively manage the various account information in a responsible way. It has also become difficult for technical personnel to manage/support of setting and resetting passwords and updating user account information for the various cloud services.

2. **Manual process of updating account information from NCWISE to disparate local systems and services**
   LEAs have described the challenging process of getting user information from the NCWISE information system into their local systems/services. There are two general parts to this process: (1) getting the accurate, updated, and complete user information from NCWISE in an automated process. (2) Transitioning this information into user accounts for the various disparate systems and services for end users. If a new service is added, administrators must repeat this process. If user information is changed or updated, the process must also be repeated for each of the systems/services. While some districts have created automated processes, many others still struggle with this process manually.

3. **Need good foundation for K-12 cloud solutions growth**
   The NC Education Cloud proposes increasing the use of services in the cloud, which will increase the need for accounts and the task of managing user account information for those accounts. For a successful migration/deployment of services to a hosted/cloud-based solution, there is a need for some middleware (“glue”) that connect the various components. A strong identity management system is one of the foundational components for a large cloud computing environment.

The authors’ primary motivation for creating this document is to facilitate IAM related communications within and among NC Education Cloud Team, LEAs, vendors, similar state or regional projects, and other interested parties. We welcome feedback from all potential stakeholders, as in our view it will enhance our future success.

*Our Vision*

“Every student, teacher/staff member, parent/guardian, and school community member has a single unique username/password to access learning resources in North Carolina”
Identity Management Overview

Per EduCAUSE:\(^4\):

*Identity management refers to the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources. In a campus setting, many information systems—such as e-mail, learning management systems, and library databases—require users to authenticate themselves (typically with a username and password). An authorization process then determines which systems an authenticated user is permitted to access. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled. Federated identity management permits extending this approach above the enterprise level, creating a trusted authority for digital identities across multiple organizations. In a federated system, participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to online resources. This approach streamlines access to digital assets while protecting restricted resources.*

Key benefits of the IAM system described in this document will include:

- Home institutions reliably manage their own user accounts, groups, roles, attributes and access privileges *(Security)*
- Easier and faster access to computer resources through workflow-assisted account creation, activation and maintenance *(Saves time and $)*
- Prevents system administrators from having to add yet-another and another account *(Saves time and $)*
- Enables easier scaling and deployment of web-based applications to include multiple additional users/organizations *(Efficiency, scalability, saves time and $)*
- Prevents users from having to know yet-another password *(Security)*
- Avoids logins becoming out of date *(Security)*
- Confidence that users are who they say they are, with up-to-date accuracy *(Security)*
- Demonstrated ability to protect electronic identities through rigorous account lifecycle management, audit and reporting capabilities. *(Security)*

---

\(^4\) EduCAUSE's “Identity and Access Management":
http://www.educause.edu/Resources/Browse/IdentityandAccessManagement/17322

and

“7 Things You Should Know About Federated Identity Management”:
http://www.educause.edu/Resources/7ThingsYouShouldKnowAboutFeder/179330
• Future Ready Solutions: Once in place, DPI and LEAs can rapidly deploy new applications and services, with minimal account management overhead and related security risks ( Agility)

• Ability for LEAs to provide access and resources to non-traditional groups of users, such as volunteers from the local community. ( Inclusive)

• Through increased efficiencies mentioned above, teachers will have additional time and energies to devote to student experiences in the classroom. ( Efficiency)

• Jeff Scheidel has succinctly summarized IAM business value thusly: “Cost savings, productivity, ease of use, efficiency, security, compliance, simplification, automation, integration, consistency, and self-service”5

---

Policy and Governance

After the end of the NC Education Cloud initiative, a transition will occur to an organization that will be responsible for the day-to-day operations and oversight of cloud services. More information regarding this organization will be released with the final cloud implementation plan.

The NC Education Cloud team is engaged with several advisory bodies from the K-12 community and other state education organizations. These advisory bodies provide input for the final cloud implementation plan and other project plans. This process greatly enhances our understanding of the issues and validates alignment of needs and solutions.

There are currently three advisory bodies for the Identity Management project in addition to the core cloud team.

1. IAM Working Group (Technical and Application Advisory)

   The tasks for the Identity Management Working Group (Phase 1) will be:
   
   • Establish a communication model for exchanging ideas, concerns, and feedback between IAM Architects and local LEA representatives
   • Review and integrate information collected in the site interviews
   • Gather functional and non-functional requirements for developing a sustainable statewide IAM system
   • Define specifications about required technologies and system processes

   The Working Group Members are:

<table>
<thead>
<tr>
<th>Region</th>
<th>Name</th>
<th>School/County</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jeff Smith</td>
<td>Pitt County Schools</td>
</tr>
<tr>
<td>2</td>
<td>Wayne Beasley</td>
<td>Craven County Schools</td>
</tr>
<tr>
<td>3</td>
<td>Walter White</td>
<td>Wake County Schools</td>
</tr>
<tr>
<td></td>
<td>Chris Withrow</td>
<td>Warren County Schools</td>
</tr>
<tr>
<td></td>
<td>Mel Cherry</td>
<td>Northampton County Schools</td>
</tr>
<tr>
<td>4</td>
<td>Janice Harliss</td>
<td>Montgomery County Schools</td>
</tr>
<tr>
<td></td>
<td>Jordan Walsh</td>
<td>Moore County Schools</td>
</tr>
<tr>
<td>5</td>
<td>Mike Ingram</td>
<td>Thomasville City Schools</td>
</tr>
<tr>
<td></td>
<td>Lee Cummings</td>
<td>Rockingham County Schools</td>
</tr>
<tr>
<td></td>
<td>Betty Weycker</td>
<td>Winston-Salem/Forsyth County Schools</td>
</tr>
<tr>
<td></td>
<td>Candace Hosey</td>
<td>Alamance-Burlington County Schools</td>
</tr>
<tr>
<td>6</td>
<td>Michael Stocks</td>
<td>Cabarrus County Schools</td>
</tr>
<tr>
<td></td>
<td>Susan Manning</td>
<td>Charlotte-Mecklenburg Schools</td>
</tr>
<tr>
<td>7</td>
<td>Marty Sharpe</td>
<td>Catawba County Schools</td>
</tr>
<tr>
<td></td>
<td>Robert Lane</td>
<td>Mooresville Graded Schools</td>
</tr>
<tr>
<td>8</td>
<td>Michael Thompson</td>
<td>Rutherford County Schools</td>
</tr>
<tr>
<td></td>
<td>Charter</td>
<td>Celest O’Brien</td>
</tr>
<tr>
<td></td>
<td>At Large</td>
<td>William Haney</td>
</tr>
<tr>
<td></td>
<td>At Large</td>
<td>NC Information Technology Services</td>
</tr>
<tr>
<td></td>
<td>At Large</td>
<td>Chanin Rivenbark</td>
</tr>
<tr>
<td></td>
<td>At Large</td>
<td>NC Department of Public Instruction</td>
</tr>
</tbody>
</table>
2. NC Education Cloud Advisory Committee (Policy and Priority Advisory)

3. State Board of Education (Governance Body)

In the IAM system, a major portion of the project is the policies and governance of the system. Most identity management systems are composed of three major components: users, services, and policies. The policies define how the users interact with the services.

In the IAM system, the Policies, Regulations, and Rules (PRRs) will be created and revised as the project moves forward. The IAM architects, K12 stakeholders, and other advisory bodies will inform the development of the PRRs. Below are the initial categories in which PRRs need to be defined. Each of these areas loosely aligns with the Requirements and Specifications defined further in this whitepaper. These PRRs will eventually become more formalized with structure and process but to begin, we will be developing PRRs from simple questions.

