Developing an Identity and Access Management Service for

North Carolina Education Cloud

A Race To The Top Initiative

Wednesday, February 29, 2012
Version 5.0
Prepared by:
Sammie Carter, Phil Emer, James Robinson, Lee Sartain
Friday Institute
(swcarter, paemer, jerobins, rlsartai}@ncsu.edu
Mark Scheible, Steve Thorpe
MCNC
(mscheible, thorpe}@mcnc.org

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

This page is left blank intentionally
Developing an Identity and Access Management Service

About the Authors

Sammie Carter

Sammie Carter is a Systems Architect for the NC Education Cloud Program. He is currently leading the Data Integration and Identity and Access Management projects, and is also a major contributor to other RttT Initiatives. Prior to his work on the NC Education Cloud, Sammie started at the Friday Institute in summer of 2005 where he designed and built the Friday Institute’s overall technology infrastructure. He served as Associate Director of Technology where he managed all IT Operations. Sammie holds a Bachelor’s of Science degree in Computer Science from the College of Engineering at N.C. State University. He also serves as an Adjunct Professor in the Department of Computer Science at N.C. State.

Phil Emer

Phil Emer has spent more than 20 years working at the intersections of data communications, research, academia and business – splitting time between the public and private sectors. In the private sector Phil worked as an engineer with IBM, as a technology executive with venture-backed Carolina Broadband and as a technology director with not for profit MCNC. In the public sector Phil directed voice, video, and data communications at NC State University and now serves as Director of Technology Planning and Policy at the Friday Institute where he leads the NC Education Cloud initiative funded under the NC Race to the Top grant.

Phil serves on the NC eLearning Commission, is a member of the advisory board of the Institute for Next Generation IT Systems, and serves as adjunct faculty in the Department of Computer Science. In November 2009, Governor Bev Perdue appointed Phil to the NC Innovation Council. Phil holds a B.S. in electrical engineering from Virginia Tech and an M.S. in computer engineering from NC State University.

James Robinson

James Robinson is a Systems Architect for the NC Education Cloud. He is currently supporting the design and deployment of platforms that provide for the tagging, grouping, storage, role-based access, and analysis of learning objects and instructional content. This work supports online professional development and instructional improvement system elements of the RttT grant. Prior to his involvement with the NC Education Cloud, James worked in Cooperative Extension at NCSU, where he worked on a national grant to design and build a collaborative content management and delivery system for land-grant universities across the US. James has held several other information technology positions at NCSU as a network management expert within the campus network group and as a senior technical staff member with the Centennial Networking Lab. He holds BS and MS degrees in Computer Engineering from NCSU.
Lee Sartain

Lee Sartain is the Education Policy Specialist at the Friday Institute for Educational Innovation at North Carolina State University. His expertise is at the intersection of where technology meets education policy, with a deep understanding of institutional practices at the school district and state levels. His focus on the NC Education Cloud is Data Management and Analysis. Prior to his work on the NC Education Cloud, he provided technical leadership on the NC 1:1 Learning Technology Initiative and the NC School Connectivity Initiative.

Mark Scheible

Mark Scheible has worked in the information technology field for over 30 years and is currently the Identity and Access Management Solutions Architect at MCNC in Research Triangle Park, NC. He is a member of the Identity and Access Management project team for the North Carolina Education Cloud initiative, a Race to the Top project for K-12. He was formerly the Identity and Access Manager for North Carolina State University in Raleigh, NC and worked to establish an IAM governance infrastructure as well as an IAM Roadmap for the university. Prior to NC State Mark worked as an IT Manager with Dartmouth-Hitchcock Medical Center. It was here that Mark's interest in Identity and Access Management was first sparked, dealing with the complexities of authentication and de-authentication in a medical setting. He also had the opportunity to explore the use of 2-factor authentication and PKI through a collaborative effort with Dartmouth College. Mark started his IT career with Digital Equipment Corporation and Compaq Computers in systems management and later as a windows system administrator. Mark is a member of the EDUCAUSE Identity & Access Management Working Group. He is also the vice-chair of the NC Federated Identity Management Task Force at MCNC/NCREN. He is also an active participant of the National K-12 Federated Identity and Access Management Task Force - a collaborative group of participants from CoSN, EDUCAUSE, InCommon and Internet2.

Steve Thorpe

Steve Thorpe is a Senior Systems Programmer Analyst on MCNC’s Advanced Services Development team, where he provides research and development on cutting-edge services to be delivered to MCNC’s K-20 customer base. Steve has extensive experience in Identity Management projects within NC’s K-20 community, including collaborations with the Department of Public Instruction and two LEAs (Rockingham and Davie County Schools) in developing the world’s first SAML-based Identity Federation to span across K-20 institutions. He has a varied background in software design, implementation and delivery, distributed computing, systems administration, computer graphics and technical leadership. Steve holds B.S. and M.S. Computer Science degrees from the University at Albany.
Contents

PREFACE .................................................................................................................................................. 10
Acknowledgements .................................................................................................................................... 11

EXECUTIVE SUMMARY ......................................................................................................................... 12

PROJECT BACKGROUND ......................................................................................................................... 13

IAM PROJECT OUTLINE AND SCHEDULE ......................................................................................... 16
Phase I – Research and Planning ............................................................................................................... 16
Phase II – Establish Service Model ........................................................................................................... 17
Phase III – Build and Implementation ....................................................................................................... 18
Phase IV – Full Production and Operation ................................................................................................ 19

IAM BENEFITS ....................................................................................................................................... 20

PART I POLICY AND GOVERNANCE ..................................................................................................... 21
Policy and Governance ............................................................................................................................... 22
IAM Policy Development ......................................................................................................................... 26
Policies, Regulations, and Rules (PRR) Workflow ..................................................................................... 27

Procedures and Workflows ...................................................................................................................... 28
Procedure 1: Granting User Access to Cloud Services and Applications ................................................. 28
Procedure 2: Changing User Identity Information ..................................................................................... 28

Selection of Initial Applications and Target Systems ................................................................................ 29

PART II REQUIREMENTS AND SPECIFICATIONS ................................................................................. 31
Requirements and Specifications Description .......................................................................................... 32
FR1 Data Integration Platform ................................................................................................................ 33
FR1.1 Connect & Monitor Authoritative Data Sources for New User Identity Data Files .......................... 34
FR1.1 Specifications .................................................................................................................................. 34
FR1.1.1 Support Various Connection Interfaces ..................................................................................... 35
FR1.1.1 Specifications ............................................................................................................................... 35
FR1.2 Consume User Identity Data for Processing .................................................................................. 36
FR1.2 Specifications .................................................................................................................................. 36
FR1.3 User Identity Data Transformations, Processing, and Maintenance .............................................. 37
FR1.3.1 Specifications ............................................................................................................................... 38
FR1.3.2 Inspection/detection of duplicate records ..................................................................................... 38
Developing an Identity and Access Management Service

FR3 Manage Access .........................................................................................59
  FR3.1 Reduced Sign On (minimal requirement)......................................................60
  FRS.1 Specifications .........................................................................................60
  FR3.2 Single Sign On ........................................................................................60
  FRS.2 Specifications .........................................................................................60
  FRS.3 Single Log Out .........................................................................................60
  FR3.3 Specifications .........................................................................................61
  FR3.4 Authentication Protocols .........................................................................61
  FRS.4 Authentication Protocols Specifications ..................................................61
  FR3.5 Delegation of Administrative Functions for Access Management ............61
  FRS.5 Delegation of Administrative Functions for Access Management Specifications ..................................................61
  FR3.6 Policy-based Access Control ..................................................................62
  FRS.6 Specifications .........................................................................................62
  FR3.6.1 Entitlement Based Access Control .........................................................62
  FR3.6.2 Group Based Access Control ................................................................62
  FR3.6.3 Role Based Access Control ..................................................................62
  FR3.7 Identity Federation Support ....................................................................62
  FRS.7 Identity Federation Support Specifications ..............................................63

FR4 Security Information and Event Management (SIEM) ......................................64

FR5 IAM Administrative Functions ......................................................................65

NFR1 Identity Data Design ..................................................................................66
  NFRS1 Identity Data Design Specifications ......................................................66

NFR2 Scale and Scope .........................................................................................67
  NFR2.1 Concurrency .........................................................................................67

NFR3 Flexibility, Modularity, and Minimum Dependencies ......................................68

NFR4 High Availability and Disaster Recovery ....................................................69
  NFRS4 High-availability Design Specifications ................................................69
  NFRS4.1 Platform Environments ......................................................................69

NFR5 Portal/Dashboard/Launchpad ......................................................................70

NFR6 Change Management and Messaging ..........................................................70

NFR7 IAM System Performance ..........................................................................71

NFR8 IAM User Accessibility ..............................................................................71

NFR9 Policy Support ............................................................................................71

IAM High-Level Design .......................................................................................72

PART III SERVICE MODEL ..............................................................................79

IAM Service Model Overview .............................................................................80

Strategic Principles .............................................................................................80
Developing an Identity and Access Management Service

IAM Service Roles ........................................................................................................... 82
IAM Policy and Governance Role .................................................................................. 83
IAM Service Manager Role ............................................................................................ 85
IAM Data Sources Role .................................................................................................. 87
IAM Managed Service Role ........................................................................................... 88
IAM Service Consumers Role ....................................................................................... 90

Project Portfolio Management ......................................................................................... 92

Service Plan Development ............................................................................................... 94
Requirements of Service Plan ........................................................................................ 94

Identity Data Sources, Target Cloud Services, and Federation Partners ............................. 96
Identity Data Sources ..................................................................................................... 97
NCWISE .......................................................................................................................... 97
UID .................................................................................................................................. 97
Target Cloud Services .................................................................................................... 99
Setup test/development/staging accounts & systems for potential target services ............. 101
List/vetting to determine target services ....................................................................... 101
Migration Strategies ....................................................................................................... 101
Federation Partners ....................................................................................................... 102

PART IV BUILD AND IMPLEMENTATION .................................................................. 103

Build and Implementation Model .................................................................................... 104

Technical Implementation Plan Development .................................................................. 105
Requirements of Technical Implementation Plan ................................................................ 105

PART V FULL PRODUCTION AND OPERATION ....................................................... 109

Full Production and Operations Model .......................................................................... 110

Ongoing Support Model ................................................................................................ 110

Ongoing Funding Model  Ongoing Migrations for Service Consumers .............................. 110

Ongoing Policy and Governance Model .......................................................................... 110

APPENDICES ................................................................................................................ 111

Appendix A – Potential IAM Future Work ...................................................................... 112
Federating with NCID ...................................................................................................... 112
NCTrust and/or other Federations ................................................................................... 112
Enterprise Sign-On .......................................................................................................... 112
North Carolina School of Science and Mathematics and other unique schools ................. 113
Alternative Authoritative Data Source Point(s) ................................................................ 113
Portal ............................................................................................................................... 113
IAM Components API Access for LEAs ........................................................................ 113
Federal Identity Management .......................................................................................... 114
Operational Data Store ................................................................................................... 114
UNC Federation ............................................................................................................. 115
Developing an Identity and Access Management Service

Appendix B – Regulatory and Compliance ................................................................. 117

Appendix C – IAM Research .................................................................................. 119

Appendix D – Requirements for Integrating Cloud Applications .......................... 120
  Provisioning and De-provisioning of Cloud Accounts .......................................... 121
  Automated (Direct) Provisioning ....................................................................... 121
  “Manual” (Indirect) Provisioning ....................................................................... 121
  Provisioning on “First Use” (Special Case) ....................................................... 122
  Provisioning and De-provisioning; Specifications .............................................. 122
  Authentication Methods for Cloud Services ..................................................... 123
  Model 1: Identity Federation ........................................................................... 123
  Model 2: Central Authentication and Authorization via Reverse-Proxy Portal .... 125
  Model 3: Centralized User Authentication and Authorization Management ........ 126
  Model 4 - Local Authentication ....................................................................... 127

Appendix E – IAM Project Assumptions, Risks, and Dependencies .................... 128
  Assumptions ....................................................................................................... 128
  Risk Analysis Table ........................................................................................... 128
  Dependencies ...................................................................................................... 134

Appendix F - Frequently Asked Questions .............................................................. 135

Appendix G – Proposed Policies, Regulations and Rules (PRRs) .......................... 138
  Business Operations PRRs ................................................................................ 138
  Data Integration Platform (Authoritative Data Sources) PRRs ......................... 139
  Managing Identities PRRs ................................................................................. 140
  Managing Access PRRs ..................................................................................... 141
  Centralized Reporting and Auditing PRRs ........................................................ 142
  IAM Service Roles PRRs .................................................................................. 143

Appendix H – MFTS File Naming Convention ....................................................... 144
  File ID Construction Convention ..................................................................... 144
  Definitions follow: ............................................................................................. 145

Appendix I – NCWISE Student Demographics Extract Data Definitions .............. 146

Appendix J – UID Staff System Extract Data Definitions ....................................... 153

GLOSSARY .............................................................................................................. 157
Preface

The purpose of this document is to provide a comprehensive set of information surrounding the identity management issues in the North Carolina K-12 Education system and a plan for developing a statewide Identity and Access Management Service to address these issues. It is important to note that the K-12 Education System includes users from Pre-Kindergarten (Pre-K) to early college high schools (13) groups. The beginning clearly describes foundational support roles of the IAM project for the NC Education Cloud Projects and other Race To The Top Pillars. This document is separated into five major parts. Part I describes the critical need for Policy and Governance standards to provide structure, guidance, and oversight to the IAM Service. Part II dives into the high-level Requirements and Specifications for the system. Part III articulates how to create a sustainable Service Model for such a system. Part IV covers the Build and Implementation part of the project, including the deployment and migration model and the development of a Technical Implementation Plan. Finally, Part V covers Full Production and Operation of the IAM Service.

The target audience for this document varies depending on which section is being read. For example, any of the beginning sections describe the background of the project and are targeted to technology directors and superintendents. The Requirements and Specifications section is aimed toward technology directors and the vendor community who would potentially be IAM Managed Service provider. The services section targets technology directors, finance, and operational support personnel.

This plan is intended to serve as a living document throughout the IAM project and will change/update as needed. There are numerous dependencies within the scope of this project and some requirements and specifications cannot be described until other parts are completed. As such, some sections of this document are incomplete.
Acknowledgements

**IAM Working Group.** The IAM Working Group, which includes representatives from the LEAs, Charter Schools, NCVPS, NCSSM, DPI and ITS, has been a tremendous value to this project. It has provided vast amounts of feedback and clarifications to the IAM team. It has also given us a vast insight into the LEA environment that has continuously improved the IAM plan.

**Vendor Information Sessions.** We would like to extend our gratitude to the many vendors that spent hours and days with us. The vendors provided an invaluable amount of information around the Identity Management spectrum and greatly informed our planning process.

**LEA Site Visits.** Several LEA districts graciously hosted the IAM team for visits to discuss their identity management systems. These visits were in addition to the larger statewide site interviews done by the NC Education Cloud project. These in-depth sessions have been and will continue to be immensely valuable to progress. The opportunity to meet the people and understand the systems in action greatly enhanced our research.
Executive Summary

The NC Education Cloud Identity and Access Management (IAM) Service 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 Service will have three major components: a centralized data repository with all user identity information collected in a single location, 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 authoritative 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 for 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 Service 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 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:

- 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:

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

### RttT Technology Snapshot

- **End Users (Students, Teachers, Staff, Parents)**
  - NCVPS $6M
  - IIS $24M
  - PDS
  - User Devices $25.5M
  - LEA Network $48.5M
  - LMS/CMS $10.8M
  - Learning Objects Repository $1.7M
  - Collaborative Tools $4.4M
  - Identity Management $1.2M
  - Shared Infrastructure $11.2M

**Figure 1 RttT Technology Snapshot**

---

1 “NC Race to the Top”, http://www.ncpublicschools.org/RttT/
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
- 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 service 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

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.

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.

This document provides a snapshot of the proposed Identity and Access Management architecture, system, and service. 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 to manage**
   The average student in NC currently has 4-6 accounts for accessing his/her learning resources, whether local LEA systems or cloud-based services. Teachers and other administrators on average have double that number. Most of these accounts have different usernames and passwords. As the number of accounts increase, it becomes difficult for the users to effectively manage their information in a responsible way. It also becomes difficult for technical personnel to manage/support setting and resetting passwords, and updating user account information for the various cloud services.

2. **Updating account information is a manual process**
   LEAs have described the challenging process of getting user identity information from the student and HR information systems into their local systems/services. There are two general parts to this process: (1) getting accurate, updated, and complete user information from student and HR information systems through 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 a manual process.

3. **K-12 cloud solutions growth requires a good foundation**
   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 service is one of the foundational components for a large cloud computing environment.
IAM Project Outline and Schedule

The overall IAM project will be completed in four major Phases. Each phase will have multiple tasks, sub-phases, and deliverables. It is important to understand that the IAM project will establish an Identity and Access Management service for the NC K-12 community. While the project will have major phases and tasks, the IAM Service must constantly adapt and be viewed as an on-going program with permanent resources. The scheduled timeline for the entire IAM project is October 2010 to July 2014.

Phase I – Research and Planning
Schedule: October 2010 – October 2011 (12 Months)

Major Tasks of this Phase

**Problem Definition and Scope.** Understand and clearly define the challenges of stakeholders and goals of the project. Having a clear understanding of the problems will allow us to set the appropriate scope. Don’t try to boil the ocean.

**Building Cross-Functional Teams.** Start building cross-functional heterogeneous teams to works on tasks and deliverables of the project. These teams will adapt and evolve over time, but identifying key members will be extremely important to getting project started with good momentum. The teams should include representatives from all organizations that will interface with the IAM Service.

**Identity and Access Management Research.** A deep and wide analysis should be done to clearly understand the IAM landscape. What have other organizations done with IAM, what products and services are available on the market, what are the major challenges and pitfalls of large IAM projects? These are some of the important questions that need to be investigated during the initial phase of the project.

**Defining Data Sources and Target Services.** Identity and Access Management is all about connecting users to services in an effective and appropriate manner. It is very important to understand the details and scope for both sources and targets, because it will have a direct impact on the direction, scope, and cost of the IAM Service.

**Develop an IAM Plan.** All the points above and below will be captured in an IAM plan. This plan serves as a crucial communication tool in the early phases of the project. The plan is a place to capture all information about the project, intentions, and expected results. The plan will also serve as a major anchor point throughout the project and will constantly be referenced.

**Review and Approval of IAM Plan.** The IAM plan will need to be reviewed and approved by the various stakeholders before moving to the next Phase of the project.
Phase II – Establish Service Model
Tentative Schedule: November 2011 – June 2012 (8 months)

Major Tasks of this Phase

**Project Portfolio Management.** Coordinate with State of North Carolina Enterprise Project Management Office and Project Management advisor to complete administrative details of the IAM Project per NC General Statutes.

**Formally establish IAM Policy and Governance Role.** Start establishing the advisory bodies that provide governance and oversight for the IAM Service. The advisory bodies will create the business rules that will be translated into workflow processes in the IAM Service.

**Formally establish IAM Service Manager.** Formally establish the IAM Service Manager that will coordinate and manage the IAM Service through collaboration and negotiation with the IAM Service Consumers and the IAM Managed Service.

**Formally establish Identity Data Sources, Target Cloud Services, and Federation Partners.** Formally establish agreements with authoritative data providers for necessary user identity data. Establish initial target cloud services and processes surrounding onboarding. Establish federation partners and necessary trust agreements required.

**Develop Service Plan.** The IAM Service Manager will develop a Service Plan that described the details of how it plans to deploy and manage the IAM Service for the IAM Service Consumers.

**Perform RFP for Products and Services.** An RFP process will be used to select the IAM Managed Service provider that delivers the IAM Service and all associated functions/components.

**Review and Approval of IAM Service Plan.** The IAM Service plan will need to be reviewed and approved by the various stakeholders before moving to the next Phase of the project.
**Phase III – Build and Implementation**
Tentative Schedule: July 2012 – June 2013 (12 months)

Major Tasks and Subphases of this Phase

Steps of each Subphase: Requirements | Design | Install | Configuration | System Acceptance Testing | User Acceptance Testing | Steady State


Subphase – Data Integration

Subphase – Identity Management

Subphase – Access Management

Subphase – Identity Federation

Subphase – Security Information and Event Management (SIEM)

IAM Service Pilots

Migrations

The IAM Managed Service will recommend the exact tasks and subphases here.
Phase IV – Full Production and Operation
Tentative Schedule: July 2013 – Ongoing

Major Tasks of this Phase

- Ongoing Support Model
- Ongoing Funding Model
- Ongoing Migrations for Service Consumers
- Ongoing Policy and Governance Model
IAM Benefits

The primary objective of the NCEdCloud is to provide a world-class IT infrastructure as a foundational component of the NC education enterprise. Moreover, the NCEdCloud 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.

