IDENTITY MANAGEMENT AND COMMON SYSTEM ACCESS

CALIFORNIA STATE UNIVERSITY,
SAN MARCOS

Audit Report 12-48
January 16, 2013

Members, Committee on Audit

Henry Mendoza, Chair
William Hauck, Vice Chair
Lupe C. Garcia Steven M. Glazer
Hugo N. Morales Glen O. Toney

Staff

University Auditor: Larry Mandel
Senior Director: Michael Caldera
IT Audit Manager: Greg Dove

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
# CONTENTS

Executive Summary ...................................................................................................................................... 1

Introduction ................................................................................................................................................... 2
  Background .............................................................................................................................................. 2
  Purpose ..................................................................................................................................................... 3
  Scope and Methodology .......................................................................................................................... 4

## APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Chancellor’s Acceptance

## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CSU</td>
<td>California State University</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal Year</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>ICSUAM</td>
<td>Integrated California State University Administrative Manual</td>
</tr>
<tr>
<td>ISO</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITS</td>
<td>Information Technology Services</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2011, the Board of Trustees, at its January 2012 meeting, directed that Identity Management and Common System Access be reviewed. The Office of the University Auditor had previously reviewed some aspects of identity management and common system access in the 2008 and 2009 audits of Information Security and in the 2011 audits of Sensitive Data Security and Protection.

We visited the California State University, San Marcos campus from October 15, 2012, through October 31, 2012, and audited the procedures in effect at that time.

In our opinion, the operational and administrative controls over identity management and common system access in effect as of October 31, 2012, taken as a whole, were sufficient to meet the objectives stated in the “Purpose” section of this report. There were no major findings revealed during our review.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our audit of identity management and common system access did not examine controls over all common system authentication techniques, but was designed to assess management control and oversight, consistency of controls on a sample basis, and compliance with California State University guidance.
Identity management is a method to provide common access and authentication to systems and data through adherence to a common set of standards, identity attributes, data and data definitions, and identity management practices.

Each California State University (CSU) campus has implemented some form of identity management technology to govern access to their local systems and data. In addition, the CSU, through its identity and access management initiative, has implemented common identity management standards and practices to support a unified identity and access management infrastructure across the CSU system. This includes efforts at the campuses and the chancellor’s office to establish the identity authentication and authorization processes necessary to allow students, faculty, and staff to easily access courses, share resources, and conduct research across networked information systems.

Identity and access management technology enables authorized campus individuals to use their local campus digital identity credentials to gain access, as appropriate, to systemwide CSU resources and services. It will also enable secure transactions between education, business, and government partners.

Integrated California State University Administrative Manual (ICSUAM) §8000.0, Information Security Policy, dated April 19, 2010, represents the most recent and specific guidance to campuses regarding the security and protection over access to systems and data. It provides direction for managing and protecting the confidentiality, integrity, and availability of CSU information assets and defines the organizational scope of information security throughout the system.

The policy states that the Board of Trustees is responsible for protecting the confidentiality, integrity, and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

According to ICSUAM §8000.0, it is the collective responsibility of all users to ensure the confidentiality of information that the CSU must protect from unauthorized access, the integrity and availability of information stored on or processed by CSU information systems, and compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection. The policy further states that auxiliary organizations, external businesses, and organizations that use campus information assets must also follow the CSU Information Security Policy.

State Administrative Manual §5300 defines information security as the protection of information and information systems and equipment from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction. Pursuant to Government Code §11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures, and filing requirements issued by the Office of Information Security and Privacy Protection in the California Office of Information Security.
State Administrative Manual §5320 states that each agency must provide for the integrity and security of its information assets by identifying all automated files and databases for which the agency has ownership responsibility and ensuring that responsibility for each automated file or database is defined with respect to owners of the information within the agency, custodians of the information, users of the information, and classification of the information to ensure that each automated file or database is identified in accordance with law and administrative policy.

**PURPOSE**

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of identity management and common system access; to determine the adequacy of controls over the related processes; and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

The objective of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, without the need for redundant user administration. Use of identity federation standards can increase security and lower risk by enabling the CSU to identify and authenticate a user once, and then use that identity information across multiple systems. It can improve privacy compliance by allowing the user to control what information is shared, or by limiting the amount of information shared. Moreover, it can drastically improve the end-user experience by eliminating the need to login to multiple systems.

Within the overall audit objective, specific goals included determining whether:

- Cross-departmental administrative and managerial internal controls are in place, including delegations of authority and responsibility, oversight committees, executive-level reporting, and documented policies and procedures.

- A management framework is established to initiate and control the implementation of identity management within the organization, and management direction and support for identity management is communicated in accordance with business requirements and relevant laws and regulations.