**Need to define Policies, Regulations, and Rules and enforcements?**
Business Operations

1. Who is involved in contracts (outside of DPI written or purchased applications)?

2. Can LEAs enter into their own agreements with vendors, and if so – can they also authorize the release of student/staff data?
Consume User Identity Information from Authoritative Data Sources

1. What is the process for getting access to the authoritative data sources for employees/staff and service providers?

2. What are the Regulatory and Compliance Rules related to IAM?

3. Who OWNs the user data? (LEA, DPI, Parent, Staff member)

4. What data (elements, attributes) will be made available to the Central Registry?

5. Will parent data be self-asserted (captured via some other mechanism) or only provided via NCWISE?

6. What data is authoritative for Parents that are also Staff (NCWISE or HRMS)?

7. Once the data is transferred to the “Cloud”, does the ownership change?
Managing Identities

1. What are the default groups that users records will be structured into?

2. Who decides on what data is released – specific attributes?

3. How are accounts generated (triggers, what data is populated, what services are provisioned)

4. How do users authenticate (student, staff, parent)

5. Can Social Identities (e.g. GoogleID, FaceBook, etc.) be used by parents to authenticate? If so, what data is required?

6. What Identity-proofing and vetting is required in order to issue an account?

7. Who issues accounts? (e.g. School, LEA, etc.)

8. What identifiers are used for individuals? (NCWISEid, HRMSid, parents – email address?)
Managing Access

1. Who has access to Central Repository and Central Directory data? (only systemic access, ad hoc reporting, etc.)

2. Who determines what applications can consume user (student, staff, parent) data?
Centralized Reporting and Auditing

1. Who can request reports from the log-reporting tool?

2. Do periodic reports need to be run for ERPA violations?
Requirements and Specifications

Any model of a systems engineering process includes activities aimed at capturing requirements. Meaning understanding what the customers and users expect the system to do. So our understanding of the intent and functions starts with examination of requirements.

A requirement is a feature of the system or a description of something the system is capable of doing in order to fulfill the system’s purpose.\(^6\)

There are two types of requirements: functional and nonfunctional.

A functional requirement \([FR]\) describes an interaction between the system and its environment as what the system will do. The system shall do …..

A nonfunctional requirement \([NFR]\) describes a restriction on the system that limits our choices for constructing a solution to the problem. The system shall be …..

**Quality**
Quality requirements define specific performance expectations that customers and users have for identified functional requirements.

**Constraints**
Constraints are the rules, relations, and conventions that determine the boundaries and limitations that a requirement must be realized within.

A specification restates the requirements in technical terms appropriate for the development of a system design.

There must be a direct correspondence between each requirement and specification.

**Formatting and Layout:**

- Functional Requirement 1 (FR1)
  - Functional Requirement Specification (FRS 1)
    - Functional Requirement 1.1 (FR1.1)
      - Functional Requirement Specification (FRS 1.1)
      - Examples
    - Functional Requirement 1.2 (FR1.2)
      - Functional Requirement Specification (FRS 1.2)
      - Examples
  - Non-Functional Requirement 1 (NFR1)
    - Non-Functional Requirement Specification (NFRS 1)
      - Non-Functional Requirement 1.1 (NFR1.1)
        - Non-Functional Requirement Specification (NFRS 1.1)
        - Examples
      - Non-Functional Requirement 1.2 (NFR1.2)
        - Non-Functional Requirement Specification (NFRS 1.2)
        - Examples

---

FR1 Consume User Identity Data from Authoritative Data Sources

The IAM system has a general need for a comprehensive data integration tool that is fully automatable. This tool should have the capability to perform general extract, transform, and load (ETL) functions. It should be able to transform, move, and synchronize data residing in numerous heterogeneous systems and applications. While there will be many places throughout the IAM system where these data integration functions are needed, the first task of the IAM system is to consume user identity data from the authoritative data sources.

The system must communicate with the authoritative data sources and retrieve the user data files. The user data files will include numerous attributes about students, parents, and staff in the NC K-12 Education System. The user data need to be processed/transformed and then loaded into the identity manager component.

FR1.1 Connect & Monitor Authoritative Data Sources for New User Identity Data Files

Initially, the North Carolina Window of Information on Student Education (NCWISE) and Human Resources Management System (HRMS) from the Department of Public Instruction (DPI) are the authoritative data sources for students, parents, and staff data. The IAM system must actively monitor the authoritative data source system for new user data files. When new user data files are produced, the system can begin the consumption process.

Example: A new user data file is generated by the authoritative data system and transferred to MFTS at 7am. The IAM system should immediately detect that a new user file is available and retrieve/consume it.

FRS1.1 Connect & Monitor Authoritative Data Sources for New User Identity Data Files Specifications

The IAM system will not have direct access to the authoritative data source systems (NCWISE and HRMS). The IAM system will have to access a copy of the user identity data from these systems through the NCDPI Managed File Transfer System (MFTS). The MFTS is essentially a secure FTP server system. On a semi-periodic basis, the user data is extracted from the authoritative sources into a tab-delimited, flat text file format, then zipped up and put into a folder on the MFTS that the IAM system has access to. This task is completed by the authoritative data source systems. There will be one file for the student user data and one file for the staff user data. An MFTS file naming Convention has been provided to the IAM team to assist with the MFTS process. The NCWISE data includes approximately 1462 data fields for each record, as documented in the NCWISE data dictionary at [http://www.ncwise.org/documents/sas_ahr/DataDictionaryWebDoc.pdf](http://www.ncwise.org/documents/sas_ahr/DataDictionaryWebDoc.pdf).
Example: The daily extract of user data may appear in the MFTS inbox at 7am Monday through Saturday, but get then appear at 1pm on Sunday instead of 7am. This is the reason of the active monitoring of the MFTS folder for new files.

FR1.1.1 Support Various Connection Interfaces

The IAM system must be able to consume data from multiple heterogeneous source systems that provide a wide array of connection interfaces. These connections could change over time as different source systems are introduced and the IAM mechanism that consumes the data will have the capability to change accordingly.

Example: The current method for accessing student information is via flat files that can be obtained periodically via SFTP. The IAM system must provide a mechanism to invoke the SFTP process according to a pre-set schedule, and then consume it.

FR1.2 Consume User Identity Data for Processing

The IAM system must have the ability to consume the user identity data via three methods. Method 1: Scheduled. The IAM system should connect to the authoritative data source on a pre-determined schedule and retrieve the data. Method 2: Manually invoked. The IAM system should be a method for manually invoking
the data consumption process.
Method 3: Simple monitoring. The IAM system should be able to watch the authoritative data sources for new files or user data changes and start the data consumption process when new user identity data files appear.

Example: Updated student, parent, or staff datasets are provided on an hourly basis. The system should be able to successfully process that new data every hour.

Example: IAM system administrator(s) should have the ability to manually start the data consumption process with the click of a button.

**FRS1.2 Consume User Identity Data for Processing Specifications**
The IAM system must be able to connect to the MFTS system and copy/move the user identity data files to the data integrator tool for processing.
Method 1 Scheduled means having the ability to set a schedule when to consume data on a granular level. This method should have similar scheduling abilities as Unix cron or modern calendaring applications.
Method 2 Manually invoked means having a button to press this manually starts the data consumption process if needed.
Method 3 Simple Monitoring means having the ability to actively monitor the inbox folder inside MFTS and listen/watch for new identity data files.

The IAM system will need to transfer the zipped files from the MFTS inbox to the IAM system for processing and then remove them from the MFTS inbox. The files cannot stay in the MFTS inbox due to storage restrictions on the MFTS side.

Example: Based on observation thus far, we have determined that MFTS does not produce data files on the same schedule everyday. MFTS may start and stop producing the user identity data files without notice. There could be dry periods of time when no data files are produced. The identity data files could appear at different times on different days. Monday through Saturday the data files are generated around 7am but on Sunday, they might not be generated until 1pm.

**FR1.3 User Identity Data Transformations, Processing, and Maintenance**
The IAM system must have the ability to parse the user data and discover the schema of the input data source files. After this discovery process, a series of checks need to be performed before processing.

**FR1.3.1 Validate User Identity Data**
The IAM system must have the ability to validate and cleanse user identity data based on pre-determined specifications/metrics. The system must be able to handle null or invalid input data records (e.g. identify incomplete or bad data fields/attributes) and alert an administrator before consuming that user identity data record. It must have self-protection
features/capabilities to avoid consuming bad data from the authoritative data sources. Input data with a minimum set of attributes must be stored in a way that allows for various maintenance on it using the Create, Read, Update, and Delete (CRUD) model.