These same benefits are reiterated in the IAM Service described in this document:

- Home institutions are responsible for reviewing and managing their users’ accounts, groups, roles, attributes and access privileges (**Security**)
- Easier and faster access to computer resources through workflow-assisted account creation, activation and maintenance – including deactivation (**Saves time and money**)
- Enables easier scaling and deployment of web-based applications to include multiple additional users/organizations (**Efficiency, scalability, saves time and money**)
- Frees users from having to manage multiple usernames and passwords (**Security**)
- More confidence that users are who they say they are, with up-to-date accuracy – assuming there is more control over issuing the Cloud account initially and that by using a single account frequently, users would notice any issues (**Security**)
- Demonstrated ability to protect electronic identities through rigorous account lifecycle management, audit and reporting capabilities. (**Security**)
- Future Ready Solutions: Once in place, DPI and LEAs can more 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**”

---

PART I

POLICY AND GOVERNANCE
Policy and Governance

At the end of the Race to the Top NC Education Cloud program, the responsibility for day-to-day operations and oversight of cloud services will transition to a more permanent body. The NC Education Cloud Work plan, approved by NC State Board of Education on September 5, 2011, describes that a support organization will establish and manage process, maintain shared infrastructure, manage LEA cooperative procurement, and support LEA use of shared services in a provider-neutral manner.

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 to 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.

At the highest level, the NC Education Cloud has oversight from the NC State Board of Education, NC e-Learning Commission, and the Governor’s Education Transformation Commission. In addition, the program will have LEA oversight from the RttT Education Cloud Shared Services Advisory Committee.

Working Groups have been formed to provide specific guidance to the major elements of the program in the areas of Infrastructure and Platform. Additional ad hoc groups may be formed to provide assistance with specific projects.

Figure 2 Organization & Collaboration
There are currently five advisory bodies for the IAM project:

1. IAM Working Group (Technical and Application Advisory)

The tasks for the Identity and Access Management Working Group will vary depending on the project phase but can be generally stated to:

- Serve as an advisory body exchanging ideas, concerns, and feedback between IAM Architects and local LEA representatives during project planning
- Provide subject matter expertise about K-12 technical system and business processes
- Define and clarify project scope based on resources and needs
- Develop policies and procedures for IAM Service

Current IAM Working Group Members are:

<table>
<thead>
<tr>
<th>Region</th>
<th>Member</th>
<th>School</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region 1</td>
<td>Jeff Smith</td>
<td>Pitt County Schools</td>
</tr>
<tr>
<td>Region 2</td>
<td>Wayne Beasley</td>
<td>Craven County Schools</td>
</tr>
<tr>
<td>Region 3</td>
<td>Walter White</td>
<td>Wake County Schools</td>
</tr>
<tr>
<td></td>
<td>Chris Withrow</td>
<td>Craven County Schools</td>
</tr>
<tr>
<td></td>
<td>Mel Cherry</td>
<td>Northampton County Schools</td>
</tr>
<tr>
<td></td>
<td>Corwin Armstrong</td>
<td>Durham Public Schools</td>
</tr>
<tr>
<td></td>
<td>Ed Chase</td>
<td>Edgecombe County Schools</td>
</tr>
<tr>
<td>Region 4</td>
<td>Jordan Walsh</td>
<td>Moore County Schools</td>
</tr>
<tr>
<td>Region 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>Region 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>Region 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>Region 8</td>
<td>Michael Thompson</td>
<td>Rutherford County Schools</td>
</tr>
<tr>
<td>Charter</td>
<td>Vacant</td>
<td>Vacant</td>
</tr>
<tr>
<td>NCITS</td>
<td>William Haney</td>
<td>NC Information Technology Services</td>
</tr>
<tr>
<td>NCVPS</td>
<td>Chanin Rivenbark</td>
<td>North Carolina Virtual Public School</td>
</tr>
<tr>
<td>NCSSM</td>
<td>Paul Menchini</td>
<td>North Carolina School of Science and Math</td>
</tr>
<tr>
<td>NCDPI</td>
<td>Vacant</td>
<td>NC Department of Public Instruction</td>
</tr>
<tr>
<td>FI</td>
<td>Sammie Carter</td>
<td>Friday Institute</td>
</tr>
<tr>
<td>MCNC</td>
<td>Steve Thorpe</td>
<td>MCNC</td>
</tr>
<tr>
<td></td>
<td>Mark Scheible</td>
<td>MCNC</td>
</tr>
</tbody>
</table>
Developing an Identity and Access Management Service

2. NC Education Cloud Shared Services Advisory Committee (Policy and Priority Advisory)

<table>
<thead>
<tr>
<th>Region 1</th>
<th>Victor Eure</th>
<th>Perquimans County Schools</th>
<th>Pitt County Schools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region 2</td>
<td>John Gilmore</td>
<td>Sampson County Schools</td>
<td>Onslow County Schools</td>
</tr>
<tr>
<td></td>
<td>Steven Myers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region 3</td>
<td>Marsha Abbott</td>
<td>Vance County Schools</td>
<td>Northampton County Schools</td>
</tr>
<tr>
<td></td>
<td>Rhonda Moses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region 4</td>
<td>Kevin Coleman</td>
<td>Cumberland County Schools</td>
<td>Moore County Schools</td>
</tr>
<tr>
<td></td>
<td>Tony Tuso</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region 5</td>
<td>Ray Reitz</td>
<td>Chapel Hill-Carboro City Schools</td>
<td>Winston-Salem/Forsyth Schools</td>
</tr>
<tr>
<td></td>
<td>Betty Weycker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region 6</td>
<td>Jerry Shepardson</td>
<td>Charlotte-Mecklenburg Schools</td>
<td></td>
</tr>
<tr>
<td>Region 7</td>
<td>Darren Hartness</td>
<td>Mount Airy City Schools</td>
<td>Mooresville Graded Schools</td>
</tr>
<tr>
<td></td>
<td>Scott Smith</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region 8</td>
<td>Monty Fuchs</td>
<td>Buncombe County Schools</td>
<td>Haywood County Schools</td>
</tr>
<tr>
<td></td>
<td>Todd Trantham</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. **Governor’s Education Transformation Commission (Oversight and Consultation)**

   In September of 2010, Governor Beverly Perdue established the 26-member Governor's Education Transformation Commission (GETC) to provide oversight and consultation on the use of Race to the Top funds and to coordinate the use of these funds to implement the Career and College: Ready, Set, Go! Initiative across North Carolina.\(^5\)

4. **North Carolina eLearning Commission (Guidance)**

   The eLearning Commission is dedicated to creating and promoting a collaborative online learning environment that promotes student achievement, business success, economic stability, and lifelong learning for every citizen of North Carolina.\(^6\)

   The Commission shall be composed of up to 30 members appointed by the Governor to serve at her pleasure for terms of two years. Commission members may be reappointed for successive terms. The persons appointed to the Commission may include representatives from educational organizations and institutions, information technology providers, nonprofits, business entities, and state and local government agencies. The Governor shall appoint a Chair and two Vice-Chairs of the Commission from the membership of the Commission.\(^7\)

5. **State Board of Education (Governance)**

   The State Board of Education consists of the Lieutenant Governor, the Treasurer, and eleven members appointed by the Governor. The Governor's appointees are subject to confirmation by the General Assembly in joint session. Eight of the appointed members represent the eight education districts of the state. Three members are appointed from the state at-large members. The State Superintendent of the Department of Public Instruction serves as secretary and chief administrative officer of the Board. The State Board also has seven advisors (non-voting): two high school student advisors (a junior and a senior, appointments made in the junior year for two-year service) appointed by the Governor; the NC State Teacher of the Year (serves two years; overlapping terms); the NC State Principal of the Year (serves one year); a superintendent appointed by the Governor (serves one year), and a local board of education member (serves one year; held by the NCSBA Raleigh Dingman award winner).\(^8\)

---

\(^5\) [http://www.dpi.state.nc.us/getc/](http://www.dpi.state.nc.us/getc/)

\(^6\) [http://www.elearningnc.gov/](http://www.elearningnc.gov/)

\(^7\) [http://www.governor.state.nc.us/newsitems/ExecutiveOrderDetail.aspx?newsItemID=1438](http://www.governor.state.nc.us/newsitems/ExecutiveOrderDetail.aspx?newsItemID=1438)

\(^8\) [http://www.dpi.state.nc.us/stateboard/about/](http://www.dpi.state.nc.us/stateboard/about/)
IAM Policy Development

In an IAM system, a major portion of the project is the work required to develop the policies and governance for the system/service. Identity management systems are simply the middleware between users and the services they access. Policies define how the users interact with the services.

Figure 4 IAM Policies

Policies, Regulations, and Rules (PRRs) that support and define aspects of the IAM Service will be created and revised as the project moves forward. The heterogeneous, cross-functional teams like IAM architects, K-12 stakeholders, and other advisory bodies will inform the development of the PRRs. The IAM Service and Implementation plans, described in the later sections of the IAM plan, will also help inform Policy and Governance. These PRRs will, however, be the responsibility of the Policy and Governance teams/committees to communicate and enforce. Proposed initial categories in which PRRs need to be defined are listed in Appendix G – Proposed Policies, Regulations and Rules. Each of these areas loosely aligns with the Requirements and Specifications and Service Model described in later sections of this document. These PRRs will eventually become more formalized with structure and process in the large NC Education Cloud context. In the beginning, however, we will be proposing PRRs in response to simple questions that need to be answered in order to make provisioning and workflow decisions.
Policies, Regulations, and Rules (PRR) Workflow

Below is a proposed workflow that describes how PRRs are developed.

A need arises for a PRR to be developed for the IAM Service.

IAM Team reviews IAM PRR need via internal discussions and NC Education Cloud Team.

IAM Working Group discusses IAM PRR need via WG Email list or scheduled WG call.

IAM PRR is proposed to appropriate level of Policy and Governance for endorsement and communication.

PRR is translated and incorporated into IAM Service as a rule, policy, workflow, etc.

Figure 5 PRR Workflow
Developing an Identity and Access Management Service

Procedures and Workflows

Procedures and workflows need to be documented and developed for known data and user access requests. Each procedure and workflow will likely have two parts: Business Procedure (the approval process) and Technical Procedure (the code). While each LEA will potentially have its own business rules, a general workflow can be derived that would be applicable to all LEAs. It is important from a Policy and Governance perspective to have appropriate separation of duties with respect to the approval of workflow requests. Particularly between the requester and approver. In some cases multiple levels of approval may be required for a request. Each step of the workflow – from request through final approval – needs to be documented (logged) for auditing purposes.

Example: A student needs access to an application for a class assignment. What does this look and feel like in the context of the new IAM system? A couple questions need to be answered: Does the whole class need access to the application or just the one student? If the former case, a rule could be developed to automatically provision access for any student that is a member of the class. If only the one student needs access, the teacher could request access on behalf of the student. The student might also be able to request access to the application himself or herself.

In either case, a workflow request would be initiated and sent to an appropriate administrator or group for approval. The administrator would determine if that application is appropriate for the student and then grant or deny the student access to the application.

Procedure 1: Granting User Access to Cloud Services and Applications

The preferred method would be through automated provisioning of access based on groups, roles, entitlements granted to users based on their attributes and affiliation(s). Manual granting of access will be considered a “special case”.

Procedure 2: Changing User Identity Information

One of the following methods could be used to change a user’s identity information:

1. Via an Administrator(s). The local LEA administrator or delegated administrator could submit the change request on behalf of the student. However, the procedure would then follow the same workflow as if a user submitted it. The request would still need to go to the local data coordinator for vetting and updating of the Source System (e.g. Student or HR system of record). Updates directly to the IAM data should never occur, since they are based on the source system data and would be over-written.

2. Self-service via the IAM Portal. A user would simply click “update my profile” and type in the correct identity information. This would initiate a workflow and send the identity
data change request to a designated individual (or group of individuals) for approval. Once the request has been approved, it would be routed to the local data coordinator who would submit the changes in the appropriate source data system. These changes would then be propagated to the IAM system during the next update cycle.

3. Manually, through a defined procedure at the local school or LEA. A user could follow the official procedures documented by his/her LEA or school, to request the identity information changes. These requests, once approved, would ultimately result in data changes being entered by the data coordinator. It is possible the IAM Portal could be configured to direct users to their documented local policies – perhaps as stated on a web page served up by the LEA.

Selection of Initial Applications and Target Systems

As the IAM system is rolled out, strategies for prioritizing those applications to onboard first will need to be developed. The final decision and communication of the applications selected should be a Policy and Governance responsibility. There are many factors that might influence these decisions, such as:

- desirability / popularity of app
- readiness of app (e.g. if it already speaks SAML, its easier than if it uses proprietary formats for which connectors aren't already built. It is also possible there are apps that will be unable to integrate with 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 the popularity of various applications (which might be onboarded), some results from the initial 40 LEA surveys are listed below. These are categorized according to application type. Percentages reflect “presence” in the LEA surveys and not necessarily the usage across the LEAs.

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

**LMS:**
- Moodle (57.5%)
Blackboard (35%)

**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 are tabulated. But the above data gives a good idea of what to expect. Google Apps (Docs) and a couple of the other more popular applications may be placed high on the priority list.
PART II

REQUIREMENTS AND SPECIFICATIONS
Requirements and Specifications Description

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

A functional requirement [FR] describes an interaction between the system and its environment as to what the system will do. “The system must…”

A nonfunctional requirement [NFR] describes a restriction on the system that limits our choices for constructing a solution to the problem. “The system must 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:

- FR1 Functional Requirement 1
  - FRS1 Functional Requirement 1 Specification
    - FR1.1 Functional Requirement 1.1
      - FRS1.1 Functional Requirement Specification
      - Examples
    - FR1.2 Functional Requirement 1.2
      - FRS1.2 Functional Requirement Specification
      - Examples
- NFR1 Non-Functional Requirement 1
  - NRF1 Non-Functional Requirement 1 Specification
    - NRF1.1 Non-Functional Requirement 1.1
      - NRF1.1 Non-Functional Requirement Specification
      - Examples
    - NTF1.2 Non-Functional Requirement 1.2
      - NRF1.2 Non-Functional Requirement Specification
      - Examples

---

FR1 Data Integration Platform

There is a common need across all the NC Education Cloud Projects and other RttT projects for a comprehensive, enterprise data integration platform. A platform for extracting, migrating, syncing, monitoring, validating, transforming, loading, and replicating data from disparate data sources to target systems in a secure manner. This integration platform is essentially an Extract, Transform, and Load (ETL) engine but has a much larger scope than just database interfaces. Most of the requirements and specifications below are applicable to the data integration needs of other Cloud projects. **As of February 2012, the NC Education Cloud has launched an independent Data Integration project that will provide services to each of the cloud projects, including IAM. This will become the mechanism for consuming identity data from authoritative sources in the future.** There are many places throughout the IAM system where these data integration functions are needed, but 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. User data will include numerous attributes about students, staff, and parents in the NC K-12 Education System. The user data needs to be profiled, processed, transformed and then fed into the provisioning component of the IAM system. In all functions of the data integration platform, measures should be taken so that active user data is not unintentionally overwritten.

---

**Figure 6 IAM Data Integration**
**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 Uniq-ID for Staff (UID) from the Department of Public Instruction (DPI) are the authoritative data sources for student data (and possibly some parent data), and staff data, respectively. 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 data integration process.

*Example:* A new user data file is generated by the authoritative data system and transferred to the Managed File Transfer Service (MFTS) at 7am. The IAM system should immediately detect that a new user file is available and start the data analysis and update process (to determine any deltas from the previous data files).

**FRS1.1 Specifications**

The IAM system will not have direct access at the start of the project to the authoritative data source systems (NCWISE and UID). 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 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 and MFTS services. 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. The MFTS file naming convention is located in Appendix H. The current data extracts field definitions for NCWISE and UID are located in Appendix I and J respectively.

*Example:* The daily extract of user data may appear in the MFTS inbox at 7am Monday through Saturday, but then appear at 1pm on Sunday instead of 7am. This is the reason for 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 secure connection interfaces. These connections could change over time as different source systems are introduced and the IAM mechanism that consumes the data must 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.

FRS1.1.1 Specifications

The MFTS provides access to the user data currently but in the future, other connection methods may be available. Therefore, the IAM system will need to have other connection capabilities besides SFTP. Only a small number of connections will be needed initially but the system must be able to support a wide variety of connections.
Other connection examples might include web service (WS) connections, like REST and SOAP, or modern database connections, like ODBC and JDBC.

Input connection interfaces such as SFTP, JDBC, Oracle ODI, SPML, LDAP. CSV and tab-separated flat file readers must also be part of the system. The IAM system shall also support a mechanism to write custom plug-ins to gather, parse, and consume input data from as yet unknown sources. The plug-in environment should support common languages such as Java, shell scripts, etc. Input events should be schedulable according to a pre-arranged schedule or triggerable, based on external events such as an input file becoming available. All user data transferred between the authoritative sources and the IAM system must be through a secure, encrypted channel.

Example: MFTS is no longer the end point for accessing the user data and we now have a direct connection to the database server. The IAM system would need to be updated to support the new connection for properly feeding user data.

Example: MFTS is no longer the end point for accessing the user data, as there is a newly available Operational Data Store (ODS) that has the necessary information. The IAM system would need to be updated to support the ODS for properly feeding user data.

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 have 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 Specifications

The IAM system must be able to connect to the MFTS system and copy/move the user identity data files to the data integration 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
Developing an Identity and Access Management Service

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 extended 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 (Data Profiling)

The Data Integration function of 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 IAM data integration component checks, and 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.
Developing an Identity and Access Management Service

FRS1.3.1 Specifications

The IAM system will ...

TBD – Still waiting to get all the input data before we can complete the specifications

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 since it is likely 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 one of the authoritative data update cycles, 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.

FRS1.3.2 Specifications

The IAM system will ...

TBD – Still waiting to get all the input data before we can complete the specifications

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 set. 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 UID 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, Timestamp of last modification, Originator of modification

b) Parent Data from NC WISE: TBD – Still waiting to get all the input data before we can complete the specifications
Developing an Identity and Access Management Service

c) Staff Accounts from UID: UID_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

**FRS1.3.3 Specifications**

The IAM system will ...

TBD – Still waiting to get all the input data before we can complete the specifications

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

The Data Integration function of the IAM system must have the ability to determine deltas or changes between updates of user identity data. Assume the authoritative sources do not have the ability to distribute only changes in the user data.

*Example: If the system consumes user identity data at 10am and a single field/record changes with a student’s address, when the system consumes the user identity data again at 11am, the system must be able to detect that single changed record, and then update only the changed address.*

**FRS1.3.4 Specifications**

The IAM system shall be able to determine deltas between successive inputs from authoritative data sources (e.g. NCWise, UID) 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.

**FR1.3.5 Identity Matching / Joining**

The IAM system must match and join user data records as appropriate from disparate authoritative data sources 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 user affiliation (e.g. students, parents, employee, and guest) based on which system(s) of record the identity is a part of or as a result of System of Record attributes.

*Example: An individual is a parent in the Student System or the Guest Registration 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 multiple roles which reflect the systems of record where it exists, e.g. “parent” and “teacher”.

FRS1.3.5 Specifications

The IAM system will ...

TBD – Still waiting to get all the input data before we can complete the specifications

FR1.4 User Data Loading

The Data Integration process must consume user data from various heterogeneous systems and load that 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. **All user data transferred between the IAM system and target systems must be through a secure, encrypted channel.**

*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 Specifications

The IAM system will...

TBD – Still waiting to get all the input data before we can complete the specifications

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 during identity repository updates. Processing changes (deltas) from the source data is the first step in the process and it is important to alert support personnel if there are any errors 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 alerted via some method.

**FRS1.5 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 administrator 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 used to update the system. The administrator(s) should be notified of this issue in an easily understandable format: 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 data integrator tool for the IAM System must support a broad set of platforms and provide an open architecture that supports multivendor IT infrastructures.

**Example:** The data integration tool of one vendor must talk to directories of competing vendors.

FRS1.6 Specifications

The IAM system must support direct out-of-the-box integration with the most common directory Systems, e.g. Active Directory, LDAP v3, Novell eDirectory. The IAM system data integrator should support customizable extensions that enable unique API integrations with uncommon identity systems when not supported by out-of-the-box integration.

The IAM system data integrator must support scripting interfaces, supporting the CRUD model, to support unique requirements for non-standard data manipulation.

**Example:** If certain role based authorizations are missing from data, these roles could be corrected through a script.

**Example:** A requirement might exist to interface with Oracle eBusiness suite only accessible via programmable API. Given the API is open, a new connection could be developed based on the extensibility of the data integrator tool.

FR1.7 User Interface

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

**Example:** Simple portal for delegated administrators and end users to access identity records.

FRS1.7 Specifications

The data integration tool should provide a web-based console and command line interface for the administration and development of the integration rules. Using a web portal to define synchronization rules at the attribute level, with the ability to combine data elements to create a distinguished name for a directory, based on attributes in the identity object.
Including the following:

- Viewing the current state of identity objects
- Viewing the applied synchronization rules on an identity object.
- Creating new synchronization rules
- Creating new workflow rules
- Developing identity policy rules
- Defining the sets of objects for which a policy is applied, or the permissions (CRUD) on objects.

*Example: If…*

**FR1.8 Identity Data Retention**

The IAM system must retain the user identity data in its original format for a certain period of time, as defined by the policy and governance body. This is the identity data consumed from the authoritative data sources prior to any transformation made during the data integration process.