- CSU campuses are participating in the federated model, which defines specific identity validation techniques, process controls, and monitoring.

- Responsibility for definitive identification of individuals is defined, and processes address acceptable forms of photo identification required prior to the assignment of user accounts.

- Responsibilities and procedures for the management of information processing and identity management architecture are defined, and technical security controls are integrated within systems and networks to ensure consistency of user account and password controls for all systems connected to this centralized authentication process.
Individual user access rights to systems, applications, and business processes are appropriately controlled through user identification and authentication techniques that are based on business and security requirements.

Formal monitoring and event reporting procedures are in place to identify information security events and weaknesses within the supporting servers and technologies, and communication of such security events is consistent and effective, allowing for timely corrective action.

The overall integration of information systems design, configuration, operation, use, and management are in conformance with statutory, regulatory, and contractual security requirements governing privacy and protected data; and the entire process is regularly reviewed for compliance with associated regulations.

SCOPE AND METHODOLOGY

The proposed scope of the audit, as presented in Action Item, Agenda Item 2 of the January 24 and 25, 2012, meeting of the Committee on Audit, stated that Identity Management and Common System Access would include review and compliance with Trustee policy, federal and state directives, systemwide guidance, and campus policies and procedures surrounding system authentication; procedures for technical specifications; program access considerations; technical architecture; and access provisioning and deprovisioning requirements.

Our study and evaluation were conducted in accordance with the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasizeed, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the administrative, compliance, operational, and technical controls over authorization processes used to validate the identity of users and ensure that users are appropriate, including security of the server hosting the directory services, the authentication process, and procedures used to create and maintain the user credentials. Specifically, we reviewed and tested:

- Information security policies and procedures.
- Identity management organizational structure and management framework.
- Directory architecture and administrative and technical procedures.
- Access and configuration controls over networks, systems, applications, business processes, and data.
- Authentication methodologies and technologies.
- Procedures to create and maintain user credentials.
- Support and maintenance of the servers used to support identity management systems.
Our testing and methodology was designed to provide a managerial level review of key practices over identity management and common system access. Our review did not examine all systems with independent authentication, but focused on those authentication techniques that were shared by multiple application systems. Our testing approach was designed to provide a view of the system security used to provide access to key networks and applications and to assess the associated identity validation methods.
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Karen S. Haynes</td>
<td>President</td>
</tr>
<tr>
<td>Candice Bebee</td>
<td>Assistant to the Vice President</td>
</tr>
<tr>
<td>Jane Cross</td>
<td>Director Payroll Services</td>
</tr>
<tr>
<td>Wayne Dilly</td>
<td>Operating Systems Analyst</td>
</tr>
<tr>
<td>April Grommo</td>
<td>Director, CMS Program</td>
</tr>
<tr>
<td>Randy Hall</td>
<td>Program Coordinator, IT Project Office</td>
</tr>
<tr>
<td>Linda Hawk</td>
<td>Vice President Finance and Administrative Services</td>
</tr>
<tr>
<td>Chris Lambert</td>
<td>Manager, Accounting and Systems Operations and Development</td>
</tr>
<tr>
<td>Penny Lanese</td>
<td>Information Technology Consultant</td>
</tr>
<tr>
<td>Teresa Macklin</td>
<td>Information Security Officer/Director, Enterprise Systems Group</td>
</tr>
<tr>
<td>Carol McAllister</td>
<td>Director Admissions and Outreach</td>
</tr>
<tr>
<td>Lisa McLean</td>
<td>Human Resources Manager</td>
</tr>
<tr>
<td>Diane Petersen</td>
<td>Analyst/Programmer, Database Group</td>
</tr>
<tr>
<td>Katy Rees</td>
<td>Assistant Vice President of Administration</td>
</tr>
<tr>
<td>Thomas Swanger</td>
<td>Registrar</td>
</tr>
<tr>
<td>Susan Thompson</td>
<td>Library Systems Coordinator</td>
</tr>
<tr>
<td>Wayne Veres</td>
<td>Dean and Chief Information Officer, Instructional and Informational Technology Services</td>
</tr>
<tr>
<td>Sarah Villarreal</td>
<td>Associate Dean Extended Learning</td>
</tr>
<tr>
<td>Deirdre Wallace</td>
<td>Faculty Personnel Generalist</td>
</tr>
</tbody>
</table>
January 16, 2013

MEMORANDUM

TO: Mr. Larry Mandel
    University Auditor

FROM: Timothy P. White
       Chancellor

SUBJECT: Draft Final Report 12-48 on
         Identity Management and Common Management Access
         California State University, San Marcos

In response to your memorandum of January 16, 2013, I accept the draft final report on Identity Management and Common Management Access, California State University, San Marcos.

TPW/amd