Example: Does every user student record have a unique student identification number based on what a student id number looks like: 9 digit number, no alpha? If the system checks an a student identification number is 123abc, it should create an alert/notification for the administrator.

Example: Perhaps having the ability to create pre-defined metrics that set the scope of input data and if input data does not comply/conform with those metrics then don’t consume and send an alert.

Example: A student record is consumed but does not include a first name or last name. The system should reject that record and notify the administrator.

**FRS1.3.1 Validate User Identity Data Specifications**

The IAM system will …

Example: The system normally consumes around a 100MB CSV file with user identity data. During the next consumption, the CSV file is 10GB. It is probably not a good idea to consume that and something on the source end made a mistake.

**FR1.3.2 Inspection/detection of duplicate records**

The IAM system must have the ability to detect duplicate records upon consumption of the data.

Example: During the next user identity data consumption, the system detects two records with the same unique student identification id. If the records are identical for all the fields that are of interest to the IAMS, only one is kept and the other is ignored. If the records have fields of interest that differ, the system should note the discrepancy (perhaps alerting the administrator) and be capable of either keeping one of the records, or tossing them both out.

**FR1.3.3 Consuming only required User Identity Data fields**

The IAM system must have the ability to only consume pre-determined fields that define user identity data. The input data may contain non-relevant data fields that should be ignored by the system.

Example: The identity data may contain a field that described EOG test scores. This information may be relevant for an LMS system but should be ignored for the IAM system.
Example: The list of NCWise and HRMS attributes that are needed might include:

a) Students Accounts from NC WISE: StudentID, FirstName, LastName, Middle Initial, School, Grade, Course Memberships, Entry Date, Exit Date, Course Enrollments (for Groups and Rostering), LEA, School, Timestamp of last modification, Originator of modification

b) Parent Accounts from NC WISE: TBD – WE NEED TO REVISIT THIS ONE

c) Staff Accounts from HRMS: HRMS_ID, FirstName, LastName, Middle Initial, Department, Division, Position Site, Position Code, Position Description, Manager, Effective Start Date, LEA, School, Timestamp of last modification, Originator of modification

FR1.3.4 Detect and handle changes in data between updates/consumptions (differentials)

The IAM system must have the capability to consume and determine the deltas or changes since the last consumption of user identity data. Assume the authoritative sources do not have the capability to distribute changes in user data.

Example: If the system consumes user identity data at 10am and a single fields/record changes with a students address, then when the system consumes the user identity data again at 11am, the system must be able to detect that single changed record, then consume only the changed address.

FRS1.3.4 Detect and handle changes in data between updates specification

The IAM system shall be able to determine deltas between successive inputs from authoritative data sources (e.g. NCWise, HRMS) that will likely consist of up to several million input data records per input. Input data set sizes will likely be on the order of up to 1-10 GB each, and may be in flat file format. Using the deltas that it computes, the IAM system shall be able to propagate appropriate changes into and beyond the IAM system. The IAM system will need to potentially have the capability to store the last set of data files to compare with to find the differential.

FR1.3.5 Identity Matching / Joining

The IAM system must have the capability to match and join data as appropriate from disparate input authoritative data sources through which individuals are "registered" as part of the identity management system. Typical data sources might include a Student System that also has Parent data, HR system for staff, Guest/Affiliate System, etc. The identity match or "join" process compares identity data across Systems of Record to ensure that a single identity is created, modified, and deleted for an individual, even if that individual exists in more than one System of Record simultaneously and/or moves back and forth between Systems of Record. The system should also be able to assign roles based on which system(s) of record the identity is a part of.
Example: An individual is a parent in the Student System, and that same individual is a Teacher in the HR system. The IAM System must provide a mechanism by which a single identity can be created, deleted, and modified for that individual, even though that individual exists in more than one System of Record. An identity of this type would be assigned roles appropriate for the systems of record it was created from, e.g. “parent” and “teacher”.

**FRS1.3.5 Identity Matching / Joining Specifications**

The IAM ...

**FR1.4 User Data Loading**

The IAM System will have the capability to consume user data from various heterogeneous systems but it must also have the ability to load data into various heterogeneous systems or applications. One load function will be into the identity manager component. The data integration tool can be used to load data from other IAM component into cloud based applications.

Example: Identity Data needs to be exported in a CSV file and uploaded to Google Apps for Education to setup the initial user base.

**FRS1.4 User Data Loading Specifications**

The IAM ...

**FR1.5 General Notifications and Alerts**

The IAM system must have the ability to create alerts/notifications to appropriate personnel based on system or processing events. This function must be in place across the whole IAM system but is particularly important in the consuming phase. The consuming identity data is the first step of the process and it is important to alert administrators if there were any challenges during this step.

Example: The input user data file changes from .csv to .sql. While IAM may be able to consume a .sql file, an alert/notification should be sent to administrator(s) describing that the normal .csv file was not found.

Example: If the number of incoming identity records changed from 1,000,000 to 100. That would be considered a significant change and an administrator should be alerts via some method.
FR1.5 General Notifications and Alerts Specifications

The IAM system must be able to create alerts/notifications via email, text, pager, and web services based on administrator-defined parameters (and system parameters). The data integration tool should have an elaborate set of logging capabilities that would be able to record all activities related to monitoring, consuming and processing of the input user data. Every activity should be logged but only certain events will generate/require a notification. The notifications should be able to be customized and preconfigured based on administrators needs.

Example: If an error occurs when the data integration tool retrieves the latest user data files and attempts to unzip the archive, this action and failure should be logged and a notification should be sent to the administrators notifying them of the issue.

Example: 1,500 of 1,000,000 input records from the NCWise system had incorrectly formatted NCWiseID fields, therefore those records are considered invalid and should not be consumed by the system. The administrator(s) should be able to be notified of this challenge in a manner suitable for human consumption: e.g. in a single notification or report that summarizes the 1,500 errors, rather than a flood of 1,500 individual notifications.
FR1.6 Architecture and Standards

The IAM system data integrator tool must support a broad set of platforms and provide an open architecture that supports multivendor IT infrastructures.

*Example: A Microsoft based Integration Tool does not talk with a Novell Based directory.*

**FRS1.6 Architecture and Standards Specifications**

The IAM system must ...

*Example: If ...*

FR1.7 User Interface

The IAM system must provide an intuitive graphical user interface and command line interface for the development, deployment, and maintenance of data integration rules.

*Example: Simple portal for delegated administrations and end users to access identity things.*

**FRS1.7 User Interface Specifications**

The data integration tool should provide a web-based console and command line interface for the administration and development of the integration rules.

*Example:*

**Notes for FR1**

What are the performance implications regarding ETL and other data processing functions?
Developing an Identity and Access Management System

**FR2 Manage Identities**

The IAM system will centrally store and manage user identity information for students, parents, staff, and community members. The identity manager component will be able to define groups, roles, and entitlements for each identity.

**FR2.1 Central Identity Manager**

The IAM system must provide a central identity manager mechanism (some refer to this function as a “Person Registry” that consolidates identity data information from disparate systems. The data ultimately originates from a process owner, such as Human Resources, NCWise/DPI, etc., and is used for matching, merging, and aggregation of data and records. Views of the data are then made available to service providers and application developers to determine access. The Central Identity Manager must store and manage identity, credentials (username/password combinations), group, role, sponsor, entitlement, and related information, all normalized to common identity standards regardless of source. It must be able to attach sponsors to identity records such that roles can be audited and possibly expired when a sponsor disappears

**FRS2.1 Central Identity Manager Specification**

1. Establish and maintain a data dictionary of defined identity attributes.
2. Implement core functions to add, modify, and remove groups, identities, roles, entitlements, and group members.
3. For newly identified individuals, assign one or more identifiers for internal and/or external use according to predefined algorithms, optionally relying on external systems that are canonical for one or more identifiers.
4. Allow multiple external source records for the same identity to be linked to that person’s identity record.
5. Attach role data and attributes to an individual's identity (person) record, linked by authoritative data source record(s).
6. Permit linking of identity records to sponsors.
7. Normalize data by executing local routines on all input data regardless of source.
8. Support the storage of credential metadata (username, password, last password change time, etc.)
9. Record all changes applied to central identity manager records, in a form/location suitable for subsequent searches of those change records.
10. API to expose core functions to external software.
11. Define a permission model that covers all data that is capable of being provided in an extract from the identity manager.
FR2.2 Central Directory Provisioning

The IAM system must provide a centralized directory provisioned with the required user identity information from the authoritative data sources.