**FRS1.8 Specifications**

The data integration process must store copies of the original input data files in a format sufficient for later retrieval, upon request of the IAM Policy and Governance bodies or other authorized parties.
FR2 Manage Identities

One of the cornerstone functions of the IAM system will be the ability to perform User Identity and Account Lifecycle management. The identity management component of the IAM system will provide this function by managing user identity data groups, roles, sponsor(s), and entitlements for students, parents, staff and community members. The identity manager, through the data integration platform, consolidates and reconciles identity data from disparate systems of record into a central system, to provide a single electronic instance of a person.

![Figure 8 Manage Identities](image)
FR2.1 User Source Data Integration and Reconciliation

In addition to the data integration component described in the previous section for authoritative sources, the IAM system must perform account reconciliation between the internal identity manager user records and user records already provisioned in cloud service systems. This process ensures that there are like accounts (matches) between systems. Orphaned accounts – those that exist only on the Cloud Service side – will need to be disabled or reviewed to see what action needs to be taken.

Example: An LEA is already providing GoogleApps or Microsoft Live@EDU services to its user community, prior to joining the NC Education Cloud. 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 IAM.

FRS2.1 Specifications

The account reconciliation function will likely be used a tool during the initial onboarding of cloud services and migration of LEA systems to the IAM system. There may be a need to reconcile accounts from some local LEA directory systems and other local guest registration systems. A deduplication process must also exist to identify and prevent multiple records from being created for an individual. An administrative interface or duplicate record report must be available to allow for manual review of potential duplicate records that cannot be resolved systemically. Views of the data are then made available to service providers and application developers to determine access.

Example: An LEA already has guest registration systems but would like to migrate those accounts to the new IAM Service. The IAM system may need to reconcile those user records and perform any necessary transformation before incorporating them into the central repository.
FR2.2 User Management

The IAM System should automatically create a base set of roles, groups, and entitlements for each identity, based upon policy settings and each user’s identity data. The creation of these value-added attributes are part of the core provisioning function of the identity manager component. Some vendor products deliver this functionality in an Access Manager component.

FRS2.2 Specifications

This will require development of a standard set of roles, groups, memberships, entitlements and policies that are agreed to by all LEAs. These will be automatically assigned or provisioned to users based on defined criteria. The standard set has not yet been developed; we expect this to occur during the early Build and Implementation phases of the project. Possible examples are described below.

Example: A rising 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, Grade 10, Durham Public Schools, and high school students 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 teachers 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
FR2.2.1 Separation of Duties

The IAM system must support separation of duties. Separation of duties prevents and detects conflicts in roles or entitlements.

Example: A teacher (who is also the designated volunteer coordinator) wants to create a Guest Account for a community member who is volunteering in his class. He enters a request for the user’s account, which would then go to the volunteer coordinator for approval. Since the IAM System workflow recognizes the requester and approver would be the same individual, it is elevated to the next lever of authority for approval (e.g. the school principal).

FR2.2.2 Entitlements

The IAM system must support entitlements. Entitlements are a more direct mechanism for granting an individual access to applications and services without using role- or group-based access controls. For example, entitlements are well suited for “one-off” approvals of access for individual community members. Additionally, some applications might be designed to look for an entitlement attribute more easily than checking for groups or roles.

Example: All teachers and students are allowed to use certain licensed library services. Rather than checking what role or group membership a user might have to determine access, the library service can simply look for an entitlement of “library services user”.

FR2.2.3 Role Management

The IAM system must support role hierarchy management. Role management represents a collection of users and their permissions. A parent/member role relationship can help automated access rights through the notion of inheritance between roles. Care should be taken, however, to consider the context of the user session when permissions might be inherited. An individual who is both a parent and teacher should ONLY have the permissions associated with the task being performed.

Example: A teacher needs to enter grades for her students, but should not have access to change her own child’s records. If parents are not allowed to view their children’s grades online (but only update contact information) then a parent who is a teacher should have the same limited permission set.
Developing an Identity and Access Management Service

**FR2.2.4 Role Modeling and Mining**

Role modeling and mining is a desired feature of the IAM System.

*Example:* The IAM system role miner function observes that administrators are granting the same permissions for many users of the same role. The role modeler would make a recommendation to create a group of those roles and make the actions again the group instead of each role. It provides greater efficiencies for IAM governance, enhanced control, and automation.

**FR2.2.5 Group Management**

The IAM system must support group management for users and their roles.

*Example:* All the teachers' roles within the IAM system could be grouped together into a single group called NC Teachers. The actions can be taking against the whole group instead of making the changes to each teacher role.

**FR2.2.6 User Attestation**

The system shall have functionality to allow managers and supervisors the ability to review access granted to their employees, and approve or reject continued access. This attestation process should be schedulable to automatically take place on a set schedule (e.g. annually, bi-annually, etc.).

**FRS2.2.6 Specifications**

The system should be able to generate online or printed reports describing 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 by either of these reviewers, the entitlement for that user will be revoked.
FR2.2.7 Deactivation of Identity Records and Accounts

The IAM system shall have functionality to deactivate user identities in the central identity repository (when an individual no longer appears in the Authoritative Source data). The system must also have the ability to automatically notify (report) and deactivate accounts after a set period of inactivity.

FRS2.2.7 Specifications

De-activation should occur automatically, based on the status of a student or employee in the System of Record (e.g. when a pre-assigned expiration date or status has been reached). It could also occur manually, as entered by a designated administrator of the IAM system for that LEA, or as entered by the sponsor of a guest account. Upon deactivation of the user record, the IAM system shall de-provision any associated accounts (e.g. Central Directory Accounts, Service Provider accounts), yet maintain the deactivated record in the system.

Example: The school year ends, and a senior graduates. The student record in the system associated with the graduated senior will be automatically deactivated. This may take place at the end of the year, or at the beginning of the following year (when the student’s record has no current school, LEA, grade level, etc.) At that point, the IAM system will deprovision any associated accounts and de-activate the identity within the system.

FR2.3 Provisioning and Deprovisioning Engine

The IAM system must provision and de-provision identity data and accounts to/from external systems, in an automated fashion where appropriate based on policy. This could include best practices 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. In addition, provisioning directly to some local LEA directories may be enabled at a future time.

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.
Developing an Identity and Access Management Service

**FRS2.3 Specifications**

Interfaces should be described in the following manner:

Connectivity:
Server Name:
Domain Name
Authentication Type (domain credentials, username/password,Kerberos)
Interface Type
Software Version
Unique Identifier attribute(s)
ObjectType
AttributeName
AttributeType
Example value
Constraints (e.g. list of values, min,max range, etc)

**FRS2.3.1 Central Directory Provisioning**

The IAM system must provide a centralized directory with accounts provisioned from the data in the Central Identity Repository. It must be updated as user records are added, changed or disabled. The Central Directory must store and manage identity, credentials (username/password combinations), group, role, sponsor, entitlement, and related attributes, 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 deactivated when a sponsor leaves the organization (school).

**FRS2.3.1 Specifications**

1. Implement core functions to add, modify, and remove groups, identities, roles, entitlements, and group members.
2. Support the storage of credential metadata (username, password, last password change time, etc.)
3. Record all changes applied to central identity manager records, in a form/location suitable for subsequent searches of those change records.

*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 on a “need-to-know” basis.
Developing an Identity and Access Management Service

FR2.3.2 Cloud Services Provisioning

Provisioning a Cloud Service for a user can be viewed in two ways - by either directly provisioning a new user account into the service site, or by creating an entitlement or granting a role or group membership to the user (which is used by the service to determine access).

Many of the issues related to this topic are covered in an appendix rather than here. Information was separated out into an appendix to enable easier sharing with application owners. Please see “Appendix D – Requirements for Integrating Cloud Applications.”

FR2.4 Delegated Administration

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. Manual and exception local group, role, membership, and entitlement management
2. Reset user passwords
3. Disable accounts (e.g. emergency, security)
4. Create system usage reports
5. Download LEA-specific data
6. Add and deactivate Guest (sponsored) accounts

FRS2.4 Specifications

This will require development of the base set of local roles, groups, memberships, and entitlements which may 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.

FR2.4.1 Group, role, membership, and entitlement management

The IAM System shall provide authorized administrative users the ability to create and manage where appropriate, customized groups, roles, memberships, and 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.

**FR2.4.2 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.

**FR2.4.3 Disable accounts**

Authorized personnel must have the ability to disable/deactivate accounts for users within their organizational realm.

**FR2.4.4 Create system usage reports**

Authorized personnel must have the ability to create reports of IAM system usage by users within their organizational realm. For further information, please see the section titled “FR4 Security Information and Event Management (SIEM).”

**FR2.4.5 Download LEA-specific data**

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

**FR2.4.6 Add and delete guest accounts**

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

Example: Accounts might need to be added to the test environment and 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.

Example: In certain situations, authorized personnel may wish to initiate a guest account setup through the Guest User Self Registration system described elsewhere in this document. In this case, the authorized personnel could enter the guest user’s information on behalf of the guest user.
FR2.5 User Self Service

The IAM System must provide a self-service function to allow users to change/reset their password (as described previously), update contact information, and request access to services not dynamically assigned. 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.*

**FRS2.5 Specifications**

TBD ...

**FR2.5.1 Self/Guest Registration**

The IAM system should have capabilities to allow sponsor-approved user self-registration and data updates in the identity manager. Typically this would be utilized by newly registering community members, parents, or a user’s sponsor(s).

**FRS2.5.1 Specifications**

The guest user self-registration system should be presented using simple, intuitively easy-to-understand web-based interfaces.

The interface should enable data entry on the registrant such as:

- Type(s) of affiliation: e.g. volunteer, community member, parent/guardian
- Associated LEA(s) (if more than one associated LEA, one of them should be identified as primary)
- Associated School(s) (it is possible more than one school could be associated with a guest user)
- Primary email address
- Secondary email address
- Home phone number
- Cell phone number
- Work phone number
- Mailing Address
- Initial password
- Is the guest user also a staff member?
- **If the guest is a staff member:**
  - The staff member’s work email address (may not be allowed by LEA policy)
  - Associated LEA(s)
  - Associated School(s)
Developing an Identity and Access Management Service

- Sponsor name(s) or institution (if applicable – could be more than one sponsor)
- Sponsor email address(es) (if applicable)
- Requested account duration (optional)
- Comment field (optional)
- If the guest user is a parent/guardian, for each student:
  - Name (First, Last – cn, sn)
  - NCWiseID
  - School
  - LEA
  - DOB

Self-registration requests should first confirm each of the user-submitted email addresses, via an email exchange workflow with those addresses. Each address will receive an email from the system, and upon receipt the user can reply either by email or by clicking a link. The reply confirms the email address is valid and associated with the self-registration request.

Next, the self-registration request process should notify the sponsor (possibly by email), who can then approve or deny the request. Depending on the policies of the individual LEA and the type of affiliation (e.g. parent, community member), approval may first require in-person verification by the sponsor, the school, or the LEA. 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.

The interface should also enable subsequent data updates by the registrant, after the initial account has been granted. For example, the registrant may return later to update the information on his/her children, address, phone numbers, etc. Subsequent data updates should be routed through the existing sponsor for approval, prior to propagation through the system.

The Guest system would essentially be a system of record for non-students and staff. Identity records created here would need expiration limits and sponsorship, so that deprovisioning of the user account and access (in the central directory) would automatically occur when the time limit expires.

Staff members who are also parents would exist in both the HR and Guest systems. They would have a single entry in the Central Identity Repository and most likely a single account, but with multiple roles/affiliations. Access rules would need to be carefully constructed to prevent these individuals from accessing data they are not entitled to as a “parent” (e.g. if their children attend school in a different LEA than where they are employed).
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 if required by the LEA’s policy, verifies in person with Joe Smith on the validity of the request. (Most likely, this request would require an additional level of approval beyond Duffy Brown). Duffy next 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.

Example: Mr. John Doe is a parent of Sue Doe and John Doe Jr., students at Bratwurst High School in the Germantown LEA. Mr. Doe is also an English teacher at the Oscar Meyer Middle School, which is also in the Germantown LEA. Mr. Doe registers as a parent, also entering his children’s’ information, his personal email addresses, his status as a teacher at the Oscar Meyer Middle School in the Germantown LEA and other personal information. Workflows are kicked off for approval by the registrars at the Oscar Meyer Middle School (who must vet Doe’s parent status) and at the Bratwurst High School (who must vet Doe’s staff member status). Once all appropriate vetting is done, access to additional “parent” services is added to John Doe’s account.

FR2.5.2 Password Reset
FR2.5.3 Access request
FR2.5.4 Update Identity Profile

FR2.6 Credential Management

The IAM system must provide a mechanism for users to choose an initial password or assign an initial password and communicate it to the owner, enforce password policies, and 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 his/her initial password. Password policies might include which combinations of characters would be considered valid, reuse of passwords (history), and expiration dates.
Example: The same application could later be visited by the user, when he/she wishes or needs to update his/her password.

**FRS2.6 Specifications**

The IAM ... TBD...

**FRS2.7 Directory Services**

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

**FRS2.7 Specifications**

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.

For the interested reader, the following diagram shows the variety of directories used by the various districts in the state, per the latest site survey results as of 9/15/2011.
Developing an Identity and Access Management Service

Directory Environments Used by LEAs

Figure 9 Directory Environments Used by LEAs

FR2.8 Workflow and Policy Engine

Workflows will be used to automatically request and approve changes to a user’s identity data (contact information) and their ability to access services. Workflows will be required to have requestor and approver security groups, with approvers at multiple levels as needed (school, district, cloud, manager, etc).

Examples of workflow requests may include: approval of change requests such as roles, entitlements, etc.; provisioning and deprovisioning varying levels of access to systems and resources as appropriate; managing guest 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.

FR2.8 Specifications
TBD...
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, staff, parents, and guest community members. The login/password will grant access to all authorized cloud-based applications. 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.

Figure 10 Manage Access
FR3.1 Reduced Sign On (minimal requirement)

The system will provide user experience of reduced sign on at minimum. Reduced Sign On means that an end user would still use the same username and password to access all cloud services but may have to login to each application separately.

**FRS3.1 Specifications**

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 (SSO) – the user only needs to enter their login / password once, and they’re granted access to all supported web-based applications.

**FRS3.2 Specifications**

Single Sign On could be achieved with a Federation approach using SAML or with a Reverse Proxy type approach.

*Example: Assume IAM system has several cloud services integrated and using Single Sign On. An LEA user has successfully authenticated with the IAM system and is using Google Apps. If you user decides to use Microsoft Live@EDU, then the user will seamlessly start using the application without having to login again.*

**FRS3.2.1 Single Log Out**

Along with Single Sign On, a user should also have a single logout experience. When a user logs out of one cloud service, it will automatically terminate the session for other applications using the same session.
Example: Assume IAM system has several cloud services integrated and using single sign on. An LEA user has successfully authenticated with the IAM system and is using Google Apps and Microsoft Live@EDU. When the user logs out of Google Apps, the session they are using for Microsoft Live@EDU is also logged out or terminated. If the user attempts to use Microsoft Live@EDU after logging out of Google, they would be prompted to login and start a new session.

FR3.3 Enterprise Single 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 a domain-provided rather than a local account.

FRS3.3 Specifications

TBD.

FR3.4 Authentication Protocols

The IAM system shall support authentication through multiple protocols.

FRS3.4 Authentication Protocols Specifications

Supported protocols for authentication should include web-services APIs (REST and SOAP based), plus broad support for web technologies including Java and PHP, SAML 2.0-based identity federation and interoperability with Shibboleth.

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 Specifications

TBD.
FR3.6 Policy-based Access Control

Access to identity data shall be limited to only authorized users, and LEA-specific data shall not be released to anyone outside that LEA. This is enforced through the use of roles, group membership and/or specific attribute values (e.g. LEA, School, Affiliation).

FRS3.6 Specifications

TBD.

FR3.6.1 Entitlement Based Access Control

FR3.6.2 Group Based Access Control

FR3.6.3 Role Based Access Control

FR3.7 Identity Federation Support

Identity federation technologies allow multiple organizations to share their digital identity information with shared resource providers. In a federated system, participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and enabling 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 authenticates the user and has access to a limited set of identity attributes – 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 evaluated 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)\(^{11}\) and by the open-source Shibboleth\(^{12}\) software.

**FRS3.7 Identity Federation Support Specifications**

The IAM System must provide SAML2.0\(^{13}\) 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.


\(^{13}\) [http://saml.xml.org/saml-specifications](http://saml.xml.org/saml-specifications)
FR4 Security Information and Event Management (SIEM)

As with the Data Integration platform services, many NC Education Cloud projects and other RttT projects have a common need for a centralized security information and event management system. The IAM system must be able to utilize a SIEM tool to centrally collect, store, analyze, and report on log data from all its internal components. This tool is needed for centrally monitoring, auditing, and reporting on user activities. This tool will be used for compliance management and create awareness for insider threats.

A set of standard reports must be available, with the ability to create customized, ad-hoc reports where appropriate. Centralized logging mechanisms may be used to support this process.

This ability will help ensure user access privileges granted to all services 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.

The use of, and responsibility for, SIEM monitoring and reporting will most likely exist outside of the IAM Service Provider role in a Cloud Security and Compliance group.
FR5 IAM 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:

- 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

*Example:* We have seen some software inside organizations that have functionality restricted so only the vendor is allowed to modify certain attributes/functions. These functions would require the customer to reengage the vendor for support or changes. The IAM System will not have any such restrictions.
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 UID authoritative data sources.

NFRS1 Identity Data Design Specifications

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

The IAM system must efficiently support millions of identities from 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. The IAM system will start with around 3 million users and would need to support up to 10 million entries.

Any platform providers must be able to provide evidence of previous successful IAM deployments of this scale and scope. Any products/services will need to provide information related to large profile performance testing.

Any systems integrators or affiliated partners associated with the software solution must be able to demonstrate competency and evidence of an IAM deployment of this scale and scope.

NFR2.1 Concurrency

The IAM software solution should be able to scale such that the number of concurrent users could equal the number of accounts with appropriate supporting infrastructure. There must be no restrictions inside the software solution that would limit the number of concurrent users on the system.
NFR3 Flexibility, Modularity, and Minimum Dependencies

The IAM system must be designed and architected to be 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 IAM Service Consumer – Cloud Services and the IAM Service Provider.

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 UID 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.
**NFR4 High Availability and Disaster Recovery**

The IAM system must be designed and implemented such that single component failures or planned maintenance events will result in a minimum service disruption. All scheduled maintenance activities will be planned, approved, and communicated well in advance. Also, any schedule downtime must be aligned/coordinated with LEA (Service Consumer) maintenance windows. It should be noted that LEAs have different schedules and a maintenance schedule for one LEA might not work for another.

**NFRS4 High-availability Design Specifications**

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.

**NFR4.1 Platform Environments**

The IAM system must have a minimum of three IAM system environments established. One environment would be used for testing, development, and general sandboxing. The second will be preproduction/staging environment configured in a highly available design to match the full production environment. The full production system will be the main environment that all users interface with.
Developing an Identity and Access Management Service

NFR5 Portal/Dashboard/Launchpad

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

After observing the various IAM services and products on the market today, we have determined that, in general, the user interfaces presented are not at the level/needs for our end user community. Therefore, the concept of a portal/dashboard/launchpad has been introduced to bridge the gap for our end users and the central IAM system.

At its core, the portal is a simple, clean, contemporary webpage that communicates with the IAM components via its APIs.

The portal must provide an integrated Web-based interface that includes simple links and wizard-based guides for delegated administrators and end-users. These links and wizard-based guides are based on the administrative functions found in the various IAM components that users might need to interact with.

The end users must be comfortable with IAM system and their user functions need to align with K-12 business processes.

NFR6 Change Management and Messaging

The IAM system will have many different interactions with various source systems, target systems, user communities, and other affiliates. These interactions drive the need for solid communication/messaging and change management processes. The IAM system must have comprehensive and efficient messaging and change management processes. All of the affected entities should be notified and made aware of changes within and associated with the IAM System. IAM Service Consumers should receive only information that is relevant to them, when needed and appropriate.
Developing an Identity and Access Management Service

NFR7 IAM System Performance

The IAM system is expected to sustain a certain operational performance level. The backend components of the system are expected to consume and process user data within certain time frames. The user experience must operate within certain performance parameters. At this time, the required information is not available to describe the specific performance parameters of the individual component or the system as a whole. However, the IAM system and its components will be compared to each component’s/product’s documented performance profiles. The performance specification and metrics will be documented, as the necessary information is available.

NFR8 IAM User Accessibility

The IAM System user facing components must comply with relevant ADA regulations, Section 508 Amendment to the Rehabilitation Act of 1973, and align with the Web Accessibility Initiative (WAI) guidelines of the World Wide Web Consortium (W3C). The IAM Systems must also support International Language for user facing components.

NFR9 Policy Support

Advisory bodies will provide oversight in terms of policies, rules and regulations surrounding the support, maintenance, and configuration of the NC Education Cloud Identity and Access Management System. It will provide information to provisioning rules, workflows, processes, governance and data access issues for each of the major components of the system. The purpose of these bodies is to provide a governing structure for a sustainable system. The IAMS system must be flexible enough to adapt to the advisory body’s requirements as they are developed and adapted over time.
Developing an Identity and Access Management Service

IAM High-Level 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.

