Meeting Agenda

• IAM Talking Points Review (2 metaphors)
  • What is Identity and Access Management (IAM)?
  • Why IAM matters?
  • Why is Improving IAM Challenging?

• Formalizing the IAM Program
  • Advisory Committee – Strategic Priorities
  • Access Management Audit & Website
  • Service Definitions & Delivery
  • Staffing Strategy
  • Strategic Roadmap

• The “BIG FINISH” – A proposed branding campaign
What is Identity and Access Management (IAM)?
Identity and Access Management refers to a set of business processes and supporting technologies that enable the **creation, maintenance, and use of a digital identity**.

Simply put, Identity and Access Management is about giving the **Right User** the **Right Access** to the **Right Resource** for the **Right Reason** and maintaining a **Record** of who has Access to What.
Core IAM services

- **Identity** is whom someone or what something is, for example, the name by which something is known.
- **Authentication** is the process of confirming the correctness of the claimed identity.
- **Authorization** is the approval, permission, or empowerment for someone or something to do something.
- **Auditing** is an official examination or verification of accounts and records.
Airport IAM Analogy
Airport IAM Analogy

Identification ----> Authentication ----> Authorization ----> Auditing ----> Administration
Core IAM Services

1. Identification
2. Authentication
3. Authorization

Audit

Protected Resource

Administration
Why Identity and Access Management (IAM) matters?
Everyone and Everything is Impacted by IAM...
Why is **IAM** important?

Identity and Access Management Impacts Everyone and Everything

- Ensures the digital safety and privacy needs of students, staff and faculty are being met.
- Ensures security of sensitive information and campus application and computing resources.
- Provides for single sign-on so that our community does not need to maintain a multitude of passwords.
- Prevents duplication of individuals among the various systems.
- Streamlines and Automates the provisioning process.
- Reduces administrative overhead for managing access and access related issues in the current environment.
What is the Vision for IAM at USC?

The University of South Carolina’s IAM Vision seeks to:

- Simplify and Improve the User Experience
- Enhance our Information Security and Compliance Posture
- Enable Research and Collaboration
- Facilitate Technology Innovation
Why is Improving IAM Challenging?
Plan for Identity and Access Management?
Formalizing IAM Program
Identity and Access Management Advisory Committee
<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joseph Bass</td>
<td>Undergraduate Student Body Vice President, Columbia campus</td>
</tr>
<tr>
<td>Glenn Bunton</td>
<td>Director of Library Technology Services</td>
</tr>
<tr>
<td>Dagmara Bruce</td>
<td>Director of Human Resources, USC Upstate</td>
</tr>
<tr>
<td>Joey Derrick</td>
<td>Director of Financial Aid, Columbia campus</td>
</tr>
<tr>
<td>Bob Dyer</td>
<td>Director of Information Technology, Palmetto College</td>
</tr>
<tr>
<td>Michael Galbreth</td>
<td>Professor, Department of Management Science, Darla Moore School of Business</td>
</tr>
<tr>
<td>Matt Heightland</td>
<td>Server Manager, USC Beaufort</td>
</tr>
<tr>
<td>Brad Holt</td>
<td>PeopleSoft Finance Program Manager, Administration and Finance</td>
</tr>
<tr>
<td>Stacy Lee</td>
<td>Human Resources Information Systems Manager, Columbia campus</td>
</tr>
<tr>
<td>Aaron Marterer</td>
<td>Registrar, Columbia campus</td>
</tr>
<tr>
<td>Darryl Nash</td>
<td>Identity and Access Management Program Manager, Division of Information Technology</td>
</tr>
<tr>
<td>Roscoe Patterson</td>
<td>Assistant Director of IT Audit, Audit and Advisory Services</td>
</tr>
<tr>
<td>James Perry</td>
<td>Associate Vice President and Chief Information Security Officer</td>
</tr>
<tr>
<td>Clint Saidy</td>
<td>President, Graduate Student Association</td>
</tr>
<tr>
<td>Randy Shelley</td>
<td>Executive Director of Application Services, Division of Information Technology</td>
</tr>
<tr>
<td>Karen Smith</td>
<td>OneCarolina Coordinator, USC Aiken</td>
</tr>
<tr>
<td>Ben Torkian</td>
<td>Senior Applications Scientist, Research Cyberinfrastructure</td>
</tr>
<tr>
<td>Oleg Uvarov</td>
<td>Facilities IT Manager, Facilities</td>
</tr>
<tr>
<td>Mary Wagner</td>
<td>Associate Vice President for Enrollment Management and Executive Director of Undergraduate Admissions, Columbia</td>
</tr>
</tbody>
</table>
2018 IAM Program Priorities

1. **Provisioning Process Improvements**
   - Improve the **timeliness of identity creation and provisioning**
   - Improved method for communicating credentials to users
   - Simplified process for managing sponsored and resource accounts
   - Reduce administrative overhead by **improving identity matching algorithms** to minimize the number of duplicate accounts being created

2. **Simplify the User Experience**
   - Reduce the number of credentials
   - Strategic **consolidation of fragmented IAM services**
   - Improved user **self-service experience**
   - Update and improve IAM program web presence
   - **Relax password** change frequency and complexity **requirements**
   - **Simplify** user experience with multi-factor authentication

3. **Enhance the Information Security Posture**
   - Expand use of **multi-factor authentication** to other university systems
   - Develop an IAM audit/reporting capability
   - Align IAM practices with revised NIST800-63-3 security guidelines
   - Upgrade/enhance IAM technical infrastructure to ensure appropriate redundancy, performance, and availability

4. **Develop Strategic Roadmap for IAM Program**
   - Support for automatic provisioning changes when users change roles
   - **Support** for role-based, group-based, and other attribute-based authorizations
   - Better support for users with multiple affiliations with the university
DOIT Strategic Priorities

Over the next four years, the Division of Information Technology will focus on the following Strategic Priorities...

