IDENTITY MANAGEMENT AND COMMON SYSTEM ACCESS

SAN DIEGO STATE UNIVERSITY

Audit Report 12-45
December 11, 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

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  
  Identity Validation ................................................................................................................................... 7  
  Security Plan Compliance .......................................................................................................................... 8
APPENDICES

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

ABBREVIATIONS

CIO                Chief Information Officer
CSU                California State University
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 San Diego State University campus from June 25, 2012, through July 20, 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 July 20, 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]

The campus had not issued guidance for verifying user identity for computer accounts, nor had it implemented validation procedures to ensure that user identity security policies were enforced. In addition, reporting and monitoring of departmental compliance with the campus information security plan required improvement. Specifically, the campus did not require that departmental exceptions be reviewed or approved by the campus information security office and did not require decentralized departments to provide evidence of compliance with the campus password policy.
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.
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 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

IDENTITY VALIDATION

The campus had not issued guidance for verifying user identity for computer accounts, nor had it implemented validation procedures to ensure that user identity security policies were enforced.

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.

The senior director and chief information officer of enterprise technology services (CIO) stated that the campus had not implemented an identity management system, and therefore had not formally addressed identity validation for existing decentralized systems. He also stated that every department certifies compliance with security policy on a quarterly basis, but that planned compliance audits had not yet been performed on all aspects of the campus security plan.

Inadequate policies and procedures over identity and access management processes may lead to organizational regulatory noncompliance and an inability to determine whether university data is being misused.

**Recommendation 1**

We recommend that the campus issue guidance for verifying user identity for computer accounts and implement validation procedures to ensure that user identity security policies are enforced.

**Campus Response**

We concur. The campus will issue a new standard in the Information Security Plan for verifying user identity and will establish validation procedures to ensure that the new standard is implemented.

This will be completed by February 28, 2013.
SECURITY PLAN COMPLIANCE

Reporting and monitoring of departmental compliance with the campus information security plan required improvement.

We found that the information security plan:

- Did not require that departmental exceptions be reviewed or approved by the campus information security office.
- Did not require decentralized departments to provide evidence of compliance with the campus password policy.

ICSUAM §8010.00, Establishing an Information Security Program, dated April 19, 2010, states in part that the campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The program should, among other things: a) provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic), b) develop risk management strategies to identify and mitigate threats and vulnerabilities.

ICSUAM §8015, Organizing Information Security, dated April 19, 2010, states in part that the information security officer (ISO) (or designee of the president) is responsible for the campuswide information security program and may organize the responsibilities as appropriate.

ICSUAM §8020, Information Security Risk Management, dated April 19, 2010, states that campuses must develop risk management processes that identify, assess, and monitor risks to information assets containing level 1 and level 2 data as defined in the California State University Data Classification Standard. Identified risks to these information assets must be actively managed by data owners and/or appropriate administrators in order to prioritize resources and remediation efforts.

ICSUAM §8045.100, Information Technology Security, dated April 19, 2010, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

The CIO stated that the campus was aware of the security limitations of certain systems, but that formal approval for such exceptions to the security plan had not been required in the certification process. The ISO stated that all departments certify compliance with campus policies on a quarterly basis, but that evidence of compliance on all aspects of the information security plan had not been required.

Inadequate oversight by the information security function could lead to exposure of sensitive data, gaps in internal control, or non-compliance with the information security program, and allowing departments to employ varied processes or circumvent established ones could jeopardize compliance.
with management objectives. Inadequate password security parameters and authentication practices increase the risk that accounts may be compromised and unauthorized access to systems and confidential data may be allowed.

**Recommendation 2**

We recommend that the campus require that:

a. All departmental exceptions to the information security plan be reviewed and approved by the campus information security office.

b. Decentralized departments provide evidence of compliance with the campus password requirements.

**Campus Response**

The campus will change the Information Security Plan to require that exceptions to password length, password changes, and administrator access for users be reviewed by the IT security office. The campus will implement validation procedures to ensure the new exception processes are followed.