The following figures 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 11: NC Education Cloud’s Major IAM Components
Developing an Identity and Access Management Service

Figure 12a: NC Education Cloud - User Account Provisioning
Developing an Identity and Access Management Service

Figure 12b: 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.

NCWISE Coordinator
HRMS Coordinator
NCDPI MFTS System
IAM System MFTS Endpoint

Step 1: NCWISE and HRMS Coordinators manage users' information as normal. The users are provisioned in IAM and granted access to new Cloud services and current LEA services.
Developing an Identity and Access Management Service

Figure 13a: NC Education Cloud - Local LEA and IAM Directory Integration

Figure 13b: NC Education Cloud - Local LEA and IAM Directory Integration Details
Developing an Identity and Access Management Service

Figure 14: NC Education Cloud - IAM System - Big Picture
Figure 15: NC Education Cloud - User Experience

1. User logs into a cloud service once
2. Cloud service passes user request to IAM for authentication
3. IAM passes user authorization information back to cloud service

User granted access to all relevant cloud services
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 16: NC Education Cloud - IAM Policies
PART III

SERVICE MODEL
IAM Service Model Overview

Through a substantial research and planning effort, we have a good understanding of the identity management challenges in K-12 and know what the design and architecture of an IAM system should contain (IAM Project – Phase I). Now we need to describe a model for supporting and managing the service in a sustainable manner that continuously brings value to the stakeholders. We begin by describing the strategies used when forming the IAM Service Model (IAM Project – Phase II). Next, it is important to understand the participants in the Service Model. We discuss each of the service roles and their characteristics.

Strategic Principles

Throughout the service model section we will be describing the different aspects of supporting and managing an IAM Service. There are some common principles applicable to each.

**Sustainability.** It is very important that the IAM system/service be designed, built, deployed, and managed in such a way that is functionally and economically sustainable for many years to come. Earlier in the IAM architecture plan, we discussed details around minimal dependencies, modular design, and redundant systems. This theme will carry over into the Service Model. Looking at each component of the service model individually but also holistically (even outside of the IAM project), will allow us to create a sustainable system and service.

**Value.** In addition to being sustainable, is important that the central system and service continuously bring value to the stakeholders and consumers.

**Purpose.** All planning for this project ultimately connects back to the purpose/vision of the IAM Service and the NC Education Cloud. From the beginning, the project has set out to solve three challenges faced by the K-12 community: too many accounts, common access to user identity data, and as a solid foundation for other cloud services. The Service Model will continue to support efforts to address those challenges.

**Community.** A system of this scale and scope requires an enormous amount of planning to be successful. Most of the planning work includes countless interactions with the variety of organizations that will ultimately play a role in the IAM Service. Getting the community involved in the planning process has increased the accuracy of requirements/specifications and created the best alignment with business processes while bringing new value to the community. This also confers ownership of the IAM system/service to the communities that it serves.
Policy and Governance. There are many different components and organizations that contribute to the IAM system/service. It is important that a well-defined policy and governance model be in place that clearly defines how those components and organizations work together to effectively deliver the sustainable and valuable service.

Measures of Success. Each step of the Service Model will clearly define measurable points, priorities, and acceptance criteria. By defining these at each step, we have success indicators and criteria to know when each step has been completed.

Scope. The IAM Service has a well-defined scope, is achievable, and promotes value to the stakeholders. The project scope lays a good foundation to continuously build upon with new and additional features around identity management.
Developing an Identity and Access Management Service

IAM Service Roles

The IAM system will be implemented and deployed as a service to the LEA community, among other consumers. The IAM service is composed of five service roles. Each role is a collection of different organizations that will serve a function in the IAM system/service. These organizations will work collaboratively (purple arrows) but have distinct responsibilities in building, deploying, and managing the IAM Service.

Next, we will describe the service roles, expectations, and general responsibilities for each.
IAM Policy and Governance Role

IAM Policy and Governance is a collection of heterogeneous, cross-functional advisory bodies that oversee, support, and “create and endorse policies”, to ensure an effective and efficient IAM system and service. The current bodies are the IAM Working Group, NC Education Cloud Team, NC Education Cloud Advisory Committee, NC eLearning Commission, Governors Education Transformation Committee, and NC State Board of Education. In the future, these advisory bodies may change as the NC Education Cloud project ends and the responsibilities/oversight transitions to an Education Service Agency.

Service Roles Partners: IAM Data Sources, IAM Service Manager, IAM Service Consumers

The IAM Policy and Governance bodies will be provided:

- Periodic reports about the IAM Service by the IAM Service Manager describing service progress, issues, successes, funding status, future plans, and recommendations
- Federal or State required reports
- Advice on what policy decisions are needed for the effective delivery of the IAM Service
- General feedback from the IAM Service Consumer about the quality of the IAM Service provided, including support
- Advise on what policy decisions are needed from the IAM Service Consumer

The IAM Policy and Governance will be responsible for:

- Developing, Updating, and Maintaining a Policy and Governance structure for the IAM Service that services the needs of the IAM Service Consumers
- Developing and defining policies and procedures needed for IAM Service
- Defining and Refining the IAM Service Roles
- Providing requirements to IAM Service Manager for the IAM Service needs
- Providing input and review of IAM Managed Service Contracts
- Serve as a configuration control board for the IAM Service components
Developing an Identity and Access Management Service

- Serve as an IAM Vision Group for shared decision-making and priority setting
- As necessary, diplomatically work with different personalities among constituents to achieve end goals and keep project/service moving forward

As mentioned earlier, each of the service role organizations will work collaboratively but have distinct responsibilities. The chart below shows the authoritative relationships between the services roles, in the context of the IAM system.

![Figure 18 IAM Service Roles Authoritative Relationships](chart)

The IAM Policy and Governance role members are the ultimate authority bodies that give direction to the IAM Data Sources, IAM Service Manager, and IAM Service Consumers. This direction will come in different forms depending on the originating body and nature of the communication. It is important to note that each of the service roles will have representatives in Policy and Governance. The IAM Managed Service will take its direction from the IAM Service Manager as granted by the IAM Policy and Governance bodies.
IAM Service Manager Role

The IAM Service Manager is an organization that serves as an intermediary between all the IAM Service roles. The current market offerings for IAM Systems do not align well with the IAM Service Consumer needs and the IAM Service Manager will serve to bridge any gaps that exist, to enable a more complete user experience.

Service Roles Partners: IAM Policy and Governance, IAM Data Sources, IAM Managed Service, IAM Service Consumers

The IAM Service Manager will have the following qualifications:

- Education Community Focused
- Previous experience delivering state-wide services as a K-12 Service Provider/Manager
- Excellent history of customer service in the K-12 community
- Understand K-12 Users and Business Processes and Business Cycles

The IAM Service Manager will be provided:

- Requirements from IAM Policy and Governance (and IAM Service Consumers when appropriate)
- Policy rules/decisions/endorsements from IAM Policy and Governance
- Documentation and Knowledge Transfer from the IAM Managed Service
- Payment/Funding for the delivery of the IAM Service Manager functions

The IAM Service Manager will be responsible for:

- Managing a statewide IAM Service to the IAM Service Consumers as specified by the NC Education Cloud and other advisory bodies
  - Pilot then Production – phased approach
- Responsible for management of the IAM Managed Service provider relationship
- Establishing relationships and coordinate as needed with owners of authoritative source data systems
• Providing technical support services and a help desk (may be part of a larger NC Education Cloud Help Desk), to the IAM Service Consumers for matters related to the IAM Service

• Ensuring the implementation and support of policies defined by IAM Policy and Governance bodies

• Providing technical and strategic guidance to the IAM Policy and Governance bodies about any necessary policies that are needed to help the IAM Service Manager deliver and support a better IAM Service for the IAM Service Consumers

• Coordinating with IAM Managed Service provider to translate IAM Service Consumer and/or IAM Policy and Governance requirements into enhancements or corrections for the IAM Service

• Coordinating with IAM Managed Service provider and IAM Service Consumers to onboard/integrate new Cloud Applications, Resources, and Services

• Providing to IAM Service Consumers and IAM Policy and Governance bodies any reporting and audit information as needed (may be provided by a Cloud Security and Compliance group)

• Providing training and documentation to IAM Service Consumers as they onboard and use the resources/services provided by the IAM Service

• Tracking user suggestions for improvements, features, and developing the methodology for IAM system enhancements

• Developing metrics and report on the impact of IAM on the Service Consumers to IAM Policy and Governance where appropriate

• Communicating new IAM Service features to appropriate IAM Service Consumer participants

• Managing vendor churn for IAM Service components

• Managing vendor contracts and developing acceptance criteria for each checkpoint of a contract
IAM Data Sources Role

The IAM Data Sources are the authoritative systems that contain K-12 user data to be populated in the IAM system. The source systems are currently centrally located at and maintained by the NC Department of Public Instruction. The IAM Service Manager will coordinate with DPI and Managed Service provider to transfer required user data from the source systems to the IAM system.

Service Roles Partners: IAM Policy and Governance, IAM Service Manager, IAM Managed Service, IAM Service Consumers

The IAM Data Sources will have the following qualifications:

- Standardized data integration interfaces and methods
- Products / services with documented APIs for data extraction

The IAM Data Sources will be provided:

- Notice / messaging about IAM Service Maintenance
- Appropriate requests for necessary data sets and fields needed in accordance with data source policies
- Feedback regarding data source feeds including any data irregularities

The IAM Data Sources will be responsible for:

- Supplying required user data sets and attributes at the specified frequencies to the IAM System
- Supplying support for user identity data and authoritative source systems
- Change management notifications of identity source systems, identity data structures, or formatting standards
IAM Managed Service Role

The IAM Managed Service is the organization(s) that provide the necessary technology components that compose the IAM service and technical support for managing the components. These could be software vendors, technical product architects, systems integrators, and/or infrastructure hosting providers. All these components put together will be presented as a single service from a single vendor / organization.

Service Roles Partners: IAM Policy and Governance (indirectly), IAM Data Sources, IAM Service Manager, IAM Service Consumers

The IAM Managed Service will have the following qualifications:

- Access to internal vendor support and development groups
- *Common Criteria Certified for IAM Software Components*

The IAM Managed Service will be *provided*:

- Payment/Funding for IAM Components and Services provided to the IAM Service Manager
- Requirements and Specifications from the IAM Service Manager
- Expectations, Rules, and Policy surrounding the IAM System’s user information

The IAM Managed Service will be *responsible* for:

- Providing to the IAM Service Manager the IAM System as a Service
- Providing the necessary cloud-hosted infrastructure, that is required by the IAM system software components, along with technical support for services provided
- Providing the service, maintenance, and operational support for the software and infrastructure components
- Performing the initial design and implementation of the IAM system as specified by the IAM Service Manager and IAM Policy and Governance bodies
- Providing the initial IAM application administration and configuration, with the possible transfer of this responsibility over time, to the IAM Service Manager, as the system matures
• Knowledge Transfer and Documentation about IAM Service components to the IAM Service Manager

• Providing recommendations on the numbers and skillsets of staff to support the IAM Service through implementation and ongoing production

• Perform data profiling and transformations of source systems data extracts

• Perform integration and target system application onboarding to IAM System

Managed Service

- **Data Match & Merge**
- **Person Registry**
- **Provisioning of Accounts**
- **Authentication/SSO**
- **Authorization**
- **User Directory (LDAP)**
- **Directory data -> LEAs**
- **Access Management**
- **Provisioning of Access**
- **Federation**
- **User Self-Service**
- **Guest System**

- **Delegated Administration**
- **Audit Logging, Reports**
- **Ongoing Support and Administration**
  - **Provisioning Rules**
  - **Request Workflows**

- **Application Onboarding & Integration with Service**
  - **All HW & SW support**
  - **Systems Integration**
  - **Vendor Technical Support**

**SW Vendor**
- **IAM SW Stack**
- **Recommends HW/OS**
- **Technical Support**

**Systems Integrator**
- **Technical Architect**
- **Service Design**
- **Implementation**
- **Technical Support**

**HW Infrastructure**

- **Cloud Service**
  - IaaS, SaaS
  - Technical Support

- **Locally Hosted**
  - HW/OS Vendor
  - Technical Support

*Figure 19 Managed Service*
IAM Service Consumers Role

The IAM Service Consumer is any person or non-person (e.g. application) who has an account in the IAM system or accesses a service that utilizes the IAM for authentication or authorization needs. Typically, the IAM consumers will be students, staff, and parents of LEAs, Charter Schools, NCVPS, or NCSSM. Other state agencies may have staff members that utilize the IAM system to access education resources. Users will interact differently with the IAM system depending on their role. Students will interact with a different set of identity attributes than a teacher would. Delegated administrators will have more identity management responsibilities than teachers.

Cloud Services are also considered IAM Service Consumers. Cloud Services are the cloud-based applications, resources, and services that IAM Service Consumers will be accessing and using for their education needs. The Cloud Services will be using the IAM Service to authenticate and authorize IAM Service Consumers.

Service Roles Partners: IAM Service Manager, IAM Policy and Governance

The IAM Service Consumers (K-12 User Community) will be provided:

- A single account (username and password) that grants access to cloud applications, resources, and services
- A self-service user interface that allows authorized individuals to manage their identity information, reset passwords, and make/grant requests for cloud services
- Training and Documentation that illustrate how each user role interacts with its respective area of the IAM system
- Assurance that the consumer’s identity information is managed in the most secure and compliant manner

The IAM Service Consumers (K-12 User Community) will be responsible for:

- Ensuring the accuracy of their user identity information over time
- Communicating service requirements to the IAM Service Manager and to IAM Policy and Governance entities
- Providing Level 1-2 Technical Support for their constituents
• Provide general feedback to the IAM Service Manager about the quality of the IAM Service, including support

The IAM Service Consumers (Cloud Services) will be provided:

• Requirements for integrating Cloud Service with the IAM System

• Policy and Governance requirements related to the IAM Service and IAM Service Consumers

The IAM Service Consumers (Cloud Services) will be responsible for:

• Ensuring the security of user identity data

• Adhering and abiding to the rules set by the IAM Policy and Governance bodies regardless of type of cloud service, and any contract requirements regarding the use of identity data

• Providing notification and messaging to the IAM Service Manager about cloud service general changes, maintenance, and outages

• Providing a dependable, responsive and available service (application), to ensure a successful and consistent user experience

Over time as the IAM project matures and the actual needs are better known, there will be an evolutionary shift in workload and responsibilities among the different service roles.

Now that we understand who the service role organizations are, their expectations, and general responsibilities, we are ready to examine the other major tasks of the service model.
**Project Portfolio Management**

The IAM team will be coordinating with the State EPMO throughout the lifecycle of the IAM project for project management requirements and procurement needs.

“The Enterprise Project Management Office (EPMO) was established in 2004 to assist the State CIO (SCIO) in his legislated responsibility to improve the management of IT projects in state government. The EPMO is one component of this legislation; NC General Statutes - Chapter 147 Article 3D.

The State CIO has legislative oversight authority to review and approve State agency IT projects; develop standards and accountability measures for IT projects (including criteria for adequate project management); to require status reporting; to assign a project management advisor (PMA); and, if necessary, to suspend projects. The purpose of this legislation is to help to ensure that quality IT projects are delivered in a cost effective and timely manner.

By law, agencies must provide for a project manager who meets the applicable quality assurance standards for each IT project. The agency project manager is responsible for managing the project and providing periodic reports which shall include information regarding projects costs; issues related to hardware, software or training; projected and actual completion dates and any other information related to the implementation of the IT project.

The EPMO provides professional oversight to facilitate successful IT projects through assessing projects and facilitating resolution of issues, risks and roadblocks and by providing early warnings if a project is likely to fail. The EPMO does this through applying professional experience and best practices and by providing full and complete information to the SCIO to ensure the SCIO can respond appropriately.

We also engage agencies in understanding and applying IT portfolio management concepts to IT projects, applications and IT investments (plans and budgets). This is done through IT Portfolio Management services, which provides financial, technical, and management personnel with a knowledge and understanding of the theories, concepts, and disciplines of portfolio management. The service also includes training and support for the use of the Portfolio Management software tool to improve the planning, budgeting, and management of IT, especially IT investments.”

---

State of North Carolina PPM Workflow for Projects > = $500,000

Investment Cost = Project Cost (Initiation thru Closeout Phase) + 5 years Operations & Maintenance

Phase 1: Project Initiation

Gate 1 Planning & Design Approval

SCI, OSBM, OSC, EPMO, EA

P & D Review & Approval

Agency Reviewers & Approvers

Implementation Signoff

Agency Reviewers & Approvers

Phase 2: Planning & Design

Gate 2 Execution & Build Approval

SCI, OSBM, OSC, EPMO, EA

E & B / Pilot Review & Approval

Agency Reviewers & Approvers

Implementation Signoff

Agency Reviewers & Approvers

Phase 3: Execution & Build

Implementation Exit Criteria and Planning & Design Entrance Criteria

Gate 3 Implementation Approval

SCI, OSBM, OSC, EPMO, EA

Closeout Approval

EPMO QA Signoff

Agency Reviewers & Approvers

Phase 4: Implementation

Implementation Exit Criteria and Closeout Entrance Criteria

Project Initiation & Review

Agency Reviewers & Approvers

Phase 5: Closeout

Implementation Exit Criteria and Project Moved to Complete Status

Gate 4 Closeout Review

EPMO QA Signoff

Agency Reviewers & Approvers

NOTES
1. ** Template provided in the PPM Tool NC HELP section and on EPMO website WWW.EPMO.SCIO.NC.GOV is required for these documents.
2. All projects >= $500K are required to submit monthly status reports.
Service Plan Development

The IAM Service Manager will develop a Service Plan that describes the details of how it plans to develop, deploy, and manage the IAM system/service for the IAM Service Consumers. As previously mentioned, some items in the Service Plan are dependent on details of the Technical Implementation Plan. The Service Model part of this IAM plan will serve as the initial draft and framework of the more detailed Service Plan.

Requirements of Service Plan

Below are expected requirements that should be outlined in the IAM Service Manager Service Plan.

**Communications Model.** Messaging, notifications, and alerts are all communication components of the IAM Service. The service plan will need to describe how the IAM Service Manager plans to effectively and accurately communicate information inside its own organization as well as to and from Service Roles for all aspects of the IAM system. Open feedback mechanisms will be important tools for continuously improving the IAM Service over time.

**Support Model.** While the IAM Policy and Governance will establish many of the rules for support, the service plan needs to describe the processes and model for supporting other Service Roles of the IAM System.

**Outreach, Training, and Documentation.** Closely related to support, the IAM Service Manager will need to provide training and documentation related to the different Service Roles. The service plan should describe the expected types of training and documentation it will provide along with other outreach and knowledge management activities/efforts.

**IAM Service Pilots.** The IAM system must be piloted and vetted with IAM Service Consumers (users) and Cloud Services (applications) before moving to full production mode. The service plan must describe details of the different IAM Service Pilots and how they relate/contribute to the overall IAM System/Service.

**Milestones and Deliverables.** The service plan must describe the different milestones and deliverables for each phase of the implementation, deployment, and management of the IAM Service.

**Personnel Requirements.** The service plan must describe the internal personnel requirements to effectively manage the IAM Service initially and long-term. The personnel requirements should include each person’s role and responsibilities within the IAM Service along with necessary skills set needed.
Sustainability and Value. The service plan must define strategies of the IAM Service Manager that will enable it to provide a long-term sustainable and continuously valuable IAM Service to the IAM Service Consumers.

Funding Model. The service plan must include a detailed budget that reflects how the IAM Service Manager intends to use the project funds to deliver the service functions requested.

Biographical Sketch. The service plan must provide a biographical sketch and qualifications of the IAM Service Managers current staff that would be involved in providing the IAM Service.

Commitments. The service plan must provide a description of other commitments by the IAM Service Manager as a metric of availability to the IAM Service.

LEA Readiness Assessment. The service plan must describe its approach for on-boarding LEA technology systems to the IAM systems/service.

Change Management. The service plan must describe the IAM Service Manager change management policies for support systems of the IAM Service.

Software Asset Management. The service plan must describe how the IAM Service Manager intends to manage and optimize the purchase, deployment, maintenance, utilization, and disposal of software applications with the IAM System/Service.

Acceptance Testing and Metrics. The service plan must describe how the IAM Service Manager plans to develop metrics for acceptance testing of products and services from the IAM Managed Service.
Identity Data Sources, Target Cloud Services, and Federation Partners

One major task of the IAM Service Model phase will be to formally establish agreements with authoritative data providers, initial targeted cloud services, and identity federation partners. This task will allow the IAM team to clearly define requirements and scope for the RFP process and Phase III of Building and Implementation.

![Major IAM Integration Points](image)

**Figure 20 Major IAM Integration Points**
Identity Data Sources
Identity Data Sources are the K-12 authoritative sources where user identity data and attributes reside. The following systems will be the main authoritative data sources for IAM:

**NCWISE**
Single Authoritative Source for all Student Data  
http://www.ncwise.org/

First introduced to North Carolina Public Schools in 2004, the North Carolina Window of Information on Student Education (NC WISE) integrates all aspects of public school life from the classroom to the central office. Web-based and centrally maintained for capturing, accessing, and reporting a wide spectrum of student information, NC WISE replaces the Student Information Management System (SIMS), which North Carolina Public School Systems have used for almost two decades.