FRS2.2 Central Directory Provisioning Specification

This will require development of a suitable schema and OU structure that takes into account all of NC’s 115 LEAs (school district) and 100+ Charter Schools, the 2500+ schools within the LEAs, and the roles / groups / entitlements discussed elsewhere in this document. Since each LEA and Charter School is considered an autonomous entity with access to only its own data, it is critically important that access to the central directory information be limited to a “need-to-know” basis.

Possible Example: Include ideas on schema here? Could possibly get some from the one D shared.... I couldn’t find it in the files from his USB stick though. Have email about it … stay tuned. - Steve

FR2.3 Central to Local Directory Syncing

The IAM system must provide a mechanism to update an LEA’s local directory with global user identity information from the central identity manager. This could include newly provisioned or de-provisioned identities, password changes, contact data, or other user attributes.

FRS2.3 Central to Local Directory Syncing Specification

It is anticipated most local directories will be Active Directory, eDirectory, or OpenLDAP. Synching must be possible in real- or near-real-time (where appropriate), or by using a batch process. Data synced to an LEA should ONLY be data on identities associated with that LEA, while all other data is not accessible to that LEA.

FR2.4 Consistent User Naming Convention

The IAM system must provide ability to enforce and maintain a consistent user naming convention that also enforces uniqueness.
FRS2.4 Consistent User Naming Convention Specification

User names must be uniquely defined, so each user name corresponds to one identity in the system. Uniqueness could possibly be across an LEA rather than across the entire system, provided scoped usernames could be used where needed to differentiate among users in different LEAs that have the same un-scoped username. Identification of the exact user naming convention has not yet been completed; we expect this to occur during the early detailed design phases of the project.

Example: Suppose the chosen user naming convention is `<firstinitial><lastname><somenumber>`, where `<somenumber>` could be blank or a non-negative integer. The `<somenumber>` could be incremented as needed when collisions would otherwise occur. If system can support scoped usernames across the LEAs, then the same unscoped username (e.g. “sthorpe”) could be used in different LEAs, as in `sthorpe@rock.k12.nc.us` and `sthorpe@davie.k12.nc.us`, which would be scoped usernames for different individuals at two different LEAs.

FR2.5 Automated Assignment of Roles, Groups Memberships, Entitlements

The IAM System should enable automatically setting a base set of roles, groups, and entitlements for each identity, based upon policy settings and each user’s attributes.

**FRS2.5 Automated Assignment of Roles, Groups Memberships, Entitlements Specification**

*This will require development of the base set of roles, groups, memberships, entitlements and policies to be automatically assigned. The base set has not yet been developed; we expect this to occur during the early detailed design phases of the project. Possible examples are describe below.*

Example: A 10th grade student from Durham Public Schools’ Hillside High School is assigned an identity in the IAM system. Based on policies configured in the IAMS, the user is assigned 1) the student role; 2) memberships in the Hillside High School, Durham Public Schools, and high school groups, plus membership in any classes that she is enrolled in, and 3) entitlements to GoogleApps.

Example: A teacher from Durham Public Schools’ Hillside High School is assigned an identity in the IAM system. Based on policies configured in the IAMS, the user is assigned 1) the staff and teacher roles; 2) memberships in the Hillside High School, Durham Public Schools, and high school groups, plus teacher of any classes that she is responsible for, and 3) entitlements to GoogleApps.
Example: Per discussions with LEA members, some example roles might be as follows:
Adult
Contractor
Counselor
District Admin
District Coordinator
EC Admin
EC General/Teacher
Finance/Personnel
IT
Media coordinator
Nurse/Social Worker
School/Site Admin
Secretary
Staff
Student
Teacher
Tech facilitator
Testing and Accountability
Volunteer

FR2.6 Password Management

The IAM system must provide a mechanism to assign initial passwords to new identities, communicate a new password to the owner of that identity, to enforce password policies, and to change passwords. This will require development of a suitable password policy.

Example: A web-based password application could be visited by a new user, through which a challenge-response interaction could be used to confirm that user’s identity and to set their initial password. Password policies might include which combinations of characters would be considered valid, and expiration dates.

Example: The same application could later be visited by the user, when he/she wishes or needs to update their password.

FRS2.6 Password Management Specification

The IAM ...

FR2.7 Self-Service Capabilities

The IAMS must have a set of self-service capabilities, including password management as described previously, as well as information update change request (e.g. contact
Developing an Identity and Access Management System

information change request), and resource access requests. Requests would trigger a workflow approval process, where authorized LEA personnel could then respond appropriately. *User-interfaces presented to self-service end-users need to be simple, clean, and intuitively easy to use and understand.*

**FRS2.7 Self Service Capabilities Specification**

TBD.

**FR2.8 Service Provider User Identity Provisioning and De-provisioning**

The IAM system must have the capability to provision and de-provision identity data and accounts to/from external systems, in an automated fashion where appropriate based on policy. In addition to local LEA directories, this could include the capability to support the provisioning and integration of accounts (including username and password) on different operating systems, to external applications such as Google Apps and potentially to “legacy” applications that require provisioning through CSV files, etc.

As the IAM system is rolled out, we'll need to consider strategies for on-boarding application capabilities into the new system. There are many factors that might influence which apps should be prioritized, such as:

- desirability / popularity of app
- readiness of app (e.g. if it already speaks SAML, it's easier than if it uses proprietary formats for which connectors aren't already built. It is also possible there are apps that won't ever speak to this IAM system, based on their formats or requirements.)
- readiness of the LEAs
- other factors such as consortium buying vs. district buying, how does that play in? Perhaps with consortium buying, we can best influence the vendors to adopt standards such as SAML.

In terms of popularity of various applications, here are some results from the initial 40 site surveys -- categorized according to application type. Here we show some of the most popular apps and how often LEAs mentioned them.

**Web Collaboration:**
- Google Apps (32.5%)
- Wiki Spaces (27.5%)
- Google Docs (25%) *(this is really Google Apps)*

**LMS:**
- Moodle (57.5%)
- Blackboard (35%)
Developing an Identity and Access Management System

Web Conferencing:
  - Skype (52.5%)
  - WebEx (20%)
  - GoToMeeting (12.5%)

Digital Content:
  - Discovery Education (52.5%)
  - NC Wise Owl (32.5%)
  - NetTrekker (12.5%)

Library Automation:
  - Follet/Destiny (80%)

ILS:
  - ClassScape (60%)
  - Study Island (20%)
  - NovaNet (15%)
  - mClass (15%)

More data from the site surveys will be available in coming months, as the surveys are winding down and the results can be tabulated. But the above data probably gives a good idea of what to expect. So perhaps Google Apps (Docs) and a couple of the other highly popular applications could be placed high on the priority list.

From our perspective, we see it as very important to pick a small application set (perhaps 1-3) to start with as we get the IAM system off the ground. Then over time, additional apps can be on-boarded according to their priority. The choice of initial application(s) is an important one, and it will be guided and vetted by various stakeholders such as the IAM Working Group which is made up of members from many LEAs.

**FRS2.8 Service Provider User Identity Provisioning and De-provisioning Specification**

TBD. Need to describe specific interfaces in specifications with examples.

**FR2.9 Delegation of Administrative Functions for Identity Management**

LEA administrators with appropriate permissions would be granted sufficient access to maintain their LEA’s data on the IAMS, including but not limited to the following items as described in subsequent subsections:

1. Group, role, membership, entitlement and policy management
2. Reset user passwords
3. Disable accounts
4. Create system usage reports
5. Download LEA-specific data
6. Add and delete accounts

**FRS2.9 Delegation of Administrative Functions for Identity Management Specification**

This will require development of the base set of roles, groups, memberships, and entitlements and policies to be manually assigned on a case-by-case basis. The LEA technology directors and other authorized personnel shall have a set of administrative controls to the central IAM System, with access limited to only authorized data from their own LEA. This ensures keeping control where it belongs – at the local LEA level. Administrative controls should be presented to authorized personnel using simple, intuitively easy-to-understand web-based interfaces.

