IDENTITY MANAGEMENT AND COMMON SYSTEM ACCESS

CALIFORNIA STATE UNIVERSITY,
MONTEREY BAY

Audit Report 12-47
December 22, 2012

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
Senior Auditor: Gordon Eng

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
Contents

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

Introduction................................................................................................................................................... 2
  Background................................................................................................................................................... 2
  Purpose..................................................................................................................................................... 4
  Scope and Methodology .......................................................................................................................... 6

Observations, Recommendations, and Campus Responses

Governance .................................................................................................................................................... 7
APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Campus Response
APPENDIX C: Chancellor’s Acceptance

ABBREVIATIONS

CIO Chief Information Officer
CSU California State University
I AM Identity and Access Management
ICSUAM Integrated California State University Administrative Manual
ISO Information Security Officer
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, Monterey Bay campus from October 8, 2012, through November 2, 2012, and audited the procedures in effect at that time.

Our study and evaluation did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on controls over identity management and common system access. However, we did identify other reportable weaknesses that are described in the executive summary and body of this report. In our opinion, the operational and administrative controls over identity management and common system access in effect as of November 2, 2012, taken as a whole, were sufficient to meet the objectives stated in the “Purpose” section of this report.

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.

The following summary provides management with an overview of conditions requiring attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [ ] refer to page numbers in the report.

GOVERNANCE [7]

Campus policies and procedures for identity and access management (IAM) needed improvement. For example, the campus did not have a process to ensure that changes in access privileges were performed consistently and in a timely manner.
INTRODUCTION

BACKGROUND

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.
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 emphasized, 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.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

GOVERNANCE

Campus policies and procedures for identity and access management (IAM) needed improvement.

We found that the campus:

- Had not developed written IAM policies and procedures for overall governance and definition of roles and responsibilities in operating, using, and monitoring the IAM system.
- Did not have a process to ensure that changes in access privileges were performed consistently and in a timely manner.

Integrated California State University Administrative Manual (ICSUAM) §8015, Organizing Information Security, dated April 19, 2010, states that each campus must develop, implement, and document the organizational structure that supports the campus’ information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program.

ICSUAM §8030, Personnel Information Security, dated April 19, 2010, states that campuses must implement procedures to revoke access to information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy and by the data owner. Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

The chief information officer (CIO)/information security officer (ISO) stated that although the campus had not formally prepared various policies nor established overall governance for the IAM system, it was following the chancellor’s office guidance, as evidenced by its committee meetings and directives. Further, he stated that the campus was aware of the various process gaps in the de-provisioning of accounts and was planning enhancements after various system upgrades had been completed.

Failure to develop sufficient policies and procedures for IAM may lead to undetected system breakdowns and data misappropriations and misuse.

Recommendation 1

We recommend that the campus:

a. Develop and implement written IAM policies and procedures for overall governance and definition of roles and responsibilities in operating, using, and monitoring the IAM system.
b. Create a process to ensure that changes in access privileges are performed consistently and in a timely manner.

**Campus Response**

The campus concurs and is formulating the governance, policy documentation, and processes recommended. The campus expects to complete this work by May 6, 2013.
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eduardo M. Ochoa</td>
<td>Interim President</td>
</tr>
<tr>
<td>Terryn Ashley</td>
<td>Payroll Services Supervisor</td>
</tr>
<tr>
<td>Hayley Azevedo</td>
<td>Academic Personnel Coordinator</td>
</tr>
<tr>
<td>Rachelle Bass</td>
<td>Assistant Director of Student Services</td>
</tr>
<tr>
<td>Diana Cockerham</td>
<td>Administrative Support Coordinator</td>
</tr>
<tr>
<td>Art Evjen</td>
<td>Director of Business and Support Services</td>
</tr>
<tr>
<td>Peter Fernandez</td>
<td>Lead Analyst, Student Information Systems</td>
</tr>
<tr>
<td>John Fitzgibbon</td>
<td>Associate Vice President for Finance</td>
</tr>
<tr>
<td>Veronica Flores</td>
<td>Director of Student Information Systems</td>
</tr>
<tr>
<td>Mike Green</td>
<td>Analyst Programmer, Administration and Finance</td>
</tr>
<tr>
<td>Grace Cardenas Leal</td>
<td>Director, Academic and Career Advising</td>
</tr>
<tr>
<td>Chip Lenno</td>
<td>Chief Information Officer/Information Security Officer</td>
</tr>
<tr>
<td>Steve Mann</td>
<td>Associate Director of Network Services</td>
</tr>
<tr>
<td>Mary Mauro</td>
<td>Director, Information Technology Compliance and Planning</td>
</tr>
<tr>
<td>William Musselman</td>
<td>Director of Accounting</td>
</tr>
<tr>
<td>Venkata Paruchuru</td>
<td>Lead Administrative Analyst</td>
</tr>
<tr>
<td>Kevin Saunders</td>
<td>Vice President of Administration and Finance</td>
</tr>
<tr>
<td>Karen Sellick</td>
<td>Program Coordinator/Analyst, Extended Education</td>
</tr>
<tr>
<td>Eric Simoni</td>
<td>Associate Director of Information Systems</td>
</tr>
<tr>
<td>Henry Simpson</td>
<td>Director of Technology Support Services</td>
</tr>
<tr>
<td>Laura Tantillo</td>
<td>Diversity, Equity, and Employee Development Analyst</td>
</tr>
<tr>
<td>Chris Villanueva</td>
<td>Credential Analyst II, Calstate TEACH Program</td>
</tr>
</tbody>
</table>
January 22, 2013

University Auditor Larry Mandel  
California State University  
Office of the University Auditor  
401 Golden Shore, 4th Floor  
Long Beach, CA  90802


Dear Larry:

Attached is our response to the Incomplete Draft Audit Report 12-47, dated December 19, 2012. A Word file of the response is attached in the email transmittal of this cover letter.

Please contact AVP John Fitzgibbon if you have any questions or comments.

Sincerely,

Kevin R. Saunders  
Vice President

Attachment

cc: Interim President Ochoa  
    Senior Director Schlack  
    Chief Information Officer Lenno  
    AVP Fitzgibbon
GOVERNANCE

Recommendation 1

We recommend that the campus:

a. Develop and implement written IAM policies and procedures for overall governance and definition of roles and responsibilities in operating, using, and monitoring the IAM system.

b. Create a process to ensure that changes in access privileges are performed consistently and in a timely manner.

Campus Response

The campus concurs and is formulating the governance, policy documentation, and processes recommended. The campus expects to complete this work by May 6, 2013.
February 15, 2013

MEMORANDUM

TO: Mr. Larry Mandel
    University Auditor

FROM: Timothy P. White
    Chancellor

SUBJECT: Draft Final Report 12-47 on
    Identity Management and Common System Access,
    California State University, Monterey Bay

In response to your memorandum of February 15, 2013, I accept the response as submitted with the draft final report on Identity Management and Common System Access, California State University, Monterey Bay.

TPW/amd