In 2009, NC WISE completed a statewide rollout, which includes all of the state’s 115 LEAs and 98 charter schools.

NC WISE is composed of three basic components:

- Electronic Student Information System (eSIS) allows individual schools to manage student information.
- Electronic Data Interchange provides the capability to electronically transmit all student instructional records and demographic information between school districts, between schools within a district, and to universities and colleges in North Carolina.
- Uniform Education Reporting System (UERS) transfers information from the local school district to the North Carolina Department of Public Instruction (NCDPI).

Essentially, NC WISE integrates all aspects of public school life from the classroom to the central office.

**Note:** The current implementation of NCWISE is using the eSIS product, which is a product by AAL. AAL was acquired in November 2010 by Pearson[^15]. NCDPI is currently evaluating alternative SIS products as a potential replacement for the current NCWISE eSIS implementation.

**UID**
Single authoritative source for staff data  
http://www.ncpublicschools.org/cedars/uniqueid/

[^15]: http://www.pearson.com/media-1/announcements/?i=1348
The NC Department of Public Instruction (DPI) has developed a Unique Statewide Student and Staff Identifier (UID) System that will be the cornerstone of the NC Common Education Data Analysis & Reporting System (CEDARS). The UID System enables LEAs and Charter Schools to assign a unique statewide identifier for every student and staff member who participates in the NC education system at any point in time. Establishing the capability to assign these identifiers is the first step in DPI’s multi-stage effort to create CEDARS. The UID enables reliable matching of student-level and staff-level records over time and across DPI applications. This capability is improving data quality at the state and local levels and supports state and local policy makers and service providers in making better data-driven decisions.

NC Staff Identification System (Staff UID)

- The Unique Identifier for Staff System (Staff UID) will assign a unique identifier to staff who participate in the North Carolina public school system.
- UIDs follow staff between school districts and remain valid even if they move out of state and then return to a NC public school.
- Staff UID is built on the eScholar Uniq-ID® for Staff product.

Wake County Public School System HR: Staff Data
TBD

Charlotte-Mecklenburg Schools HR: Staff Data
TBD

(Guest System): Guest Data
TBD

Other ancillary sources (possibly through Federation rather than direct data consumption) may include the North Carolina School of Science and Math, ITS NCID etc., as described in the appendices.
**Target Cloud Services**

Target Cloud Services are the web-based applications, systems, and services that the IAM Service Consumers (User Community) will be utilizing. We expect initial targeted services will likely include some or all of the following, in addition to applications to be determined in coming months that are not yet included in this table.

<table>
<thead>
<tr>
<th>Initial Targeted Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Moodle</strong></td>
</tr>
<tr>
<td><strong>Blackboard</strong></td>
</tr>
<tr>
<td><strong>Microsoft Live@EDU</strong></td>
</tr>
<tr>
<td><strong>Follett Destiny Library Manager</strong></td>
</tr>
<tr>
<td><strong>ClassScape Assessment System</strong></td>
</tr>
<tr>
<td><strong>MCNC Web Security</strong></td>
</tr>
<tr>
<td><strong>DiscoveryEd</strong></td>
</tr>
</tbody>
</table>
Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th>Initial Targeted NC Education Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NCLOR</strong></td>
</tr>
<tr>
<td><strong>SchoolDude</strong></td>
</tr>
<tr>
<td><strong>SAS EVAAS</strong></td>
</tr>
<tr>
<td><strong>SAS Curriculum Pathways</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial Targeted RttT Project Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IIS</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial Targeted DPI Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TBD</strong></td>
</tr>
</tbody>
</table>

Each of the Target services described above represents an application that is delivered as a cloud service offering. This means the IAM system will integrate with any of the above applications that LEAs are purchasing as a cloud service offering (i.e. not hosted inside a local district).
Setup test/development/staging accounts & systems for potential target services
Test, development, and staging systems will be used to test potential target services, along with a set of test accounts.

List/vetting to determine target services
Potential target services will be prioritized for onboarding to the NC Education Cloud IAM service taking into account a number of variables. For example, these might include (in no particular order):

- LEA readiness – Do LEAs have the time and resources to dedicate to a migration or integration of target services?
- Service readiness – Does the target service have necessary resources and documented integration methods?
- Consortium Buying – Are any of the targets services being acquired as part of a larger state collaboration purchasing agreement?
- Need – Is this target services needed for 1 school in an LEA, a single LEA, or the whole state?
- Cost of Service – How much does the integration cost? Target Service cost? Sustainability costs?

Migration Strategies

- New Migration – A new target service in which new user account provisioning is required.
- Rip and Replace – The current target service is replaced and new user account provisioning is required.
- Migration of existing services to cloud – A migration will occur from the current instance to a new instance and reconciliation of accounts would be required.
Developing an Identity and Access Management Service

Federation Partners

**SLC – Shared Learning Collaborative**

http://slcedu.org/

The Shared Learning Collaborative (SLC) is an alliance that aims to accelerate the progress of our public schools toward personalized learning for all students. The collaborative is designing a shared technology infrastructure that will support the implementation of the Common Core State Standards and help states and districts provide teachers with the instructional data and tools they need. Instructional data will be linked to high-quality and diverse sets of curricular resources, so each student gets what he or she needs most at that moment in time. And, because the Common Core State Standards create more consistency across states than ever achieved in the past, we have an opportunity to create an infrastructure that works better and costs less per state than what can be accomplished by each state working individually.

The SLC is building a set of shared services that will connect disparate student data and learning content that currently exist in different formats and locations and don’t integrate with one another. The SLC technology will include the following:

- **Middleware**: Software that integrates and orchestrates activities across different state systems, components and applications, enabling them to interact
- **Data store**: A secure, cloud-based repository for structured and unstructured learning data
- **Dashboards**: Out-of-the-box dashboards to make student data more manageable and useful for educators in a customizable format
- **Learning maps**: Graphical representations of student learning data to help visualize student achievements and needs
- **API**: An open API to enable vendors and developers to create applications and content that can interface with the SLC technology

The initiative is a state-led effort. The Council of Chief State School Officers is coordinating the multistate alliance and ensuring the new technology meets the needs of the states and reflects their input. Initially, Colorado, Delaware, Georgia, Illinois, Kentucky, Louisiana, Massachusetts, New York and **North Carolina** are participating in the pilot of this collaborative effort that will eventually be available to all states. The Bill & Melinda Gates Foundation and Carnegie Corporation of New York are providing the initial funding.

The IAM Service will integrate with the SLI using Identity Federation. This method will allow K-12 users in NC to utilize SLC applications with their local credentials.

---

16 http://www.slcedu.org/
PART IV BUILD AND IMPLEMENTATION
Build and Implementation Model
Technical Implementation Plan Development

The Technical Implementation Plan will describe the technical details of how the IAM system will be implemented in the context of a specific set of vendor products and platforms. The implementation must follow industry and product-specific document best practice guidelines. The IAM Managed Service vendor will lead this effort with oversight from the IAM Service Manager. The implementation plan will require approval from both the IAM Service Manager and IAM Policy and Governance before actual implementation is started. Several details of the technical implementation plan will inform the Service Plan that is being developed by the IAM Service Manager.

Requirements of Technical Implementation Plan

In addition to the details/steps of how the IAM system will be physically and logically implemented, the requirements below must be included in the implementation plan.

Infrastructure Specifications. The implementation plan must provide the necessary hardware and other infrastructure requirements, specifications, and recommendations needed for the particular product components of the IAM system.

Authoritative Source Data Analysis. The implementation plan must provide an analysis of the user identity data that will be provided as input to the IAM system. Any findings that impact the system should be described along with any recommendations from the IAM Service Manager.

Approach. The implementation must provide details about strategies and general approach of the system implementation.

Data Schema Design. A large portion of work in the implementation of any identity management system will be the data schema design. The implementation plan must include the expanded data schema design to be used in the IAM system.

Software Maintenance. The implementation plan must describe the necessary software maintenance operations that are required to maintain a secure, high performing, and sustainable system.

Infrastructure Maintenance. The implementation plan must describe the necessary hardware/infrastructure maintenance operations that are required to maintain a secure, high performing, and sustainable system.

Data Maintenance. The implementation plan must describe the necessary data maintenance operations that are required to maintain a secure, high performing, and sustainable system.
Best Practices. The IAM system implementation must adhere to documented industry and product-specific best practices. The IAM Managed Service should reference and highlight these best practices in the implementation plan as related to the actual IAM system implementation.

Test Plans. The implementation plan must describe the system test plan and performance testing results. The results should correlate to system requirements and product performance profiles.

Associated Risks. The implementation plan must highlight any perceived risks associated with the IAM System/Service.

Biographical Sketch. The implementation plan must provide a biographical sketch and qualifications of the current staff that would be involved in providing the platform components.

Commitments. The implementation plan must provide a description of other commitments by the IAM Managed Service as a metric of availability.

Personnel Requirements. The implementation plan must describe the internal personnel requirements to effectively manage the IAM Platform initially and long-term. The personnel requirements should include each person’s role and responsibilities within the IAM Platform along with necessary skills set needed.

Milestones and Deliverables. The implementation plan must describe the different milestones and deliverables for each phase of the implementation, deployment, and management of the IAM Service.

Regulatory Compliance. The implementation plan must describe the audit standards level for any infrastructure hosting used for the IAM System where appropriate. All IAM System components are desired to be hosted in data centers that meet new SSAE 16 standards, including SOC1, SOC2, and SOC3\(^\text{17}\).

---

\(^{17}\) See http://resource.onlinetech.com/soc-1-soc-2-soc-3-report-comparison/
Developing an Identity and Access Management Service

**HA and DR.** The implementation plan must describe the design and implementation aspects of how the IAM system will perform and support High Availability and Disaster Recovery efforts. Also include Load Balancing, Fault Tolerance, and Scalability measures.

**Change Management.** The service plan must describe the IAM Managed Service change management policies for all services rendered to IAM Service Manager.
After all of the vendors/partners are chosen and in place, and detailed technical implementation and service plans are developed and signed off on, the deployment and migration will likely occur in a phased approach with intermediate milestones along the way. Though the specific phases and milestones will be decided on during the early detailed technical implementation planning stage, we expect they might include milestones similar to the following:

- Basic User Directory Structure Defined
- Identify first set of LEA's that will provide input data
- User Directory Populated with test data
- **Authentication using test data**
- 1st target DPI app identified
- 1st target web app identified
- **Authorization through a web-services API to 1st target app, using test data**
- **SSO Authorization to 1st target web app, using test data**
- User Directory Populated with 1st Real LEA's data
- Web-services Authorization to DPI's 1st target app, using Real LEA's data
- SSO Authorization to 1st target web app, using Real LEA's data
- Initial set of 5-10 target apps identified (both Web-services & SSO methods)
- **Self-service password reset**
- **Delegated administration of group/role/user management**
- Initial set of 5-10 target apps can be authenticated/authorized
- **Automated provisioning to Directory**
- **Automated provisioning to Microsoft Office 365 and/or Google Apps**
- Successful authorization of NCSSM users via SAML-enabled SSO
- Stress/Load Testing
- Synching from central to LEA directories
- Federation among K-12/State Agencies
- Handling external users – parents/guardians/community members

At the end of this phase, the IAM System/Service framework is ready. All the IAM Service components will be in place. The next phase in the IAM Project will be the Full Production and Operation of the service.
PART V

FULL PRODUCTION AND OPERATION
Developing an Identity and Access Management Service

Full Production and Operations Model

Ongoing Support Model

Help Desk (Support) Escalation Process

K-12 User Encounters Problem

Support – District (Technology Director)

Support – School (Teacher/Technology Facilitator)

Support – Cloud (NC Education Cloud Help Desk) Triaged to appropriate Cloud Service

Support – Service Manager

Support – Vendor (Managed Service Provider)

*** It’s unclear at this time where a response would go, but likely to the school or district level (not the user)

Ongoing Funding Model

Ongoing Migrations for Service Consumers

Ongoing Policy and Governance Model
Developing an Identity and Access Management Service

APPENDICES
Appendix A – Potential IAM 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 North Carolina Identity Management Service (NCID) is the standard identity and access management platform provided by the Office of Information and Technology Services. NCID is a Web-based application that provides a secure environment for state agency, local government, business and individual users to log in and gain access to real-time resources, such as customer-based applications. 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 one 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

In one authentication model, an end user logs onto his/her local device (e.g. a laptop, desktop, or mobile device) with his/her unique username/password. From that point access to all local and cloud-based resources is automatically provided by the system. This method would require the device login to be using a domain-provided rather than a local account.

18 http://www.ncpublicschools.org/ncid/
North Carolina School of Science and Mathematics and other unique schools
The North Carolina School of Science and Mathematics (NCSSM) is a unique institution, in the sense that it is a member of the University of North Carolina state system yet also a high school. The NCSSM users are not part of the NCWISE student information system and the UID data, thus their data will not flow into the IAM system in the same fashion as the data from North Carolina’s LEAs. In order to make NC Education Cloud services available to users from unique schools such as NCSSM, alternative methods will be needed to handle those user identities. One possible alternative method would be to use SAML-based federation technologies. The NCSSM already has a SAML Identity Provider through the UNC system, thus this may be a viable solution. Further research on how to handle these unique schools will need to be done in coming months.

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 UID 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.

Portal
The portal component of the IAM system will present a simple user interface to the end users for managing their identity information. The initial scope of the portal will be limited to simple tasks such as updating information, requesting access to applications/services, and resetting passwords. In the future, the portal has the potential to be expanded and include many more user-centric functions. It could support user and/or LEA branding. It could be integrated into an LMS/CMS system or larger Education Cloud portal. 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.

IAM Components API Access for LEAs
While the IAM Components will have available APIs, the initial scope of the service will not be open to LEAs for directly communicating with the individual components. During the initial phases of the project, API access would be considered a non-standard interface. However, in the future, this functionality could be opened and extended to LEAs/others if needed. This could create a significant dependency and should be approached with caution.
Developing an Identity and Access Management Service

Federal Identity Management
There are several federal identity management initiatives that the IAM project could potentially get involved with. Some of the initiatives are the Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors, Federal Public Key Infrastructure (PKI), and the U.S. General Services Administrations Identity, Credential and Access Management (ICAM) Subcommittee, which is tasked with aligning the Identity Management activities of government.

Operational Data Store
During the course of our research and planning for the IAM system, we have determined that there is a need for a single, centralized, data repository that all user identity data resides. In one of the earlier functional requirements, we described the process of consuming user identity data into the IAM system. This process requires a complex tool that communicates with various source data systems and retrieve pieces of user identity information. Upon retrieval, it must perform various transformations on the user data to prepare it for processing by the IAM system. Because a single data repository for gathering user identity information does not exist, the IAM system is required to perform this additional functionality to in order to create and manage identity information.

As a matter of fact, each of the cloud services has this challenge. Data systems that handle HR and Finance will need to connect and retrieve user data for processing. Each data system would need to connect to multiple sources for getting the necessary user data. Instructional Data systems, such as LMS or CMS, would need to connect and retrieve user data for processing. Each of these systems would need to connect to multiple sources for getting the necessary data also.

The same process that the IAM system described in the functional requirements is repeated in the requirements throughout many cloud and other RttT systems. This creates several issues.

Data Integration Duplication. Without a single, centralized, data repository, each of the cloud and/or RttT systems will need to have a data integration component as part of its project. This integration tool must be complex enough to support the various disparate source systems. This duplicates the cost and effort of each project.

Data Integration Interpretations. Without a single, centralized data repository, each of the cloud and/or RttT systems will need to consume the data and perform transformations of the data before provisioning into itself. There is a high probability that each of the systems will do this in a different way. Therefore, if you had two LMS systems, the user data could potentially be different in each of them, for the same user.

Security of Access. Without a single, centralized data repository, each of the cloud and/or RttT systems will need to have access to various source system for user data. This means each of these source systems would need to manage user authentication
and authorization. In general, the IAM systems goal is to mitigate this situation. Managing the access for the different data sets is a challenging problem and could potentially lead to unauthorized access or data leakage. Having a single data repository would mean managing the authentication and authorization in one place instead of at each of the individual source systems.

Alignment with National Shared Learning Infrastructure. On a national stages, the Gates and Carnegie foundations have partnered through the Council of Chief State School Officers (CCSSO) to support and fund a multi-state collaboration to develop and deploy a national level shared learning infrastructure (SLI). The CCSSO SLI work comprises content and data standards; content, data, and identity management infrastructure; a core set of “built-in” applications that leverage the content and data management infrastructure; and, application interfaces supporting third-party development and integration with the SLI. Without a single, centralized data repository, the national SLI will have the same issues described above. A single, central data repository would enable better alignment with SLI initiatives.

Recommendation: Design, develop, and deploy (or acquire as a service) a single, centralized data repository that contains all attributes about student, staff, and parent users. The data about each user will be fed from the various disparate source systems into the single, centralized repository. The repository will present contemporary and standardized interfaces to the target systems for consuming the data.

**UNC Federation**

Each member of the University of North Carolina operates its own identity management infrastructure and assigns identity credentials independently. However, many web-based applications need access to these independent authentication systems to provide services to UNC members. Therefore, the UNC Identity Federation was created to provide this access in a secure way.

The UNC Identity Federation utilizes Shibboleth as a SAML 2.0 identity assertion service to enable users from one university to access information hosted by General Administration or any other university in the federation\(^1\).

---

\(^{1}\) [http://www.northcarolina.edu/ir/initiatives/uncif.htm](http://www.northcarolina.edu/ir/initiatives/uncif.htm)
Formal Impact Analysis of IAM System / Service
What impact has the IAM system / service has on the LEAs, State Agencies, and Education in general. Did/Does it bring added value to the service consumers?

Strong Authentication
Many of the vendor IAM software suites we researched supported strong authentication methods. Some examples are multi-factor authentication, challenge-response protocols, or no password-based authentication. All of these methods increase the level of security for the end user but add additional complexity to the usability area. In the future, there could be a need or want for this additional level of security, but in the initial implementation of the IAM system, we will be solving the single-factor authentication problem first.

Open Source IAM Components
Most technology projects look to the open source community for solution opportunities during the initial planning stages. The IAM project is no different. During the initial planning, we explored IAM solutions based on Open Source technologies but found that many of them had not been demonstrated at the scale and scope of this IAM project. There is also the challenge with supporting an open source infrastructure. However, we acknowledge that the open source community could become a viable alternative in the future for components or as a whole for the NC IAM system.

Schema Standards for K-12 Identity
One of the challenges we faced in the research and planning stages of the IAM project was related to schema. We initially had the idea of creating a single large directory system and providing a syncing capability for the local LEA directory servers. We learned that most of the LEA districts had developed custom directory schema that did not match other districts’ directory schema. Therefore trying to create a single directory with a common schema became a challenge beyond the scope of the IAM project. eduPerson and eduOrg are LDAP schema designed to include widely-used person and organizational attributes in higher education. It would be nice if there was a standardized directory schema (e.g. eduK12Person) for the K-12 community that could be adopted by local districts and the authoritative bodies.

OpenID and OAuth
During our research for IAM we explored the realm of OpenID and OAuth technologies but decided not to include this as part of the initial implementation. While easy to integrate to the proposed IAM service, we do believe such support merits resources in the context of our problem space. In the future, if this focus changes, the IAM Service will supply a viable platform to incorporate these technologies.
Appendix B – 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 and various legislation regarding individuals with disabilities. Each of the following will impact the IAM Service at different levels.

**American Disabilities Act (ADA)**

The American Disabilities Act (ADA) is a wide-ranging civil rights law that prohibits, under certain circumstances, discrimination based on disability. Disability is defined by the ADA as "a physical or mental impairment that substantially limits a major life activity." It was intended so that Americans with disabilities would be kept in the mainstream in terms of scientific and medical research and developments.

**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.

**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.

20 http://www.ada.gov/
22 http://www.coppa.org/comply.htm
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.

Individuals with Disabilities Education Act (IDEA)

The Individuals with Disabilities Education Act (IDEA) is a United States federal law that governs how states and public agencies provide early intervention, special education, and related services to children with disabilities. It addresses the educational needs of children with disabilities from birth to age 18 or 21.

Federal Information Security Management Act (FISMA)

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

North Carolina Identity Theft Protection Act

The North Carolina Identity Theft Protection Act of 2005 is a series of broad laws that was passed by the General Assembly of the U.S. state of North Carolina to prevent or discourage identity theft as well as guarding and protecting individual privacy.

---

26 [http://csrc.nist.gov/groups/SMA/fisma/overview.html](http://csrc.nist.gov/groups/SMA/fisma/overview.html)
Appendix C – IAM Research

This appendix will provide a summary of research done by the IAM team to better understand the work of Identity and Access Management. Also, including RFPs released by other organizations related to IAM systems.

IAM Working Group. The IAM Working Group, which includes representatives from the LEAs, Charter Schools, NCVPS, NCSSM, DPI and ITS, has been a tremendous value to this project. It has provided vast amounts of feedback and clarifications to the IAM team. It has also given us a vast insight into the LEA environment that has continuously improved the IAM plan.

Vendor Information Sessions. Many vendors spent hours and days with us. The vendors provided an invaluable amount of information around the Identity Management spectrum and greatly informed our planning process.