**FR2.9.1 Group, role, membership, entitlement and policy management**

The IAM System shall provide authorized administrative users the ability to create and manage customized groups, roles, memberships, and entitlements, as well as the policies used for automated assignments described in FR2.5 Automated Assignment of Roles, Groups Memberships, Entitlements.

*Example:* A customized cloud-based application for use by AP Physics students becomes available. An entitlement authorizing use of that application could be created, along with a policy that all members of the AP Physics class would be granted that entitlement.

**FR2.9.2 Reset user passwords**

While end users have the ability to reset their own password, authorized personnel must have the ability to reset user passwords for accounts they manage.

*Example:* A third grade teacher is granted the privilege to reset the passwords for students in his classes.

**FR2.9.3 Disable accounts**

Authorized personnel must have the ability to disable/deactivate accounts for users within their organizational realm.
FR2.9.4 Create system usage reports

Authorized personnel must have the create reports of IAM system usage by users within their organizational realm. For further information, please see the section titled FR4 Provide Centralized Reporting and Auditing

FR2.9.5 Download LEA-specific data

Authorized personnel must the ability to download LEA-specific data in various formats, e.g. CSV files or spreadsheets of users and limited attribute information.

FR2.9.6 Add and delete accounts

Authorized personnel must have the ability to create, update, and deactivate identities within their organizational realm.

Example: Accounts might for example be added for testing purposes, or for community members, and the accounts would typically be created for a finite authorized duration. At the end of that duration, authorized personnel would need to reauthorize an account otherwise it would be automatically disabled by the system.

FR2.10 Workflow Support

Automated workflows shall enable approval of change requests such as roles, entitlements, etc., initiate manual data update procedures as required at the local LEA level, and initiate provisioning and de-provisioning access to systems and resources as appropriate, managing community, student, and parent roles, account lifecycles, privilege granting, administrative approvals, etc., while having the flexibility to allow for manual exceptions to standard defined roles.

The administrators of the IAMS, not the delegated LEA administrators, shall perform design and construction of workflows.

FRS2.10 Workflow Support Specification

TBD.

FR2.11 Guest User Self Registration

The IAM system shall have capabilities to allow sponsor-approved user self-registration in the identity manager; typically this would be utilized by newly registering community members or their sponsors.
FRS2.11 Guest User Self Registration Specification

The guest user self registration system should be presented using simple, intuitively easy-to-understand web-based interfaces. Self-registration requests should notify the sponsor (likely by email), who can then approve or deny the request. Approved accounts would be enabled for a specific period of time, with the sponsor granted the ability to extend the account or terminate it early.

Example: Joe Smith, proprietor of Joe’s Muffler Shop, is collaborating with the students in Hillside High School’s 10th Grade shop class. Duffy Brown, teacher of the shop class, has an account that is authorized to sponsor community members to become a member of a group shared with that shop class. Joe Smith (or Duffy Brown on Joe’s behalf) requests an account through the self-registration system, specifying Duffy Brown as his sponsor. A workflow is kicked off that generates an emailed authorization request to Duffy Brown. Duffy Brown receives the request, and follows a link in the email to authorize the community account. A time limit and Duffy Brown’s sponsorship is associated with the community account. Duffy Brown’s approval would be needed to continue the account’s activation status beyond its expiration date, and Duffy Brown would also have the ability to initiate deactivation of the account at his discretion.

FR2.12 Account Reconciliation

The IAM system shall have the capability to perform account reconciliation between the central identity manager and service provider directory systems. This function might also be referred to as “adopting orphaned accounts” – pre-provisioned accounts that already exist in external systems. [Question: Do we want & could we actually have the ability to “grandfather in” existing account names/conventions, then use the new convention only for new accounts? - Steve]

Example: An LEA is already providing access to the GoogleApps or Microsoft Live@EDU services to its user community, prior that LEA’s joining the IAM system. The IAM system must have a mechanism to identify all those pre-provisioned user accounts, and associate them with identities in the system. Furthermore, as part of this process, the IAM system should be able to utilize any account renaming API(s) that might be provided by the external service, to synch up the users names in the service with the user naming convention employed by the IAMS.

FRS2.12 Account Reconciliation Specification

TBD.
FR2.13 Attestation

The system shall have the capability for attestation, a process that enables users designated as reviewers to be notified of reports they must electronically review.

**FRS2.13 Attestation Specification**

The system should be able to generated reports describe provisioned user identities and their access to resources. A reviewer can attest to the accuracy (or inaccuracy) of the entitlements by providing a response. The attestation action, and reviewer response, is tracked and audited to provide a complete trail of accountability.

*Example: An LEA has a set of IAM System administrator identities, with a “super-user” entitlement that grants them the ability to access highly sensitive, private information about all users at that LEA. On a monthly basis, the LEA’s superintendent and technical director each must review a report identifying those users, and approve (or disapprove) the users granted “super-user” entitlement. Should a user’s “super-user” status be disapproved of by either of these reviewers, the entitlement for that user will be revoked.*

FR2.14 Identity Deactivation

The IAM system shall have the capability to deactivate identities.

**FRS2.14 Identity Deactivation Specification**

De-activation could occur automatically, for example when a pre-assigned expiration date or status has been reached. It could also occur manually, as entered by an LEA-designated administrator of the IAM system for that LEA. Upon deactivation of the identity, the IAM system shall de-provision any associated accounts, yet maintain the deactivated record in the system.

*Example: The school year ends, and the senior graduates. All identities in the system associated with a graduated senior have passed their pre-assigned expiration date. At that point, based upon the exceeded date, the IAM system shall de-provision any associated accounts and de-activate the identity within the system.*
FR3 Manage Access

Automated granting of access to shared services must be a feature of the system, according to settings granted through the delegated administrative functions described elsewhere in this document. As per our vision: “Every student, teacher/staff member, parent/guardian, and school community member has a single unique username/password to access learning resources in North Carolina”. As described in earlier sections on managing identities, a login/password credential will be provided to all students, faculty, staff, guest community members, and DPI staff. The login/password will grant access to all authorized DPI and cloud-based applications through directory-based and other mechanisms. The credentials (login/password combination) assigned to an identity shall enable Reduced Sign On at a minimum, possibly Single Sign On, and perhaps at some point in the future Enterprise Single Sign on.

FR3.1 Reduced Sign On (minimal requirement)

The system will provide user experience of reduced sign on at minimum.

FRS3.1 Reduced Sign On Specification

The user would have the same username/password but might have to actually type their login / password more than once.

Certain applications and legacy systems would not work with a single authoritative store of username / password. In those (less desirable) circumstances, it may be required to hold the username / password within the application’s custom store rather than externally. The IAM system should support automated propagation of username/password updates to those applications, when the central registry detects a changed password.

Example: Suppose an LEA is using Google Apps but not with its SSO configuration. In that case the user’s password is stored within Google Apps. Using API’s provided by Google, it is possible for updated passwords to be propagated into Google, which would allow the user to use their same password when logging onto Google. We refer to this as Reduced Sign On (“RSO”), where the user would have to actually type their login / password more than once, however it would be the same username/password.
FR3.2 Single Sign On

To the extent possible, all web-based applications will have a single sign on (SS) – the user only needs to enter their login / password once, and they’re granted access to all supported web-based applications.

**FRS3.2 Single Sign On Specification**

The system should support directory authentication, SAML, cookies, and/or Kerberos tickets as needed to achieve SSO.

FR3.3 Enterprise Single Sign On (future work)

This describes a scenario where the end user logs onto their local device (e.g. a laptop, desktop, or mobile device) with their unique username/password, and from that point access to all local and cloud-based resources is automatically provided by the system. This would require the device login to be using an domain-provided rather than a local account.

**FRS3.3 Enterprise Single Sign On Specification**

TBD.

FR3.4 Authentication Protocols

The IAM system shall support authentication through multiple protocols.