1. Advance the academic and research missions of the university
2. Enhance the student digital experience
3. Improve administrative efficiencies
4. Establish a best-in-class service delivery model
5. Provide a reliable and flexible technology infrastructure

Provisioning Process Improvements
Simplify the User Experience
Enhance the Information Security Posture
Develop Strategic Roadmap for IAM Program
Establishing the IAM “Program”

• IAM Advisory Committee
• IAM Strategic Priorities
  • Transition IAM services off the mainframe (PeopleSoft HCM)
  • IAMAC Program Priorities
• IAM Website
  • Satisfy AAS findings in recent audit
  • Consolidate, organize, simplify, and update
• IAM Service Definitions & Delivery Strategy
• IAM Staffing
• IAM Program Roadmap
1) Clarification of Access Management Policies

The Chief Information Security Officer's (CISO) office agrees that Data Stewards are likely unaware of the requirement for periodic reviews. Although several policies and standards state the requirement, consolidating that information into a summary and sharing that with Data Stewards will increase awareness.

The CISO's office will:
* Draft guidance that clarifies Data Stewards' responsibility to perform user access reviews.
* Make this information available on security.sc.edu.

The CISO's office will also collaborate with the Chief Data Officer (CDO), who will:
1.) Share this guidance with Data Stewards (one Quarter after CISO makes available), and
2.) Maintain records of communication (begin one Quarter after CISO makes available and annually thereafter, as well as during iterative training activities).

4) Identity and Access Management Program

The CISO's office agrees there is a need to advertise the creation of the Identity and Access Management (IAM) program.

To address this, the CISO will:
* Establish the IAM program's web presence; and
* Publish important IAM-related guidance, such as the requirement to review account access.

The CDO will ensure Data Steward's are aware of their responsibility to maintain an inventory of information systems and system owners.

To that end, the CDO will:
* Investigate tools to collect and store inventories in a central location (by the end of Q3-2018).
* Collaborate with the CISO to establish a process where Data Stewards attest whether their information systems comply with the program (by the end of Q4-2018).
Identity and Access Management Program

**Getting Started >>**
View important information for end users, system administrators, security liaisons and data owners.

**Announcements>>**
Read the latest releases from our office about the identity and access management program and future plans.

**Policies & Standards>>**
Explore the various identity and access management obligations of the university and its members.

**Services>>**
Explore the various identity and access management obligations of the university and its members.

**Technologies>>**
Learn more about the technologies that enable the identity and access management services.

**About Us>>**
Get to know our mission, values, and future plans.
Getting Started
• User – faculty, staff, students, affiliates, and guests
• System Admin – how do I setup my app to use authentication?
• Security Liaison – what security controls does my OU need to implement?
• Data Steward – what am I responsible for?

Announcements
• Program updates
• Stories of interest
• Miscellaneous IAM related communications

Policy & Standards
• Link to same pages as security policy

Services
Identity Services:
NetID
VIPID
USCID

Authentication Services:
CAS (w/ Single-Sign-On)
Shibboleth (w/ Federation)
Active Directory
Multifactor Authentication

Authorization Services:
User Attributes
Group Memberships

Directory Services:
Enterprise Directory
Active Directory
VIPID LDAP
BlackBoard Local Users Directory

Administration Services:
Oracle Identity Management
Umpire Identity Resolution
Provisioning
Self-Service

Technologies
• CAS
• SAML
• LDAP
• DUO
• OIM
• Self-Service
• Etc.

About Us
• Vision
• Mission
• Advisory Committee
• Strategy
IAM Service Definitions & Delivery
Identity and Access Management
Staffing Plan
IAM Staffing Strategy

• IAM Roles:
  • IAM Program Manager ($125K) – FY19 New Budget Request for (1) Prog. Mgr.
  • IAM Developers ($95K) – IBM providing ~180 hours/month (1.125 FTE)
    • 180 hours = ~25% of IBM’s Application Infrastructure Engineering (AIE) Total Capacity
  • IAM Analyst/Consultant ($85K) – FY19 New Budget Request for (1) Analyst
  • IAM Administrator ($70K) – FY19 New Budget Request for (2) Administrators
    • IBM resources are performing some of these duties today
      • ~100 hours/month supporting the DIRT process
      • ~700 tickets in last 6 months = 3,963 hours of effort

• Phase One Budget Request: $350K + fringe benefits (recurring)
  • Will likely need additional cash investments to contract expert skills in support of specific projects (i.e. self-service app development, Oracle RAC implementation, additional OIM development capacity, etc.)

• Phase Two Staffing Request: TBD