LEA Site Visits. Several LEA districts graciously hosted the IAM Team for visits to discuss their identity management systems. These visits were in addition to the larger statewide site interviews done by the NC Education Cloud project. These in-depth sessions have been and will continue to be immensely valuable to progress. The opportunity to meet the people and understand the systems in action greatly enhanced our research.

Various RFPs. Much useful information has been garnered from previously released RFPs from a variety of sources, including the Delaware Department of Education, Denver Pubic Schools, North Carolina ITS, New York City, Swarthmore, Tennessee, Wisconsin, MnSCU, etc. We believe this will enhance any procurements associated with our IAM project.
Appendix D – Requirements for Integrating Cloud Applications

This appendix will serve as a reference and requirements guide for vendors, cloud-based service providers, and other RttT project teams, for planning purposes around identity management. Two main areas are discussed – the provisioning of service accounts at the vendor site, and recommended authentication methods.

The following are applicable to all models:

**Policy and Governance.** Each cloud application, resource, or service that integrates with the central IAM system will require a certain level of policy and governance that defines how and what user data identities are exchanged. Personal identifiable information (PII) will be provided for some applications, and service level agreements (SLAs) or contracts need to be in place to enforce confidentiality and data disclosure policies.

**Detailed Technical Specifications.** When the time comes to integrate cloud-based applications, resources, or services with the IAM system, a more detailed set of technical specifications will be needed and provided. Some of these specifications cannot be documented until the central IAM system actually exists, but sufficient planning can be done based on the information provided below.

**Security.** The IAM system will require the secure transfer of the user identity data to and from itself. Whether from the source systems to the IAM system, or between the IAM system and cloud applications, all user data will be encrypted during transfer. Data transferred internal to the IAM System will also be over encrypted channels where necessary. If user identity data is provisioned into a cloud application, the policy and governance section will define how data is managed throughout the process, along with any SLA or contractual obligations related to its storage and protection at the vendor site.

**“Currency” of Identity Data.** Updates made to user data in the Source Systems will be reflected in the IAM System as soon as it is available and can be processed. This will vary greatly depending on the availability and format of the feeds. Initially, it is expected that updates will take place nightly, with full database extracts from the source systems being processed in a batch mode. This will naturally result in up to a 24-hour delay in user updates being made available to the IAM System. A more “realtime” availability of user changes would be possible if the source systems could provide deltas of changed data only, on a more frequent basis. This may be possible once the IAM system is in production and more is known about the entire process.
Provisioning and De-provisioning of Cloud Accounts

Automated (Direct) Provisioning

The IAM System will have the ability to provision, update, and de-provision user accounts to target resources using a variety of connectors. Updates to the Systems of Record or source systems will trigger changes to the IAM Service, and if configured, changes to any service accounts that are part of the provisioning process. Requested user information will be provided during the provisioning process, including an individual’s user ID and (if part of the vendor agreement), his/her password in encrypted form. The cloud service providers will need to have automated mechanisms in place to consume the identity data or provide an API into their applications.

Advantages: Less configuration and implementation work for cloud application owners. De-provisioning removes accounts (or access), which eliminates cleanup of old accounts for the vendor as well as reducing the security risk to users or client organizations.

Disadvantages: If the user’s account and password exist at the service provider site, it needs to be maintained (synchronized) and could get out of sync if not done properly. There is also the risk that if the service site is compromised, the user’s credential could be used to access other cloud resources including self-service modifications to the IAM System (if the password exists at the service site). Lastly, the user’s account name and password may need to be passed to the service every time they login.

“Manual” (Indirect) Provisioning

If automated provisioning and de-provisioning is not an option at the time of implementation, manual updates can be handled by the vendor with user files provided through encrypted file transfers. These can be made available in different formats depending on the service provider’s update process (e.g. CSV files, spreadsheets, etc.). A de-provisioning process should also be in place to prevent inactive accounts from existing in the vendor application. The vendor should have a mechanism in place for handling new, changed and deleted/disabled account updates.

Advantages: Eliminates the need for individual user provisioning of accounts, which is primarily a benefit for the user. Authoritative data provided by the IAM Service will be more dependable than self asserted user data. A de-provisioning process removes accounts (or access), which eliminates cleanup of old accounts for the vendor as well as reducing the security risk to users or client organizations.

Disadvantages: Similar disadvantage to automated provisioning for applications where the passwords are stored at the service site. Disadvantage to manual provisioning is that there is more of a time lag between changes to the user data and updates to the application accounts. If the updates themselves are also done manually, there is more room for error or process failures.
Provisioning on “First Use” (Special Case)
This process is used by some applications that require a limited amount of user data, usually including username, first name, last name and email address. Release of this data is governed by policy and any SLA or Contract in place with the vendor. The preferred method is “automated” provisioning where the expected data is supplied by the IAM System, usually using a SAML assertion during federated access. Manual processes don’t differ from any public web service/application where users provide their own data (self asserted).

Advantages: In the “federation” case above, the data provided is authoritative, coming from the IAM System. It eliminates the need for passing files to the vendor for (manual) account creation. There are no real advantages to the self-asserted process.

Disadvantages: Major disadvantage is that this process only works for applications that require a limited amount of user data to be supplied to the service provider. Applications requiring user accounts with “protected” data or multiple attributes might favor one of the other options.

Provisioning and De-provisioning: Specifications
The IAM System will support APIs using most standard protocols, transports, and formats, like JDBC, LDAP, JMS, JNDI, and XML. The IAM system will package the identity information into the appropriate format and provision the identity information into the application, resource, or service using the target’s preferred method. Identity provisioning mechanisms typically should be through one or more of the following: API (preferred method), local directory services, or flat file (not preferred).

API example: The IAM System could create user accounts in Google Apps for Education using Google Provisioning API28 calls from the central identity manager. If a similar, well-documented provisioning API is available from another resource provider, then a suitable connector could be identified (or written) in the IAM system to communicate with the other resource providers.

Local directory services example: The IAM system could populate and maintain user identity information to a directory server that is local to the resource provider, such as Microsoft Active Directory. The resource provider application uses its local directory for authentication and authorization, and the IAM system is configured to make updates as necessary to that local directory.

Flat file example: Simple ASCII files in CSV or tab-separated format could be provided to external service providers from the IAM system, with the required information. This is

28 The Google Provisioning API is available in several languages: Java, .NET, PHP, and Python. For further information, please see “Google Provisioning API Reference Guide” at http://code.google.com/googleapps/domain/gdata_provisioning_api_v2_0_reference.html#How_the_API_Works
Developing an Identity and Access Management Service

not a preferred method of provisioning, and if it is the only available method for a given service provider, we expect that service provider to be given lower priority in the on-boarding process.

Authentication Methods for Cloud Services

Model 1: Identity Federation

The IAM system will include federated identity management functionality that supports exchanging authenticated user identity information between member organizations using SAML assertions. The federation or vendor agreement will document the necessary procedures and policies to securely and effectively exchange the user identity information. The application/resource vendor will need to have federation software in place and satisfactory security and privacy policies and procedures to take advantage of this model. This model is typically used for accessing shared services within an identity federation, although single vendor implementations can be configured.

Advantages: The major advantage of using federated access is that authentication accounts do not need to be set up at each cloud service, which prevents remote service account passwords from having to be synchronized whenever the user makes a change. It allows the service provider to rely on the user’s home institution to maintain the account and any information about the user – whether his/her role has changed, whether he/she has left the organization, when he/she changes schools, etc. Cloud service providers can focus on providing their service and not on the management of accounts. Coupled with direct provisioning and de-provisioning from the IAM Service, this is the best option for the vendor and the NC Education Cloud. An additional advantage for the identity provider (and the K-12 user community) is that it frequently takes little effort to “onboard” new applications that are added to the federation. If the Cloud Service is already enabled for federated access, it is a very simple process for them to add another client.

Disadvantages: Disadvantages for Cloud service providers exist if their application is not already SAML/Federation-ready. Depending on the requirements for authentication and whether there are associated service accounts, the effort on the part of the vendor can be relatively simple (standing up a federation service in front of their application) or required a programming effort to consume the SAML assertion and convert or map attributes to service account data elements. However, once this is done, any client then has the ability to use federated access.

Model 1: Specifications

Federation is enabled using the Security Assertion Markup Language (SAML) protocol. Identity and attribute assertions are shared through the user’s web browser session
Developing an Identity and Access Management Service

using SAML. Service Providers (SPs, or applications) and Identity Providers (IdPs) “recognize” each other as federation members based on previously exchanged metadata information.

An IdP is a web application that uses its organization’s authentication mechanism. A user logs in to his/her home institution’s IdP with his/her usual login and password. The IdP then obtains user attributes through a query to the central directory. The IdP generates a SAML assertion according to the IdP organization’s security policies as configured in the IdP. Attributes are shared through the user’s web session and consumed by an SP, which is often hosted by a different administrative organization. The SP determines whether to grant access to the user, based on its own policies and the attribute values asserted by the IdP.

Two well-known implementations of the SAML protocol are provided by Microsoft’s Active Directory Federation Service (ADFS)\(^{29}\) and by the open-source Shibboleth\(^{30}\) software. The IAM system will provide one or more instances of a SAML IdP, for use by approved SAML-capable SPs hosted by application providers.

Example: The NC Cloud organization and the Cabarrus County Google Apps service have setup a federation between their two entities, which allows a user from an NC Cloud IdP to access the Google organization’s Cabarrus County service with his/her attributes as presented through SAML assertions. Sue, a Cabarrus County teacher, attempts to log in to Google Apps with her NC Cloud login and password and is redirected to an NC Cloud IdP. Upon successful authentication, her browser is redirected back to Google Apps and she is granted access with the attributes presented through SAML assertion. Note: Assuming a Google Apps domain existed for NCID users, was configured for SAML-based SSO access, and an NCID IdP was operational and federated with the Google Apps NCID domain, then a user with an NCID could log in to the Google Apps NCID domain using a similar process.


Model 2: Central Authentication and Authorization via Reverse-Proxy Portal

In this model, authentication and authorization for applications takes place through the IAM User Portal. Users access the portal and are authenticated against a central directory. Applications only needing authentication for access could rely on the users being authenticated through the portal and would not allow access through other means (e.g. local login, direct browser access).

Service Providers that required a more granular authorization decision (based on directory attributes for the user) could have the portal check for valid attribute values before passing the user through to the application.

Advantages: This provides authentication (and authorization) to the application through a common interface (the portal) for the user, and is essentially “single sign-on”. While more complex to configure than using the federated access model (and likely unique for each application using this method), it prevents the transmission of the user’s institutional credential (username and password) to the service site where it might be stored and later compromised.

Disadvantages: This just adds complexity to each individual configuration, particularly on the IAM Service side. Given the choice between this method and Federation, it would be much more efficient (and take less time) to use federation.

Model 2: Specifications

The cloud application, resource, or service would apply a simple firewall or web-based filter that only allows network traffic from the central IAM system. The user authenticates against the IAM portal and then if authorized, would be allowed to see the cloud application, resource, or service. The central IAM system grants access to these authorized systems based on group, role, or entitlement policy defined inside the IAM system. The target cloud application, resource, or service does not have any user management capabilities other than standard OS or service filtering.
Model 3: Centralized User Authentication and Authorization Management

The IAM system will provide a central access control service that resource provider applications could use for authentication and authorization.

**Advantages:** The benefit of this approach is that the user accounts and data are always current and passwords do not need to be maintained at the resource. If a user’s role or status changes which removes his/her entitlement to access to the resource, it is updated in the central directory and prevents access.

**Disadvantages:** Depending on how this model is implemented, it still requires the user to send his/her username and password to the vendor before it is “tested” against the central IAM Service. If the user is redirected to an authentication site at his/her own institution to login (similar to federated logins) then security is not an issue.

Model 3: Specifications

Applications would be configured to use the IAM system and user authentication requests would be passed to the central system instead of using the application’s local authentication service. These mechanisms would typically use a Web Service API.

**Web Services API Example:** The IAM system will provide a web services API (SOAP or REST based) to service authentication requests over an encrypted http channel.
Model 4 - Local Authentication

Disaster Recovery

Depending on how critical the availability of an application is (as determined by the governance committees of the NC Education Cloud and its stakeholders) there may be a requirement to provide an alternate method of access in the event that the Cloud IAM Service is unsustainable. This would not need to be a failover mechanism or even activated, unless a planned migration away from the IAM Service is decided upon or in the event of a prolonged service outage.

Model 4: Specifications

The application or service would likely need to support creating users, possibly groups, and a mechanism for managing access controls internally for those accounts.

Example: An LEA has a Moodle Server that is using the central IAM system for user authentication and authorization. The central IAM system experienced an extreme circumstance and could no longer be provided as a state IAM service. The LEA could either find another authentication source for its Moodle system or just use the application’s internal capabilities to manage users. The Moodle application allows administrators to create and manage user accounts in a variety of ways. One of these methods\textsuperscript{31} includes local application authentication. The administrator would create users, groups, and access control rules internally to its Moodle server.

\textsuperscript{31} http://docs.moodle.org/20/en/Authentication
Appendix E – IAM Project Assumptions, Risks, and Dependencies

This section will describe Assumptions, Risks, and Dependencies of the IAM project. Risks that are described could become significant obstacles and pitfalls for the project. These will be captured in reviewed during a Monthly Risk Assessment (of the document).

Assumptions
One key assumption, upon which all of this IAM work is based, is that over time LEAs will be moving to cloud applications and reducing their use of locally based services.

Risk Analysis Table

<table>
<thead>
<tr>
<th>Category:</th>
<th>Risks are grouped under Category Heading (e.g. RFP Process, Project - Development, Project - Production, People Issues, Security &amp; Compliance).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rating:</td>
<td>Color indicator designating the amount of risk based on the formula* (below).</td>
</tr>
<tr>
<td>Risk Description:</td>
<td>A description of the risk or dependency, in just enough detail so I remember what I was afraid of. Some people are fanatical that it must be worded as a risk (for example, &quot;Hardware schedule&quot; is not a risk, but &quot;The hardware schedule might slip&quot; is a risk.). I'm not fanatical about anything; whatever works for you works.</td>
</tr>
<tr>
<td>Likelihood:</td>
<td>How likely it is that the risk will evolve into a real problem. The likelihood may change over time; something that is unlikely to be a problem at the start of a project may become very likely when the due date is approaching and the risk has not yet been avoided. A simple ranking of high, medium, low is used.</td>
</tr>
<tr>
<td>Impact:</td>
<td>What is the impact if the risk becomes a real problem. Impact is a bit subjective, but it should address the impact to the overall product. For example, a high impact risk is one that could cause the entire product to be canceled or significantly delayed. A low impact might mean increased cost or a small impact to product schedule. Again, in this case a simple rating system of high, medium and low is used.</td>
</tr>
<tr>
<td>Prevention Plan:</td>
<td>This is what I'm going to do to ensure that the risk does not become a problem. For dependencies, this might include communicating with the supplier early and often, tracking interim milestones, etc. For technical risks it might mean doing early prototype work, or adding subject-matter experts to the team.</td>
</tr>
<tr>
<td>Contingency Plan:</td>
<td>This is what I'm going to do in case the risk evolves into a problem. That is, in case my prevention plan has failed.</td>
</tr>
<tr>
<td>Narrative:</td>
<td>This contains a more detailed description of the risk, along with possible examples.</td>
</tr>
</tbody>
</table>

---

*Adopted from http://blogs.oracle.com/tacticalleadership/entry/know_what_you_re_doing3
Developing an Identity and Access Management Service

**Likelihood & Impact Scale:** Low=1, Medium=2, High=3

* Formula for Red, Yellow, Green Risk Color:
  
  Likelihood x Impact = Risk factor. 1-3 (Green), 4-5 (Yellow), 6-9 (Red)

- **RFP Process**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Risk Description</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Prevention Plan</th>
<th>Contingency Plan</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFP BAFO Too High</td>
<td>Me d h</td>
<td>M e d h</td>
<td>IAM Service needs to be broken into very specific phases/stages with what functionality will be delivered in each phase. Early phases must stand on their own (deliver basic functionality) Later stages can be “optional” functionality Respondents need to price each phase/stage</td>
<td>If all prevention plan items have been followed, contingency would be to either further reduce requirements, or look at some lower tier vendors</td>
<td>Responses to RFP for IAM Service Solution come back with too high a cost (possibly due to complexity of product/solution, extent of functionality/features, scope creep beyond specified requirements)</td>
<td></td>
</tr>
</tbody>
</table>
| Ineffective Technical Product Architect (Systems Integrator) | Me d h | M e d h | Need to really do our due diligence in the vendor evaluation phase. Try and get to know the actual people who will be doing the work, before choosing the vendor | Demand the primary respondent replace the SI | - Incompetent (skillset, knowledge)  
- Ineffective Project Management  
- Personality issues  
- Lack of collaboration (no knowledge transfer)  
VERSUS What’s NEEDED:  
- Understanding of Products and Functionality  
- Excellent Communication skills  
- Collaboration with IAM Service Manager  
- Ability to effectively execute Product knowledge transfer |
| Target Systems (Services) not identified prior to RFP release | L o w d | M e d h | Confirm (before RFP?) with rest of Cloud Team on which target(s) should be first priority. Then speak directly to these targets in the RDP. | Make a best effort to list our expected top-10 apps, and ask vendors which one(s) they could support? (Then decide later which to pursue first) | Other Cloud Services aren’t identified to enable “target systems” to be listed in the RFP – may impact solution or at least “cost” |
## IAM Service Configuration & Implementation

<table>
<thead>
<tr>
<th>Rating</th>
<th>Risk Description</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Prevention Plan</th>
<th>Contingency Plan</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unreliable Authoritative Data Sources</td>
<td>High</td>
<td>High</td>
<td>Continued communication with all stakeholders. (Are there data steward(s) who are willing and able to work with us to facilitate proper access to and interpretation of any needed data?) Governance Board/Committee to review? Messaging to LEA community needs to include info on their data responsibilities. LEAs could be required to provide/maintain a page describing process users should take to change their data. Require that LEA web page be maintained and communicated appropriately (through Governance &amp; Policy) Should we begin formalizing the [change management] committee now?</td>
<td>Get data needed directly from LEAs? Technical committee / cloud team would be the fallback for enforcing Change Management</td>
<td>Is the input data quality absolutely horrible, irreparably so? What if input data sources stop being available? Or if they’re corrupted? When the input data sources change, will we be adequately notified? What if the input data doesn’t have everything we need? (e.g. if don’t have course enrollment / teaching info).</td>
</tr>
<tr>
<td></td>
<td>Unreliable Support for Data</td>
<td>High</td>
<td>High</td>
<td>Need to approach Source System “owners” now to identify the authorized, capable Point of Contact who will help us through data issues. LEAs will need to update / clean data, also web page(s) with instructions</td>
<td>This one doesn’t really have a contingency. It requires the Governance committees to impose stricter requirements on the data stewards to provide appropriate support.</td>
<td>DPI, Wake, Charlotte, NCSSM, must provide input data consistently, along with advice and assistance on that data. “One off” systems such as NCSSM, standalone HR systems, etc. may also need to provide data.</td>
</tr>
</tbody>
</table>
Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th>Guest System Solution</th>
<th>HIgh</th>
<th>High</th>
<th>Ensure RFP specifies need for standalone Guest System of Record. Guest accounts may need to be used for local (non-cloud) apps – if so, how will this be done?</th>
<th>Determine whether any “Cloud” apps need access by Guest users, versus “Local” apps. Possible use of Social Identities where appropriate (rather than new system)?</th>
<th>Need stand-alone Guest System to hold identities of non-students, staff Use of a directory results in accounts that are not well controlled Allows dups to be created - Internally - Externally (Already exist in IAM) Not able to be used/sync’d to local LEA directories (needed for LEA Apps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope Creep</td>
<td>Medium</td>
<td>Medium</td>
<td>Stay focused on clear, measurable, achievable, and beneficial functionality (the 80/20 rule)</td>
<td>Reprioritize to focus on the absolute bare essential requirements only.</td>
<td>Scope Creep – attempting to provide too much functionality, too many “bells &amp; whistles”, political pressure to add more than what can be funded</td>
</tr>
<tr>
<td>Use/requirement of Nonstandard Connector/Adapter</td>
<td>Low</td>
<td>Low</td>
<td>Make sure these issues are addressed with questions in the RFP or Q&amp;A during selection Ensure that a “connector” is needed for a resource. If user accounts are not being provisioned into the app, then this may not be a requirement.</td>
<td>One option might be to develop (program) the connector “in-house” rather than use the vendor, or contract it out to a lower cost 3rd party.</td>
<td>- Lack of appropriate connectors - New connectors difficult to add - New connectors too slow to add - Additional cost for “development” - Proprietary lock-in</td>
</tr>
<tr>
<td>Missed Key Requirement(s) from Stakeholders (LEAs)</td>
<td>Low</td>
<td>Low</td>
<td>Continued communications with LEAs LEA internal communication (top to bottom, regional representative to LEAs)</td>
<td>Require funding to accommodate changes, additional features</td>
<td>Requirement may impact the way the IAM Service works, or the priority of functionalities implemented.</td>
</tr>
</tbody>
</table>
### Communication & People Issues