**FRS3.4 Authentication Protocols Specification**

Supported protocols for authentication should include a web-services APIs, plus broad support for web technologies including Java and PHP, SAML 2.0-based identity federation and interoperability with Shibboleth. For further information on federation, please see the section titled FR3.7 Identity Federation Support.

FR3.5 Delegation of Administrative Functions for Access Management

Similar for delegation of user administration capabilities, LEA administrators with appropriate permissions shall be granted sufficient access to configure their LEA’s Access Management. *This will require development of the base set of roles, groups, memberships, and entitlements and policies to be manually assigned on a case-by-case basis.*

**Example:** An LEA’s IAMS Administrator wishes to grant access to a newly available NC Cloud Based application to all of his LEA’s high school students. That administrator needs to be
able to enable that application for all users in his LEA with the student role and members of the high school group.

**FRS3.5 Delegation of Administrative Functions for Access Management Specification**

TBD.

**FR3.6 Access Limited to Authorized Users**

Access to identity data shall be limited to only authorized users, and LEA-specific data shall not be released to anyone outside that LEA.

**FRS3.6 Access Limited to Authorized Users Specification**

TBD.

**FR3.7 Identity Federation Support**

Identity federation technologies allow digital identity information to be shared across multiple organizations. In a federated system, participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to web-based applications. Identity and attribute assertions are shared through the user’s web browser session using the SAML (Security Assertion Markup Language) protocol. Service Providers (SPs, or applications) and Identity Providers (IdPs) “recognize” each other based on previously exchanged metadata information.

An IdP is a web application that makes authentication decisions – a user logs in to their home institution’s IdP with their usual login and password. The IdP produces attribute assertions shared through the user’s web session, according to the IdP organization’s security policies as configured in the IdP. Attributes are then consumed by an SP, which is often hosted by a different administrative organization. The SP grants access to the user, if appropriate based on its own policies and the attribute values asserted by the IdP.

Some of the benefits of identity federation are:
- Extends existing identity-management and resource services
- Integrates new users, services, and resource providers faster and easier
- Reduces need for per-service account provisioning
- Eases account management, as users manage fewer accounts
• Privacy maintained: Users identify themselves locally with their home institution, then pass only relevant and necessary attributes to the resource
• Security: reduces opportunities for accounts to be compromised

Two well-known implementations of the SAML protocol are provided by Microsoft’s Active Directory Federation Service (ADFS)\(^7\) and by the open-source Shibboleth\(^8\) software.

**FRS3.7 Identity Federation Support Specification**

The IAM System must provide SAML2.0\(^9\) Identity Provider functionality capable of interoperation with SAML Service Providers hosted by outside organizations. IdP functionality may need to be exposed as one IdP per LEA and Charter School, or as one large configuration that would encompass all LEAs and Charter schools under a single IdP.

---

\(^8\) [http://shibboleth.internet2.edu/](http://shibboleth.internet2.edu/)
\(^9\) [http://saml.xml.org/saml-specifications](http://saml.xml.org/saml-specifications)
FR4 Provide Centralized Reporting and Auditing

The system must have the capability to generate reports of prior system activity for audit and other purposes. A set of standard reports must be available, and the ability to customize reports where appropriate. Centralized logging mechanisms may be used to support this process.

This capability will help ensure access privileges granted to all systems accurately reflect an individual’s status and role with the organization. Reporting and reconciliation processes must provide the assurance that accounts and privileges in individual systems match up with the information in the IAM system.

Ability to audit for regulatory compliance is also desired. Please see Appendix C – Regulatory and Compliance for a list of the key regulations involved.
FR5 IAMS Administrative Functions

The IAMS administrative staff must have a more advanced user interface and appropriate additional functionality and privileges, as compared to the LEA administrators and end-users. Supported IAMS administrative tasks could include for example:

- Care and feeding of the overall system
- Applying policies as appropriate to the various user roles
- Managing which attributes are consumed by the system
- Adjusting the user interface(s) / controls seen by the delegated LEA administrators, and by the end-users for self-service functionality
- Designing / maintaining customized workflows to be used by LEA-designated administrators
- **Management / User Portal**
NFR1 Identity Data Design

A common standard schema for identity data must be designed for the IAMS, based partially on data already maintained within NCWise and HRMS authoritative data sources.

NFRS1 Identity Data Design Specification

The standard will include recommended minimal baseline set of attributes (e.g. name, ID number, etc.) and groups/roles (e.g. student, teacher, parent, principle, employee, community, etc.). The design must include ability to handle multiple and hierarchical roles for each user, within e.g. each school, LEA, etc. It shall be vetted with stakeholders such as the IAM Working Group, with its representatives from the LEA communities.

Example: Per discussions with LEA members, some example roles might be as follows:
Adult
Contractor
Counselor
District Admin
District Coordinator
EC Admin
EC General/Teacher
Finance/Personnel
IT
Media coordinator
Nurse/Social Worker
School/Site Admin
Secretary
Staff
Student
Teacher
Tech facilitator
Testing and Accountability
Volunteer
NFR2 Scale and Scope

Ultimately, the system must efficiently support millions of identities from 2600+ schools in NC’s 115 LEAs and 100+ charter schools, which include more than 2600 schools, 1.3 million students, 180 thousand faculty / staff, between 1-2 million parents/guardians, and additional stakeholders from the various local communities. A system that can support up to 10 million entries will more than support growth and churn of NC K-12 users over the next 10 years.

Any vendor software solution should be able to provide evidence of previous successful IAM deployments of this scale and scope.

Any systems integrator, affiliated partners, or other service providers associated with the software solution should be able to demonstrate competency and evidence of an IAM deployment of this scale and scope.
NFR3 Flexibility, Modularity, and Minimum Dependencies

The IAM system must be designed and architected as flexible and modular as possible and demonstrate the concept of minimum dependencies. Minimum dependencies means, to the extent possible, the IAM system will be designed in such a way that no single component (e.g. authentication mechanism, directory platform, registry database, federation software) is highly dependent on any other single component such that it could not be changed or modified with a reasonable amount of effort. The IAM System will be designed in such a way that various components can be updated and/or changed with minimum impact on the overall system. It will have a plug and play feel. The design should that allows the system to grow and adapt to new user sources and targets services over time without requiring a re-architecture of the core system.

These same three concepts also apply to any system integrators, partners, or service providers. The system and services surrounding the IAM system will not be dependent and proprietary to any one organization or solution for support, service, or operations.

All aspects of the IAM system will uphold the utmost continuity between the cloud services body and services providers.

*Example:* We have Directory Service Software version 2011 and then version 2013 comes out. We must be able to update our software to the latest version with minimum changes.

*Example:* Initial system consumes NCWise data, but then NCWise system is replaced with an alternate Student Information System (SIS). We must be able to update our software to the new SIS with minimum changes.

*Example:* NCWise and HRMS input datasets are deprecated in favor of an ODS which becomes available and allows more efficient data access. The IAMS system must be straightforward to adapt.

*Example:* Phased implementation approach

*Example:* New User Data Sources

*Example:* Scale and Scope

*Example:* Cloud Services / Applications
**NFR4 High-Availability Design**

The IAM system must have a design and infrastructure such that single component failures or planned maintenance events will result in a minimum service disruption. It is expected that upgrades and planned maintenance events will occur with no (or perhaps minimal) disruption in service. All scheduled maintenance activities will be planned, approved, and communicated well in advance.

**NFRS4 High-availability Design Specification**

While the design of the IAM system shall be for 100% uptime, the system shall have a Service Level Agreement (SLA) specifying at least 99.9% uptime on a quarterly basis. Thus no more than 2.19 hours total per quarter of unexpected downtime would be acceptable according to the SLA. This may require development, testing, and redundant production environments.
NFR5 Policy Support

An advisory body will provide oversight in terms of policies, rules and regulations surrounding the support, maintenance, and oversight of the NC Education Cloud Identity and Access Management System. It will inform the workflows, processes, governance and data access issues for each of the major components of the system. The purpose of this is to provide governing structure for a sustainable system. The IAMS system must be flexible enough to adapt to the advisory body’s requirements.
NFR6 Simple, clean, easy user interfaces

Administrative user-interfaces presented to LEA personnel need to be simple, clean, and easy to understand and use. Higher-end functionality such as workflow design would not be available to the delegated administrators at the LEAs.
NFR7 End-to-end Monitoring

The IAMS must be monitored end-to-end, 24x7, for successful current operations, with administrative personnel notified in case of problems.
Design

We currently have several high level illustrations that describe a proposed model for addressing the identity management challenges facing K-12 stakeholders. These illustrations show the major components of an NC K-12 Identity and Access Management System and how they could potentially interact with local LEA resources, the authoritative data sources, and various cloud-based service providers.