Changes will be completed by February 28, 2013.
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elliot Hirshman</td>
<td>President</td>
</tr>
<tr>
<td>Scott Burns</td>
<td>Associate Vice President, Financial Operations (At time of review)</td>
</tr>
<tr>
<td>Mikhail Burstein</td>
<td>Director, Student Information Management System</td>
</tr>
<tr>
<td>Valerie Carter</td>
<td>Director, Audit and Tax</td>
</tr>
<tr>
<td>Tony Chung</td>
<td>Director, Information Systems Management, Student Affairs</td>
</tr>
<tr>
<td>Bob Hilchey</td>
<td>Staff College of Sciences</td>
</tr>
<tr>
<td>Darrell Irwin</td>
<td>Staff College of Engineering</td>
</tr>
<tr>
<td>Lorretta Leavitt</td>
<td>Associate Vice President, Financial Operations</td>
</tr>
<tr>
<td>Gene LeDuc</td>
<td>Information Technology Security Officer</td>
</tr>
<tr>
<td>Diana Osborn</td>
<td>Operating Systems Analyst, Expert, College of Sciences</td>
</tr>
<tr>
<td>Rich Pickett</td>
<td>Senior Director and Chief Information Officer, Enterprise Technology Services</td>
</tr>
<tr>
<td>Michael Pietrzak</td>
<td>System Administrator</td>
</tr>
<tr>
<td>Kimberlee Reilly</td>
<td>Assistant Controller</td>
</tr>
<tr>
<td>John Ross</td>
<td>Academic Information Technology Coordinator/Information Technology Interim Director</td>
</tr>
<tr>
<td>Sally Roush</td>
<td>Vice President, Business and Financial Affairs</td>
</tr>
<tr>
<td>Jim Varnell</td>
<td>Staff, College of Sciences</td>
</tr>
<tr>
<td>Felecia Vlahos</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>Rayanne Williams</td>
<td>Registrar</td>
</tr>
</tbody>
</table>
January 8, 2013

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802

Dear Mr. Mandel:

Attached is San Diego State University’s response to Audit Report 12-45, Identity Management and Common System Access. Documentation of policy and control changes will follow under separate cover.

Should you have any questions or require additional information, please contact Valerie Carter, Audit and Tax Director, at 619-594-5901.

Sincerely,


Sally F. Roush
Vice President, Business and Financial Affairs

Attachment

c: Elliot Hirshman, President
   Loretta Leavitt, Associate Vice President, Financial Operations
   Rich Pickett, Senior Director and CIO, Enterprise Technology Services
   Valerie Carter, Director, Audit and Tax
IDENTITY MANAGEMENT AND COMMON SYSTEM ACCESS

SAN DIEGO STATE UNIVERSITY

Audit Report 12-45

GOVERNANCE

IDENTITY VALIDATION

Recommendation 1

We recommend that the campus issue guidance for verifying user identity for computer accounts and implement validation procedures to ensure that user identity security policies are enforced.

Campus Response

We concur. The campus will issue a new standard in the Information Security Plan for verifying user identity and will establish validation procedures to ensure that the new standard is implemented.

This will be completed by February 28, 2013.

SECURITY PLAN COMPLIANCE

Recommendation 2

We recommend that the campus require that:

a. All departmental exceptions to the information security plan be reviewed and approved by the campus information security office.

b. Decentralized departments provide evidence of compliance with the campus password requirements.

Campus Response

The campus will change the Information Security Plan to require that exceptions to password length, password changes, and administrator access for users be reviewed by the IT Security Office. The campus will implement validation procedures to ensure the new exception processes are followed.

Changes will be completed by February 28, 2013.
February 15, 2013

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Timothy P. White
       Chancellor

SUBJECT: Draft final report 12-45 on
         Identity Management and Common System Access,
         San Diego State University

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, San Diego State University.

TPW/amd