<table>
<thead>
<tr>
<th>Rating</th>
<th>Risk Description</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Prevention Plan</th>
<th>Contingency Plan</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ineffective/Inadequate Communication</td>
<td>High</td>
<td>High</td>
<td>Regularly scheduled status meetings between these groups should specifically address this point, as well as written status updates.</td>
<td>This is a leadership issue that the Governance Committees must address if it becomes a problem.</td>
<td>Among and between stakeholders, technical, management, data stewards, and IAM Service “roles”, etc.</td>
</tr>
<tr>
<td></td>
<td>Ineffective Governance Boards/Committees</td>
<td>High</td>
<td>High</td>
<td>This gets back to the need for project “champions” throughout the governance structure, to encourage timely responses to Governance and Policy queries.</td>
<td>Where do you go if the top-level leaders are not effective? (Might require some lobbyists!).</td>
<td>Failure of Governance committees to determine/make policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Collaborate between Agencies, LEAs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Inability to reach consensus on - Roles - Standards - Onboarding requirements (acceptance) - No accountability, authority, enforcement</td>
</tr>
<tr>
<td></td>
<td>Poor Transitions / Handoffs</td>
<td>Medium</td>
<td>Medium</td>
<td>Set expectations early on and build in clear, regular, measurable checkpoints! Need to really do our due diligence on the primary vendors -- and hold them accountable in case of problems. If Vendor is remote, perhaps the regular checkpoints should be F2F?</td>
<td>Might have no other choice than to reduce the deliverables of early phases.</td>
<td>Initial IAM Managed Service development phase could take too long</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Vendor sub-contractors could be in over their heads</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Possible vendor bait and switch (they might bring in a SI team that’s different?)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Communication with IAM Managed Service (non-responsiveness) -&gt; if SI is remote, how will that impact us?</td>
</tr>
</tbody>
</table>
Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Prevention Plan</th>
<th>Contingency Plan</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Experiences</strong> with respect to Applications/Cloud Services (benefit, ease of use, adoption, etc.)</td>
<td>High</td>
<td>High</td>
<td>Initial target apps MUST be high value and MUST be identified soon. Password self-service needs to be high priority to reduce help desk calls. Need to ID several friendly LEA early adopters from the Cloud Team (WG), who may provide positive word-of-mouth feedback to other LEAs.</td>
<td>This is a critical risk to the success of not only the IAM Service, but the entire NC Education Cloud initiative. A lot of attention needs to be paid to this issue – in selection, user acceptance testing, etc. The only contingency is to “spend money” to quickly rectify the situation – whether adding additional applications, adding resources to deal with helpdesk support, etc.</td>
<td>Can we on-board a sufficient number of high-value applications quickly enough? Will the system perform with adequate responsiveness? Training, Documentation, Helpdesk availability (skill level required to use IAM Service exceeds that of users) Business processes of LEAs could differ enough to cause major problems during implementation and user acceptance testing.</td>
</tr>
<tr>
<td><strong>Sustainability</strong></td>
<td>Medium</td>
<td>Medium</td>
<td>Need to plan starting now for the end of RttT funding - what is the model after that? Functionality provided needs to match funding – if funding is reduced, then functionality might need to be restricted Cost of additional functionality, apps, connectors/adapters - will need to be funded by either DPI, LEAs (for small group of beneficiaries), State, App Vendor, etc.</td>
<td>Each of these concerns needs to be addressed. The contingency is to cut back on services or find additional funding. Some of these might need to be dealt with as they arise, and do whatever it takes to maintain the IAM Service – this assumes that Cloud project and Shared Infrastructure and Services are successful.</td>
<td>We MUST develop a sustainable plan to address the critical cost issues!! Lack of funding Inability to complete(expand IAM Service Later phases Add additional LEAs Onboard additional Apps Etc. Loss of funding Nationals/State economic downturn (essentially same as above) Vendor Product Ongoing Cost/Increased Cost Vendor buyout Product change Lack of mitigation strategies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rating</th>
<th>Risk Description</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Prevention Plan</th>
<th>Contingency Plan</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td><strong>User Experiences</strong> with respect to Applications/Cloud Services (benefit, ease of use, adoption, etc.)</td>
<td><strong>High</strong></td>
<td><strong>High</strong></td>
<td>Initial target apps MUST be high value and MUST be identified soon. Password self-service needs to be high priority to reduce help desk calls. Need to ID several friendly LEA early adopters from the Cloud Team (WG), who may provide positive word-of-mouth feedback to other LEAs.</td>
<td>This is a critical risk to the success of not only the IAM Service, but the entire NC Education Cloud initiative. A lot of attention needs to be paid to this issue – in selection, user acceptance testing, etc. The only contingency is to “spend money” to quickly rectify the situation – whether adding additional applications, adding resources to deal with helpdesk support, etc.</td>
<td>Can we on-board a sufficient number of high-value applications quickly enough? Will the system perform with adequate responsiveness? Training, Documentation, Helpdesk availability (skill level required to use IAM Service exceeds that of users) Business processes of LEAs could differ enough to cause major problems during implementation and user acceptance testing.</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td><strong>Sustainability</strong></td>
<td><strong>Medium</strong></td>
<td><strong>Medium</strong></td>
<td>Need to plan starting now for the end of RttT funding - what is the model after that? Functionality provided needs to match funding – if funding is reduced, then functionality might need to be restricted Cost of additional functionality, apps, connectors/adapters - will need to be funded by either DPI, LEAs (for small group of beneficiaries), State, App Vendor, etc.</td>
<td>Each of these concerns needs to be addressed. The contingency is to cut back on services or find additional funding. Some of these might need to be dealt with as they arise, and do whatever it takes to maintain the IAM Service – this assumes that Cloud project and Shared Infrastructure and Services are successful.</td>
<td>We MUST develop a sustainable plan to address the critical cost issues!! Lack of funding Inability to complete(expand IAM Service Later phases Add additional LEAs Onboard additional Apps Etc. Loss of funding Nationals/State economic downturn (essentially same as above) Vendor Product Ongoing Cost/Increased Cost Vendor buyout Product change Lack of mitigation strategies</td>
</tr>
</tbody>
</table>
# Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th>Rating</th>
<th>Risk Description</th>
<th>Likelihood Impact</th>
<th>Prevention Plan</th>
<th>Contingency Plan</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security of PII Data (Target Services, Apps)</td>
<td>Low</td>
<td>Contracts and SLA with Vendors need to stipulate requirements and responsibilities of any data they store – as well as liability in the event of an incident</td>
<td>If contracts are written carefully, then litigation is the contingency to non-compliance.</td>
<td>Service providers -- can we trust them to protect PII? Will they responsibly consume assertions?</td>
</tr>
<tr>
<td></td>
<td>Breach of Systems &amp; Data, Password Compromise (IAM System - Internal)</td>
<td>Low</td>
<td>Breaches and sharing of passwords can and do happen. Having a well thought out (and tested) plan for remediation of any security issue is critical to keeping data and passwords secure. The ability to quickly disable user accounts (through delegated administration or centrally), along with a process for re-activation should be required. Better if IAMS could use a portal, to enter the (unknown, and otherwise not-used) password on behalf of the user.</td>
<td>Having a detailed plan for addressing any type of breach or data release would be the appropriate contingency.</td>
<td>IdPs -- could they be compromised? Central directory -- could it be accessed/used maliciously? Passwords - if stored at an SP (and it's the user’s primary password) - could be a HUGE exposure risk. Users -- they could intentionally share their login / password. Viruses -- keystroke loggers could nab someone’s password. Active sessions left running in a browser on a public machine could lead to an identity risk.</td>
</tr>
<tr>
<td></td>
<td>Intentional or Unintentional Exposure or Release of PII Data by Delegated Admins</td>
<td>Low</td>
<td>In either case, this involves a well thought out and detailed mitigation plan. If the release was intentional, procedures for disciplinary action by the appropriate authority (school, LEA, DPI, etc.) should be in place and communicated through normal channels.</td>
<td>SIEM Tool</td>
<td>Delegated admins - can we trust them to do the right thing? Compliance risks – what if we accidentally (or intentionally) violate one of the state or federal privacy regulations (FERPA, HIPAA)? If so, how to fix? What would be the ramifications?</td>
</tr>
</tbody>
</table>

## Dependencies

Key dependencies, such as timely access to accurate data sources, have been outlined in the above risks table. If critical dependencies are not realized, this project’s success will be impeded.
Appendix F - 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, and Web Services. However, direct access to the central directory via LDAP may not be exposed externally, especially in the early phases of the project. Over time and with sufficiently vetted security procedures and applications, LDAP access to the central directory may possibly become available.

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 may be capable 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 IAM system will have some basic groups predefined based on NCWISE and UID attributes. It will also 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 system 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.
Developing an Identity and Access Management Service

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.
Appendix G – Proposed Policies, Regulations and Rules (PRRs)

*These questions will eventually become more formalized PRRs with structure and process in the larger NC Education Cloud context. We will be proposing PRRs in response to these simple questions that need to be answered in order to make provisioning and workflow decisions.*

**Business Operations PRRs**

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?

   A: LEAs can certainly enter into their own agreements with vendors, however it would not be guaranteed the IAM system would release any data to those external vendor applications. The IAM governance body, in collaboration with the IAM technical team, would need to approve and then implement releasing data from the IAM system. If this approval and implementation does not occur, the LEA would need to interact directly with the vendor to provide any necessary data to that service.

3. What happens to the IAM system (service) after the NC Education Cloud program is over? (How is the IAM project sustained to continue providing value to stakeholders?)

4. Who oversees the IAM project after the Cloud Project is completed?

5. What are the procedures for how an LEA interacts with the IAM Service? How do they request information, access, and resources?
Data Integration Platform (Authoritative Data Sources) PRRs

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

2. What Regulatory and Compliance Rules impact or apply to the IAM System?

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

   A: LEAs “own” the user data on students and staff members. They also approve, or “sponsor” the data on guest members such as parents, volunteers, etc., so in a sense the LEAs own that data as well. The IAM system does not own any of the data; it simply has custody of it on behalf of the LEAs.

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?

   A: Parent data in NCWISE will likely not be used until it becomes a more reliable source. Instead a self-registration (guest) system combined with LEA-approval will probably be used.

6. What data is authoritative for Parents that are also Staff (the Guest or HR System)?

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

   A: No, however, the custodian may change, e.g. from the IAM system to a vendor application provider. External service providers will be mandated to adhere to strict safeguards to protect the privacy of any such transferred data.
Managing Identities PRRs

1. What are the default groups that user identities will be provisioned into (e.g. student, teacher, staff, parent, guest, etc.)?

2. Who decides on what data elements are released (e.g. specific attributes)?

3. How are accounts generated? (Triggers? what data is populated? what services are provisioned?)

4. How do users authenticate (e.g. Accessing a portal, using one of many web apps, etc.)

5. Can Social Identities (e.g. GoogleID, Facebook Connect, etc.) be used by parents or guests to authenticate? If so, what identity data is required/supplied?

   A: Not in the initial phases of the IAM project. These could be added as part of future work.

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

   A: Since these are central accounts that are used for cloud services, the identity proofing and vetting processes should be standardized across all LEAs. While there may be some flexibility or options with respect to what is acceptable, the overall process and documentation requirements will need to be approved by the IAM Governance group(s) and followed by all participants. This is particularly important when using federated identity management, as the service providers must trust that appropriate processes are used to ensure that their rightful owners are using accounts.

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

   A: This is also an IAM Governance issue, although multiple processes or options may be defined for use by LEAs.

8. What identifiers are used for individuals? (SIS id, HR id, parents – email address?)
Managing Access PRRs

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

A: Each LEA will have access to its own data, but not to any data from other LEAs. Within an LEA, high-level administrator(s) will be able to delegate access privileges to other users from that LEA. Cloud applications will also have access to certain parts of this data, subject to policies approved by the IAM governance body and to approval by each LEA that would participate.

• Who determines what applications can consume user (student, staff, parent) data?

A: The IAM governance body, which will include advisory input from the LEAs, will approve any applications that will interact with the IAM system and what data will be provided. LEAs will be welcomed to submit requests to the IAM governance body, to have additional applications added to the approved list, however, review of the application vendor, their data requirements, and the security of their environment will determine whether they can participate as a Cloud Service.

• What are the Policies around managing federated access (Federated Identity Management)?
Centralized Reporting and Auditing PRRs

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

   A: LEAs will have access to their own log data, but not to any log data from other LEAs. Within an LEA, high-level administrator(s) will be able to delegate access privileges to other users from that LEA.

2. Do periodic reports need to be run for Regulatory and Compliance violations?

   A: Reports would be created for audit purposes. Regulatory violations would be focused on individuals and would most likely be generated by ad hoc queries.
IAM Service Roles PRRs

IAM Service Roles are: IAM Service Consumer (LEAs and Cloud Services), IAM Service Manager, IAM Managed Service, and IAM Policy and Governance.

1. What are the approval workflows or processes for the IAM Service Roles? Example: If an LEA wants feature X in the IAM system, how does that get reviewed, approved, or denied? Who funds it?

2. How much decision-making responsibility does the Service Manager have versus what do they need permission/approval for from the policy/governance bodies?

3. When is it appropriate for the Service Consumer to make requests of the Service Manager directly, versus needing to go through the Policy/Governance bodies?

4. If a law enforcement officer wants access to a user’s information, whom do they make this request to? What paperwork is required?

5. While each of the IAM Service roles has designated responsibilities, what is the authoritative “chain of command” when decisions must be made or policy and procedures enforced.

6. Will there be steering committees formed? A configuration control board?

7. Should there be a Center of Excellence formed?

8. Who will review submitted requests for purpose, benefit, value, cost savings, longevity, and risk? These reviews could be approved, denied, or delayed on consensus.

9. Will there be an IAM Visioning Group that does not perform governance per se, but has more of shared decision making and priority setting role?
Appendix H – MFTS File Naming Convention

Each file submitted by an authoritative publishing system will contain the following attributes as part of the file name. This data is critical to both the correct processing and identification of files and can contain no blanks or white space.

File ID Construction Convention

\[ \text{[Customer ID]}\text{-[File Creation DateTimeGroup]}\text{-[Customer File ID]}\text{-[Movement Group ID]}\text{-[File Type ID]}\text{-[Reference ID]}\text{-[Customer String]}\text{-[Extension]} \]

1. Customer ID – 4 position Alphanumeric Identifier issued by the system to registered customers. The customer ID represents a logical endpoint node in the MFTS network. Multiple logical endpoints may exist on a single physical server – for example in the case of an application-hosting server with multiple applications residing on it. Each application that participates in the MFTS network as an endpoint must have its own Customer ID. Files distributed by the MFTS are delivered on the basis of one copy per endpoint.

1. File Creation DateTimeGroup (DTG) – CCYYMMDDhhmmss – century year month day hour minute seconds

1. Customer File ID – 2 position Numeric Identifier determined by the customer. Needs to be unique within a DTG. Range 0-99. This number is always represented as 2 digits, eg. 00, 01, 02, …99

1. Movement Group ID – 4 position alphanumeric identifier issued by the system when a transfer configuration record is created. This ID tells the system which transfer record is applicable to this file allowing it to route the file correctly. This effectively provides the addressing instructions for the file in the absence of an address label and makes multiple addressees possible. This element is not guaranteed to remain consistent throughout MFTS processing so consumer applications should not use it to control processing.

1. File Type ID – A 5 position alphanumeric identifier for use by the target system in processing the file. This value will typically identify the file as being a specific publication that should have meaning to consuming endpoints.

1. Reference ID - Optional ID that combines the Customer ID, File Creation DateTimeGroup, and Customer File ID of a previous file that this file references. If there is no previous file to reference, this group should contain nothing which will result in 2 segment separators being created next to each other.

1. Customer String – A customer created string to help humans looking at logs, directory entries, etc. group and locate files manually. Does not need to be unique at any level but must insure that the total length of the filename does not exceed 128 characters including the extension. The delimiter for this string must be included even if the string is null.

1. Extension – A 3 position Alpha Identifier extension that identifies the type of file. Acceptable values are: txt, csv, dat, xml. Files that are in the process of being written must use the ‘.tmp’ extension to identify them as in process. MFTS pickup routines will not collect any files ending in ‘.tmp’.
Developing an Identity and Access Management Service

WARNING:

Your process must write files with the ‘.tmp’ extension during transfer to the MFTS, then rename the files to one of the acceptable data file extensions. Failure to follow this procedure could result in data corruption including partial record collection and record loss.

Definitions follow:

- Alphanumeric Identifier: (a-z), (A-Z), (0-9), ( underscore)
- Numeric Identifier: (0-9)
- Segment separator: - (dash)
- Extension separator: . (period)
- Alpha Identifier: (a-z) – generally lower case

Examples:

Example 1:

[Customer ID] = UIDS
[File Creation DateTimeGroup] = 20080329144533
[Customer File ID] = 01
[Movement Group ID] = UID2
[File Type ID] = UIDR
[Reference ID] = NCWS2008032912220301
[Customer String] = UID Response
[Extension] = csv

Filename: UIDS-20080329144533-01-UID2-UIDR1-NCWS2008032912220301-UIDResponse.csv

Example 2:

[Customer ID] = NCWS
[File Creation DateTimeGroup] = 20080115122243
[Customer File ID] = 06
[Movement Group ID] = 1001
[File Type ID] = UIDSB
[Reference ID] = [NULL]
[Customer String] = Burns_High_School
[Extension] = txt

Filename: NCWS-20080115122243-06-1001-UIDSB--Burns_High_School.txt
Appendix I – NCWISE Student Demographics Extract Data Definitions

Purpose: Daily export of Student Demographics data from NCWISE

Extract Filename: 1NCW-20110310103414-00-2602-SUREQ--NCWISE.zip  File Type: zip  Delimiter: Tab
Last Updated: 2/28/12 5:52 PM  MGID: 2602  Escape: none

Sample Filename:

Population:
• Extract contains Active Student Records from NCWISE (WITHDRAW_DATE is null, and REGISTRATION_DATE is not null)

Fields:

<table>
<thead>
<tr>
<th>Col</th>
<th>Field</th>
<th>Size</th>
<th>Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PUPIL_NUMBER</td>
<td>9</td>
<td>Alpha</td>
<td>NCWISE Student ID. Pupil number is generated by the state and is unique to each student. Pupil Number contains leading zeros.</td>
<td>012345678</td>
</tr>
<tr>
<td>2</td>
<td>LAST_NAME</td>
<td>30</td>
<td>Alpha</td>
<td>(LEGAL_NAME) Student legal last name</td>
<td>Smith</td>
</tr>
<tr>
<td>3</td>
<td>FIRST_NAME</td>
<td>30</td>
<td>Alpha</td>
<td>Student First name</td>
<td>John</td>
</tr>
<tr>
<td>4</td>
<td>SECOND_NAME</td>
<td>40</td>
<td>Alpha</td>
<td>Middle/Maiden Name</td>
<td>Andrews</td>
</tr>
<tr>
<td>5</td>
<td>LAST_NAME_SUFFIX</td>
<td>4</td>
<td>Alpha</td>
<td>Student’s last name suffix.</td>
<td>Jr., II, III, etc</td>
</tr>
<tr>
<td>6</td>
<td>BIRTH_DATE</td>
<td>10</td>
<td>Alpha</td>
<td>Student birth date MM/DD/YYYY</td>
<td>03/15/2001</td>
</tr>
</tbody>
</table>
Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th></th>
<th>Field Name</th>
<th>Length</th>
<th>Type</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>PHYSICAL_STREET_ADDRESS</td>
<td>37</td>
<td>Alpha</td>
<td>Student physical street address. (STREET_NUMBER space STREET_NAME)</td>
<td>123 Main St</td>
</tr>
<tr>
<td>9</td>
<td>APARTMENT</td>
<td>10</td>
<td>Alpha</td>
<td>Student apartment number or letter</td>
<td>B</td>
</tr>
<tr>
<td>10</td>
<td>POSTAL_BOX</td>
<td>6</td>
<td>Alpha</td>
<td>Student Post Office Box number</td>
<td>1234</td>
</tr>
<tr>
<td>11</td>
<td>CITY</td>
<td>30</td>
<td>Alpha</td>
<td>The city in which the student lives. (MUNICIPALITY_DESC from MUNICIPALITIES table).</td>
<td>Aberdeen</td>
</tr>
<tr>
<td>12</td>
<td>STATE</td>
<td>4</td>
<td>Alpha</td>
<td>The standard two-letter state postal abbreviation for the state in which the student lives. Note: NCWISE field size is 4. (PROVINCE)</td>
<td>NC</td>
</tr>
<tr>
<td>13</td>
<td>ZIP_CODE</td>
<td>10</td>
<td>Alpha</td>
<td>The postal zip code for the student address. (POSTAL_CODE)</td>
<td>28888</td>
</tr>
<tr>
<td>14</td>
<td>MAILING_ADDRESS</td>
<td>150</td>
<td>Alpha</td>
<td>The address to which correspondence is mailed. This address can be the same as the property address, or it may be different.</td>
<td>543 Creek Rd APT# 123</td>
</tr>
<tr>
<td>15</td>
<td>PHONE_NUMBER</td>
<td>10</td>
<td>Alpha</td>
<td>The home phone number of the student. (PHONE)</td>
<td>1234567890</td>
</tr>
<tr>
<td>16</td>
<td>GRADE</td>
<td>2</td>
<td>Alpha</td>
<td>Grade of the student upon admission into the school</td>
<td>12</td>
</tr>
<tr>
<td>17</td>
<td>HOME_LANGUAGE_SURVEY</td>
<td>1</td>
<td>Alpha</td>
<td>Home Language Survey has been returned. Values: Y, N</td>
<td>Values: Y, N</td>
</tr>
<tr>
<td>18</td>
<td>LANGUAGE_CODE</td>
<td>5</td>
<td>Alpha</td>
<td>Home Language Code, primary 147erive147e code. See LANGUAGE_CODES table</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>LANGUAGE_DESC</td>
<td>30</td>
<td>Alpha</td>
<td>Home Language Description, primary language. From LANGUAGE_CODES table</td>
<td>English</td>
</tr>
<tr>
<td>20</td>
<td>COUNTY</td>
<td>6</td>
<td>Alpha</td>
<td>Code for county of residence. See COUNTY_CODES table</td>
<td>025</td>
</tr>
<tr>
<td>21</td>
<td>COUNTY_DESC</td>
<td>50</td>
<td>Alpha</td>
<td>County description of residence. From COUNTY_CODES table</td>
<td>Cabarrus</td>
</tr>
<tr>
<td>22</td>
<td>CITY_OF_BIRTH</td>
<td>30</td>
<td>Alpha</td>
<td>Student city of birth</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>STATE_PROV_OF_BIRTH</td>
<td>3</td>
<td>Alpha</td>
<td>The standard two-letter state postal abbreviation for the state in which the student was born. NOTE: NCWISE field size is 3.</td>
<td>NC</td>
</tr>
</tbody>
</table>
### Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th></th>
<th>Field</th>
<th>Length</th>
<th>Type</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>COUNTRY_OF_BIRTH_CODE</td>
<td>3</td>
<td>Alpha</td>
<td>Country Code where student was born (COUNTRY_OF_BIRTH). See COUNTRIES table</td>
<td>33</td>
</tr>
<tr>
<td>25</td>
<td>COUNTRY_OF_BIRTH_DESC</td>
<td>30</td>
<td>Alpha</td>
<td>Country name where student was born. (COUNTRY_DESC from COUNTRIES table)</td>
<td>Botswana</td>
</tr>
<tr>
<td>26</td>
<td>MOTHERS_MAIDEN_NAME</td>
<td>40</td>
<td>Alpha</td>
<td>Not populated from NCWISE data, repository no longer needs this field.</td>
<td>NULL</td>
</tr>
<tr>
<td>27</td>
<td>NCWISE_LEA</td>
<td>9</td>
<td>Alpha</td>
<td>NCWISE Board/District/LEA identifier, up to 3 characters. (BSID from SCHOOLS table matched via SCHOOL in STUDENTS table)</td>
<td>57</td>
</tr>
<tr>
<td>28</td>
<td>SCHOOL</td>
<td>9</td>
<td>Alpha</td>
<td>NCWISE numeric school code combines LEA code and school. From STUDENTS table</td>
<td>57057</td>
</tr>
<tr>
<td>29</td>
<td>LEA_SCHOOL_CODE</td>
<td>6</td>
<td>Alpha</td>
<td>DPI school designation including LEA and school number.</td>
<td>60G000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>School Code definition FFFLL – EDDIE Format:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FIRST 3-DIGITS FFF:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>001-009</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Regional Education – Service Alliances/Consortia</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>01A-995</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LEAs (When all positions are numeric)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Charter schools (When first 2 positions are numeric and 3rd position is alphabetic)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Special LEAs:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>209 – Cherokee Central</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>269 – Fort Bragg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>679 – Camp Lejeune</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>997 – Dept of Human Resources</td>
<td></td>
</tr>
</tbody>
</table>
Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th>LEA_CODE</th>
<th>Length</th>
<th>Type</th>
<th>LEA Code definition EDDIE Format:</th>
</tr>
</thead>
<tbody>
<tr>
<td>998 – Office of Juvenile Justice</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAST 3-DIGITS LLL:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000 for LEAs and charter schools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>300 or greater for schools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>3</td>
<td>Alpha</td>
<td>LEA Code if all positions are numeric</td>
</tr>
<tr>
<td>Charter school Code if first 2 positions are numeric and 3rd position is alphabetic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Special LEAs:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>209 – Cherokee Central</td>
<td>60G</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Developing an Identity and Access Management Service

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>SCHOOL_CODE</td>
<td>3</td>
<td>Alpha</td>
</tr>
<tr>
<td>32</td>
<td>GENDER</td>
<td>1</td>
<td>Alpha</td>
</tr>
<tr>
<td>33</td>
<td>MINORITY_CODE</td>
<td>3</td>
<td>Alpha</td>
</tr>
<tr>
<td>34</td>
<td>MINORITY_DESC</td>
<td>30</td>
<td>Alpha</td>
</tr>
<tr>
<td>35</td>
<td>HISPANIC_ETHNICITY</td>
<td>1</td>
<td>Alpha</td>
</tr>
<tr>
<td>36</td>
<td>AMIN_IND</td>
<td>1</td>
<td>Alpha</td>
</tr>
</tbody>
</table>

**SCHOOL_CODE**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Alpha</td>
<td></td>
</tr>
</tbody>
</table>

- 269 – Fort Bragg
- 679 – Camp Lejeune
- 997 – Dept of Human Resources
- 998 – Office of Juvenile Justice

**GENDER**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>(SEX)</td>
</tr>
</tbody>
</table>

- Values: M/F

**MINORITY_CODE**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>Alpha</td>
</tr>
</tbody>
</table>

- Currently, race/ethnicity in NC WISE is simply the old minority_code_1 field from the students’ table.
- But, because of new Federal requirements, the race/ethnicity value has been updated to come from a different area of NC WISE and it is a more complex value.
- This field uses function get_race_fnc to derive the new Minority Code value, which may be different in some cases from the old MINORITY_CODE_1 value.
- Values: AMIN=1, ASIA= 2, HISP=3, BLCK=4, WHTE=5, MULT=6, PACI=7

**MINORITY_DESC**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>Alpha</td>
</tr>
</tbody>
</table>

- This field uses function get_race_fnc to derive the new MINORITY_DESC values.
- White

**HISPANIC_ETHNICITY**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>Alpha</td>
</tr>
</tbody>
</table>

- Based on NCWISE STUDENTS table column MINORITY_CODE_1, if ‘3’ return Y.
- Values: Y/N

**AMIN_IND**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>Alpha</td>
</tr>
</tbody>
</table>

- Based on NCWISE STUDENT_HUMAN_RACES table column HUMAN_RACES_CODE column, if 1 return Y. (American Indian/Alaskan Native)
- Values: Y/N
<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>ASIAN</td>
<td>1</td>
<td>Alpha</td>
<td>Based on NCWISE STUDENT_HUMAN_RACES table column HUMAN_RACES_CODE column, if 2 return Y.</td>
<td>Values: Y/N</td>
</tr>
<tr>
<td>38</td>
<td>BLACK</td>
<td>1</td>
<td>Alpha</td>
<td>Based on NCWISE STUDENT_HUMAN_RACES table column HUMAN_RACES_CODE column, if 4 return Y.</td>
<td>Values: Y/N</td>
</tr>
<tr>
<td>39</td>
<td>WHITE</td>
<td>1</td>
<td>Alpha</td>
<td>Based on NCWISE STUDENT_HUMAN_RACES table column HUMAN_RACES_CODE column, if 5 return Y.</td>
<td>Values: Y/N</td>
</tr>
<tr>
<td>40</td>
<td>HAW_PI</td>
<td>1</td>
<td>Alpha</td>
<td>Based on NCWISE STUDENT_HUMAN_RACES table column HUMAN_RACES_CODE column, if 7 return Y. (Hawaiian/ Pacific Islander)</td>
<td>Values: Y/N</td>
</tr>
<tr>
<td>41</td>
<td>LEGAL_RES_DISTRICT_NUMBER</td>
<td>9</td>
<td>Alpha</td>
<td>Displays the LEA to which the student is zoned based on the student residence address. This functionality is only available if the LEA has selected this field for use in the Company File and the Board/Districts Table is populated.</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>PREVIOUS_SCHOOL_NUMBER</td>
<td>9</td>
<td>Alpha</td>
<td>Student’s previous school/district information populates if a student moves from one NC WISE school to another.</td>
<td>900312</td>
</tr>
<tr>
<td>43</td>
<td>DIPLOMA_TYPE</td>
<td>6</td>
<td>Alpha</td>
<td>Diploma Type Code. From DIPLOMAS table</td>
<td>AA</td>
</tr>
<tr>
<td>44</td>
<td>DIPLOMA_NAME</td>
<td>30</td>
<td>Alpha</td>
<td>Diploma Name. From DIPLOMAS table</td>
<td>FRC1 (7) 2009/10</td>
</tr>
<tr>
<td>45</td>
<td>MINISTRY_CODE</td>
<td>6</td>
<td>Alpha</td>
<td>Diploma Name From DIPLOMAS table. This is used by CTE as &quot;Course of study&quot;.</td>
<td>FRC1</td>
</tr>
<tr>
<td>46</td>
<td>REGISTRATION_DATE</td>
<td>Date</td>
<td></td>
<td>Student’s registration date. Date student is &quot;in the seat&quot;.</td>
<td>18-AUG-10</td>
</tr>
<tr>
<td>47</td>
<td>AIG_FLAG</td>
<td>1</td>
<td>Alpha</td>
<td>Academically or intellectually gifted. One character values: B= 01-academically gifted in reading and math - AG R= 20-academically gifted in reading - AR M= 19-academically gifted in math - AM or Null in EXCEPTIONALITY_CODE column of the SPED_EXCEPTIONALITIES table, matched on</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Field Name</td>
<td>Max</td>
<td>Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-------------------------</td>
<td>-----</td>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>EMAIL_ADDRESS</td>
<td>100</td>
<td>Alpha</td>
<td>Student email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Note: Parentheses indicate NCWISE column name when different from APEX</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Repository column name.)</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>CD_PROGRAM_CODE</td>
<td>9</td>
<td>Alpha</td>
<td>Career development program code - intended career cluster</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Value descriptions are found in CD_PROGRAM_CODES table.</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>MOD_USER</td>
<td>30</td>
<td>Alpha</td>
<td>User that last modified the record</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>MOD_DATE</td>
<td></td>
<td>Date</td>
<td>Date record was last modified</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>RUN_DATE</td>
<td></td>
<td>Timestamp</td>
<td>Timestamp when record loaded in to repository - YYYYMMDD:HH24:MI:SS</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: Parenthesis indicate NCWISE column name when different from APEX Repository column name.
Appendix J – UID Staff System Extract Data Definitions

Purpose: M-F export from the UID Staff System of staff identification data.

Extract Filename: UID All Staff Extract Version 1.1
File Type: 00000
Delimiter: Tab

Last Updated: 2/28/12 5:52 PM
MGID: 1022
Escape: None

Sample Filename: UID1-20111011060044-00-1022-00000-0-ALLSTAFF_V_1_1.txt

Population:
• Includes all staff records

Fields:

<table>
<thead>
<tr>
<th>Col</th>
<th>Field</th>
<th>Size</th>
<th>Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Staff ID</td>
<td>10</td>
<td>Text</td>
<td>The identifier assigned by the eScholar Uniq-ID for Staff system.</td>
<td>1234567890</td>
</tr>
<tr>
<td>2</td>
<td>School Code</td>
<td>6</td>
<td>Text</td>
<td>The staff member’s organizational location.</td>
<td>367</td>
</tr>
<tr>
<td>3</td>
<td>District Code</td>
<td>8</td>
<td>Text</td>
<td>The staff member’s district.</td>
<td>400</td>
</tr>
<tr>
<td>4</td>
<td>Last Name Long</td>
<td>60</td>
<td>Text</td>
<td>The staff member’s legal last name (surname).</td>
<td>Smith</td>
</tr>
<tr>
<td>5</td>
<td>First Name Long</td>
<td>60</td>
<td>Text</td>
<td>This field should be the staff member’s legal first name.</td>
<td>John</td>
</tr>
<tr>
<td>6</td>
<td>Middle Name</td>
<td>60</td>
<td>Text</td>
<td>This field should be the staff member’s legal middle name. This value can be either the middle initial or the full middle name.</td>
<td>Thomas</td>
</tr>
<tr>
<td>7</td>
<td>Name Suffix</td>
<td>10</td>
<td>Text</td>
<td>The staff member’s suffix for his/her surname, if applicable.</td>
<td>Jr.</td>
</tr>
<tr>
<td>8</td>
<td>Gender Code</td>
<td>6</td>
<td>Text</td>
<td>The staff member’s gender.</td>
<td>M or F</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Type</td>
<td>Description</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------</td>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Birth Date</td>
<td>10</td>
<td>The staff member’s date of birth.</td>
<td>10/01/1995</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Alternate Staff ID</td>
<td>20</td>
<td>The identifier used in the local data system to uniquely identify the staff member. The primary purpose of this field is to provide a mechanism for the local agency to import the Staff ID assigned by the system back into their local systems.</td>
<td>3432439a4</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Social Security Number</td>
<td>11</td>
<td>The staff member’s social security number.</td>
<td>123455931</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Hispanic Ethnicity Indicator</td>
<td>3</td>
<td>This field identifies whether or not the staff member is of Hispanic or Latino descent.</td>
<td>0 or 1</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Ethnic Code Short</td>
<td>10</td>
<td>The new Race and Ethnicity (RE) codes allow staff members to be identified by more than one race and/or ethnicity. The new RE codes more accurately reflect a staff member’s racial and ethnic background by not limiting responses to only one racial or ethnic category, and expand reporting options.</td>
<td>100111</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 or 1: HI7 (position 1)</td>
<td></td>
<td>(identified as: HI7, BL7, PI7, WH7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 or 1: AM7 (position 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 or 1: AS7 (position 3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 or 1: BL7 (position 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 or 1: PI7 (position 5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 or 1: WH7 (position 6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Race or Ethnicity Subgroup code</td>
<td>2</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Address 1</td>
<td>30</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Address 2</td>
<td>30</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>City</td>
<td>25</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>State</td>
<td>2</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Full Zip Code</td>
<td>10</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Job Class Code</td>
<td>2</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3rd Position: AS7 - Asian (Required; 0=No, 1=Yes)

4th Position: BL7 - Black (Required; 0=No, 1=Yes)

5th Position: PI7 - Native Hawaiian or Other Pacific Islander (Required; 0=No, 1=Yes)

6th Position: WH7 - White (Required; 0=No, 1=Yes)

Example: 000101, would be interpreted as Non-Hispanic, Black, White

- Race or Ethnicity Subgroup code: The staff member’s racial or ethnic subgroup. For example, if the staff member is American Indian/Alaska Native, this field could represent the specific tribe to which he/she belongs.

- Address 1: The street name and number of the staff member’s home address.

- Address 2: This field should contain additional information concerning the staff member’s home address, such as apartment number.

- City: The city of the staff member’s home address.

- State: The state of the staff member’s home address.

- Full Zip Code: The official US postal code for the staff member’s home address.

- Job Class Code: The staff member’s primary position within the location and/or district.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Original Hire Date</td>
<td>10</td>
<td>Date as Text</td>
<td>The date the location/district originally hired the staff member.</td>
</tr>
<tr>
<td>22</td>
<td>Highest Degree Earned</td>
<td>20</td>
<td>Text</td>
<td>The type of degree or certificate the staff member has earned. If the staff member has multiple degrees/certificates, the highest level should be used.</td>
</tr>
<tr>
<td>23</td>
<td>Annual Salary</td>
<td>10</td>
<td>Text</td>
<td>The total compensation for the staff member for services provided to the location/district. This number should include any additional stipends the staff member receives from the location/district for such services as coaching athletic teams or moderating after school activities, but still within the context of the primary designation.</td>
</tr>
<tr>
<td>24</td>
<td>Full Staff Name</td>
<td>255</td>
<td>Text</td>
<td>The staff member’s full name, using the form Last Name, First Name (e.g., Doe, Jane). The middle name can also be included. This value will be primarily used for reporting and/or other user interface display purposes.</td>
</tr>
<tr>
<td>25</td>
<td>Itinerant Teacher</td>
<td>3</td>
<td>Text</td>
<td>Indicates whether or not the staff member has been classified as an Itinerant Teacher (on loan from another agency or a staff member who provides services in more than one agency).</td>
</tr>
<tr>
<td>26</td>
<td>Active/Inactive Indicator</td>
<td>1</td>
<td>Text</td>
<td>The staff member’s current status (e.g., Active/Inactive) in the location/district.</td>
</tr>
<tr>
<td>27</td>
<td>Previous Last Name</td>
<td>60</td>
<td>Text</td>
<td>The former last name of the staff member, if applicable. The Previous Last Name data can include changes in last name due to marriage, divorce, legal name change or other forms of name changes.</td>
</tr>
<tr>
<td>28</td>
<td>Last Update</td>
<td>10</td>
<td>Date as Text</td>
<td>The date of the last update for this staff record.</td>
</tr>
</tbody>
</table>
# Developing an Identity and Access Management Service

## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Affiliation</strong></td>
<td>Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alumni, guest, volunteer, parent, guardian, etc.</td>
</tr>
<tr>
<td><strong>Attestation</strong></td>
<td>To determine each user's current access to a target system and having a reviewer, specific that resource, verify that the user is in fact entitled that access.</td>
</tr>
<tr>
<td><strong>Attribute</strong></td>
<td>A single piece of information associated with a digital identity. Examples of an attribute are name, phone number, and institution affiliation.</td>
</tr>
<tr>
<td><strong>Authentication (AuthN)</strong></td>
<td>Assertion of “who you are”. Usually gated by login/password</td>
</tr>
<tr>
<td><strong>Authorization (AuthZ)</strong></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><strong>Credential</strong></td>
<td>An electronic identifier (e.g., logon id, username) and corresponding personal secret (e.g., password, PIN) associated with an electronic identity. An identity credential typically is issued to the person to enable that person to gain access to the applications or other resources that to controlled and/or accessed.</td>
</tr>
<tr>
<td><strong>DPI</strong></td>
<td>North Carolina Department of Public Instruction[^33]</td>
</tr>
<tr>
<td><strong>Entitlement</strong></td>
<td>Entitlements are a mechanism for centrally defining the applications and services to which user may be given authorization.</td>
</tr>
<tr>
<td><strong>ESSO</strong></td>
<td>Enterprise Single Sign On</td>
</tr>
<tr>
<td><strong>ETL</strong></td>
<td>Extract, Transform, Load</td>
</tr>
<tr>
<td><strong>Federation / SAML IdP, SP, DS (WebSSO)</strong></td>
<td>AuthN from home institution to AuthZ by remote web-based app, usually orchestrated through user’s web browser.</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>A group is a collection of IAM users. You might think of group membership as a simple list; can be added to or removed from a group. A user can belong to multiple groups. Groups can belong to other groups. Groups can be granted permissions using access control policies. This makes it easier to manage permissions for a collection of users, rather than having to manage permissions for each individual user.</td>
</tr>
<tr>
<td><strong>Group Management</strong></td>
<td>Stores information about which identities are in particular groups. Examples include Custc web-based tool, Grouper &amp; AD, home-grown using LDAP, etc.</td>
</tr>
<tr>
<td><strong>UID</strong></td>
<td>eScholar Uniq-ID[^34]</td>
</tr>
</tbody>
</table>

[^34]: [http://www.ncpublicschools.org/cedars/uniqueid/](http://www.ncpublicschools.org/cedars/uniqueid/)
### Developing an Identity and Access Management Service

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>MFTS</td>
<td>Managed File Transfer System</td>
</tr>
<tr>
<td>NCID</td>
<td>North Carolina Identity Management System&lt;sup&gt;35&lt;/sup&gt;</td>
</tr>
<tr>
<td>NCWISE</td>
<td>North Carolina Window on Student Education&lt;sup&gt;36&lt;/sup&gt;</td>
</tr>
<tr>
<td>ODS</td>
<td>Operational Data Store</td>
</tr>
<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>RFI</td>
<td>Request for Information</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposals</td>
</tr>
<tr>
<td>Role</td>
<td>Usually this refers to an business/enterprise role that roughly equates to a job title, position, or responsibility (e.g. student, teacher, principle, technician, teacher’s assistant system administrator, etc.). A role in the context of IAM implies certain privileges to access resources (such as applications, data, or administrative functions). Roles are important for both user enablement and user access control. Using roles in the context of IAM is often called Role-Based Access Control (RBAC).</td>
</tr>
<tr>
<td>RSO</td>
<td>Reduced Sign On</td>
</tr>
<tr>
<td>RttT</td>
<td>Race to the Top&lt;sup&gt;37&lt;/sup&gt;</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>

<sup>35</sup> [https://ncid.nc.gov](https://ncid.nc.gov)

<sup>36</sup> [http://www.ncwise.org/](http://www.ncwise.org/)

<sup>37</sup> [http://www2.ed.gov/programs/racetothetop/index.html](http://www2.ed.gov/programs/racetothetop/index.html)
This page is left blank intentionally