Figures 1 through 5 pictorially represent various components of the desired system.

**Identity and Access Management (IAM) System has 3 Major Components**

1. **Central Data Repository**
   The central repository will be comprised of relevant user data from various authoritative data sources

2. **Central Directory Service**
   The central directory will contain all user IDs, passwords, and other identity information. It will serve as master authentication and authorization point for all cloud-based services and allow syncing to LEAs

3. **Federation Software**
   The federation software security extends identity information to cloud-based services providing end users with single sign on experience

*Figure 1: NC Education Cloud’s Major IAM Components*
Developing an Identity and Access Management System

Figure 2a: NC Education Cloud - User Account Provisioning
Developing an Identity and Access Management System

Figure 2b: NC Education Cloud - User Account Provisioning

User Data is consumed from the authoritative data systems using the NCDPI Managed File Transfer System (MFTS). The MFTS system provides a secure SFTP connection between DPI and Cloud IAM.

User data is retrieved on a scheduled interval into the IAM system for account provisioning. A heartbeat application is also running to monitor endpoint connections.
Developing an Identity and Access Management System

Local users log into devices and authenticate against Local LEA Directory Service as normal.

Local LEA Directory Service can sync to Central Directory Service for global user accounts.

Central Directory Service gets provisioned from Authoritative Data Sources.

Figure 3a: NC Education Cloud - Local LEA and IAM Directory Integration

Figure 3b: NC Education Cloud - Local LEA and IAM Directory Integration Details
Figure 4: NC Education Cloud - IAM System - Big Picture
Developing an Identity and Access Management System

Figure 5: NC Education Cloud - User Experience
Most Identity Management Systems are divided into three core pieces: USERS, POLICIES, and SERVICES. The POLICIES define how the USERS interact with the SERVICES.

Figure 6: NC Education Cloud - IAM Policies
**Implementation**

*Building the shell/framework and preparing for use*

**Strategies**

Phased Implementation  
Close Vendor and other Service Provider Relationship  
Well defined Policy and Governance Model  
LEA ownership of IAM System

**Tentative RFP Process Timeline**

Tentative Timeline/Schedule (October 2011 – May 2012)

- **Step 0:** Preplanning (1 month, September 2011)
- **Step 1:** RFP Preparation (3 months, October – December 2011)
- **Step 2:** RFP Release (1 month, January 2012)
- **Step 3:** RFP Team Reviews (1 month, February 2012)
- **Step 4:** Face-to-Face Interviews with leading RFP candidates (2 weeks, March 2012)
- **Step 5:** Final Administrative Details and RFP Awarded (2 weeks, March 2012)
- **Step 6:** Start Project (April 2012)

**Tentative Phases**

After RFP is awarded...

**Phase 0: Vendor Design/Planning Period**

- Develop plan
  - Identify people / roles / responsibilities / expectations of vendor(s), cloud team, etc.
  - Staff requirements / skill sets
  - Hardware
  - Milestones
  - Deliverables
  - Sustainability
  - Identify candidate pilot participants
  - Identify candidate initial applications
Developing an Identity and Access Management System

- Plan for integration with ODS
  - Obtain and study NCWise / HRMS Data
  - Data sanity checking
  - Data / policy design
    - Default groups / roles / memberships / entitlements
    - Decide on Account conventions
      - Account naming
      - To scope or not to scope?
      - To allow grandfathered accounts with different naming conventions or not?
      - How to synch up pre-existing, “orphaned” accounts

**Phase 1: Data Consumption / Populate Identity Store**
- Consume data into IAM system with basic error detection / match / global merge
- Basic schema and OU structure defined for central / global directory
- Populate Global Directory, including automated population of basic roles / groups / memberships / entitlements
- Develop LEA readiness-assessment
- Develop Application (service provider) readiness assessment

**Phase 2: Basic Identity and Access Management Pilot**
- Initial password assignment
- Authentication
- Self Service Password Reset
- Delegated Administrative functions (password reset, roles, group management)
- Deploy initial cloud service(s)
- Test with initial LEA(s)

**Phase 3: Federation Services**
- Single Sign-on using SAML

**Phase 4: Expanding to Production**
- See Deployment and Production Sections
Deployment

Strategies

Policy / Governance

Migration of LEAs

Pilots

Onboarding of Service Providers
Production
Support / Help Desk Model
Outreach
Communication Model
Training and Professional Development
Developing an Identity and Access Management System

Current Work

We have many areas to focus on now and in coming months. Right now we’re only at the beginning of the process. Here are some of the our tasks – in no particular order and certainly this is not a complete list:

• **Vet our thought process with LEAs.** Currently, all 115 LEAs are completing detailed site based interviews related to the NC Education Cloud initiative effort. The interviews have three major objectives: 1) educational; 2) information gathering, and 3) engender support of the Cloud effort. We expect interview results to substantially help inform our implementation plan. The interviews during site visits will provide us with anecdotal evidence and direction from real users, real customers, and real issues in the field.

• **Decide on partners.** We have already engaged in productive information gathering sessions with several potential partner vendors. Our intent is to continue informal discussions with additional vendors during the next couple months. Later, we may issue a more formal Request for Information (“RFI”) or Request for Proposals (“RFP”), after we’ve gained a better understanding of the requirements and objectives.

• **Design / study / implement (or buy) / test many things.** For example:
  - Prototypes / experimenting / possibly attend training classes
  - Tools to populate master registry from multiple disparate input data sources, ensuring data deduplication and unique statewide logins are handled correctly
  - Delegation of administrative functions to LEA level
  - Self service password management tools
  - Addresses need of attribute / grouping / directory functionality
  - Systems to enable (hopefully live?) centralized -> local directory transfers
  - Test various apps (e.g. GoogleApps, Live@EDU, Moodle, API access methods, etc.) against centralized system
  - Robust, highly available centralized SSO solution (plus possibly local option)
  - Test and retest all this stuff to ensure the proposed system can handle the expected load!

• **Description of Current IAM related work of others.** What are other organizations/LEAs/etc doing around the state that relate or are similar to our project? Are there areas in which collaboration is appropriate?
Frequently Asked Questions

FAQs are gathered from LEA Site Interviews, LEA conference presentations, webinars, and other communication mediums between stakeholders and NC Education Cloud team. They will be listed below and have the best response available with the current information and plans.

Q. Do you foresee the backend central directory having standard interfaces like LDAP that many applications know how to talk to?

   A. Yes, the central IAM system will have the ability to talk common protocols and standards, such as LDAP, SAML, WS-Federation, Web Services.

Q. Do you see the user information sync as a real-time or scheduled event?

   A. Currently, we believe user information sync will be done in two phases. Phase 1 sync will be from the authoritative data sources to the central IAM system approximately every hour. Phase 2 sync will be between the central directory service to the local LEA directory services. This sync time will vary depending on local requirements but we anticipate a 1 to 24-hour time frame.

Q. Will the LEA have control over which cloud-based services each user can access?

   A. Yes, the central IAM system will provide some simple control mechanisms to the LEAs that allow access control changes for their respective services.

Q. Will changes in the LEA directory service sync up to the central directory service?

   A. No, the central directory service will provide a one-way sync of global user information to the local LEA directory service. The local data managers, according to current LEA processes, would make any necessary user information changes. During the initial migrations, the IAM system will have abilities of reconciliation of identity information from local systems.

Q. Is there a plan to incorporate NCID staff/student processes with the IAM or is the IAM completely separate from NCID?

   A. The NC Education Cloud IAM team is currently having discussions with the ITS NCID team about potential opportunities for collaboration between the teams and systems. One opportunity would be federation of identity between the Education Cloud IAM and NCID IAM system.
Q. Will the central IAM system allow LEAs to connect and build our own groups, or will we have to manually, or script downloads as we do from NCWISE.

A. The central directory service would have some basic groups predefined based on NCWISE and HRMS attributes. However, it would provide LEAs with a mechanism to customize the users and groups to the necessary granularity and needs of each particular LEA.

Q. When will the IAM pilots be ready?

A. We are tentatively planning to have IAM pilots running in Fall 2012.

Q. Who and how many people will run the state help desk for user IDs?

A. The Cloud team is currently developing a help desk model that encompasses support for the IAM components as well as other services driven by the cloud project. The team is in the early stages of requirements gathering to help define LEA support needs surrounding the new cloud services model.

Q. Will the cloud project provide assistance to LEAs for any migrations/conversions/interfaces necessary to take advantage of the new cloud services?

A. Yes, the identity management project has significant resources to assist LEAs get migrated/connected/interfaced with the new, upcoming cloud based services. We will be working with LEAs on an individual level to see that you are able to take advantage of the new service offerings.

Q. Will I be able to access DPI applications, like the Apex Reporting System, with my single cloud account?

A. There are two parts to this answer: (1) We will approach DPI as a Service Provider at the appropriate time and discuss which applications they would like to interface with the IAM. (2) Many of those applications use NCID, which could be federated with our cloud IAM.

Q. Who will manage the IAM when it is finished?

A. The cloud team is working to build a sustainable support model for all cloud bases services. Some current recommendations are to form an education service agency and support network.
Q. Are you working with vendors that are currently deploying or have deployed identity management services to the districts?

A. Yes. We are communicating with organizations who have worked in this area and with NC LEAs. The IAM system will require some levels of migration/changes at LEAs who opt in and the organization you are currently familiar with and use may be a good fit. So far, we have talked with Data Networks, TiberCreek, CSI Technology Outfitters, and others.

Q. What reliability can the LEAs expect for the IAM system?

A. One of the topics that came up during vendor discussions was that of Service Level Agreements (SLAs) and how many "nines" of availability the IAM system should have. Of course, we plan for the IAM system to operate continuously, with any *expected* downtime scheduled well in advance and during off-hours, and communicate to all stakeholders. Through discussions with the IAM Working Group members, it was determined that 99.9% uptime would be sufficient. This would allow no more than 2.19 hours per quarter of unexpected downtime.

Should the IAM system experience an unexpected downtime, that would mean unavailability of administrative and self-service interfaces for maintaining passwords, roles, groups, new users, etc. However, unexpected downtime of the IAM system would in some cases NOT interrupt access to external accounts that are accessed directly and have previously been pre-provisioned by the system.
Potential Future Work

This section describes a few additions, enhancements, etc. to the IAM system that are under consideration for future work efforts.

Federating with NCID

The state’s NCID system maintains identities for thousands of state employees and citizens. In situations where cloud applications might benefit both NCID and NC Cloud users, it could make sense to federate that application. Through federating the application with these two identity systems, the same application could allow access to users from both. The NC Cloud and ITS NCID teams have started discussing this possibility.

NCTrust and/or other Federations.

Through the NCTrust Federation pilot, some SAML-based success has already occurred among DPI, Davie County Schools, Rockingham County Schools, and several other organizations in NC (MCNC, Duke, UNC-Chapel Hill, NC State, Wake Tech Community College, Central Piedmont Community College). For Davie and Rockingham County Schools, the pilot allowed students to be authorized using the Shibboleth SP (service provider) software and SAML assertions with their NCWiseID, as provided by their LEA’s Shibboleth Identity Provider (IdP) as enabled by the NCTrust Federation. Once the NC Cloud’s IAM system is in place, one big Identity Provider (IdP) could be set up for all LEAs, or alternatively on IdP per LEA could be set up. Any such IdPs could easily be added to the NCTrust Federation, or other Federations. As a result, connecting to Higher Education and Community College Services would require less effort.

Enterprise Sign-On

This describes a scenario where the end user logs onto their local device (e.g. a laptop, desktop, or mobile device) with their unique username/password, and from that point access to all local and cloud-based resources is automatically provided by the system. This would require the device login to be using an domain-provided rather than a local account.

Identity Management Tools Portal

An Identity Management Tools Portal might provide a single web-based “launch-pad” to all NC Cloud based applications. In addition to a clean interface for the identity management self-service functionality described elsewhere in this document, it could include simple icons to access any of the cloud application(s) the portal user is authorized for.
Alternative Authoritative Data Source Point(s)

The NC Cloud team is developing plans for an Operational Data Store (ODS), which would likely provide a convenient access point for the same NCWise and HRMS data described in this document. The current NCWise system itself may be replaced by an alternate system in coming years. Likewise, additional as-yet-unknown data sources may become available. In any of these situations, the IAM system may be modified to adapt to the new sources of authoritative data.
References


Designing an IAM Framework with Oracle Identity and Access Management Suite, by Jeff Scheidel, ©2010

Identity and Access Management RFP, by Swarthmore College, downloadable from https://sites.google.com/a/swarthmore.edu/idm_rfp/home/rfp-documents

### Appendix A – Acronyms List

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPI</td>
<td>North Carolina Department of Public Instruction[^10]</td>
</tr>
<tr>
<td>ETL</td>
<td>Extract, Transform, Load</td>
</tr>
<tr>
<td>ESSO</td>
<td>Enterprise Single Sign On</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>LEA</td>
<td>Local Education Agency (school district)</td>
</tr>
<tr>
<td>NCID</td>
<td>North Carolina Identity Management System[^12]</td>
</tr>
<tr>
<td>NCWise</td>
<td>North Carolina Window on Student Education[^13]</td>
</tr>
<tr>
<td>RFI</td>
<td>Request for Information</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposals</td>
</tr>
<tr>
<td>RSO</td>
<td>Reduced Sign On</td>
</tr>
<tr>
<td>RttT</td>
<td>Race to the Top[^14]</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SLO</td>
<td>Single Log Off</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
</tbody>
</table>

[^11]: [http://hrms.dpi.state.nc.us/](http://hrms.dpi.state.nc.us/)
[^12]: [https://ncid.nc.gov](https://ncid.nc.gov)
## Appendix B – Terminology Review

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning</td>
<td>The create, update, delete process for user identities, groups, roles, privileges and accounts (both user and “service” accounts.)</td>
</tr>
<tr>
<td>Registry</td>
<td>The “master”, or “meta” directory / database holding official data for user identities (with a single record per subject), roles, passwords. Often reconciles data integrated from a variety of sources (e.g. could be HR systems, NCWisEID from ESIS, etc.). This likely has a large backend database as a component.</td>
</tr>
<tr>
<td>Group Management</td>
<td>Stores information about which identities are in particular groups. Examples include Custom web-based tool, Grouper &amp; AD, home-grown using LDAP, etc.</td>
</tr>
<tr>
<td>Authentication (AuthN)</td>
<td>Assertion of “who you are”. Usually gated by login/password</td>
</tr>
<tr>
<td>Authorization (AuthZ)</td>
<td>Granting of permission to an authenticated user’s access to a specific resource (often an application, perhaps web-based)</td>
</tr>
<tr>
<td>Federation / SAML IdP, SP, DS (WebSSO)</td>
<td>AuthN from home institution to AuthZ by remote web-based app, usually orchestrated through user’s web browser.</td>
</tr>
</tbody>
</table>
Appendix C – Regulatory and Compliance

The IAM project will need to comply and observe numerous federal/state regulatory and compliance rules due to its interaction with sensitive, personal identifiable information.

**Health Insurance Portability and Accountability Act (HIPAA) of 1996**

The Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. The Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

**Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment)**

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

**Children's Internet Protection Act (CIPA)**

The Children’s Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

**Children’s Online Privacy Protection Act of 1998 (COPPA)**

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children’s privacy and safety online.

---

18 [http://ww.coppa.org/comply.htm](http://ww.coppa.org/comply.htm)
Developing an Identity and Access Management System