INTERNAL AUDIT
IAS
ADVISORY SERVICES

Internal Audit Report

IS-3 COMPLIANCE

Report No. SC-11-05

June 2011

UC SANTA CRUZ

This page intentionally left blank

SANTA CRUZ: INTERNAL AUDIT

INTERNAL AUDIT
IAS
ADVISORY SERVICES

June 10, 2011

MARY DOYLE
Vice Chancellor, Information Technology Services

Re: Internal Audit Report No. SC-10-05 - IS-3 Compliance

Dear Mary,

Internal Audit and Advisory Services (IAS) has completed a UC systemwide internal audit of IS-3 Compliance at UCSC. A copy of the report is attached. The audit was conducted to review campus compliance with Business and Finance Bulletin IS-3 Electronic Information Security (IS-3) by examining controls to ensure the security of ITS-managed information technology (IT) resources.

In general, systems we reviewed were in compliance with IS-3 and practices for compliance were adequate. Opportunities were identified for improving controls as supporting conditions become available in four areas: enforcing password standards; use of encryption in systems containing restricted data; consistency of audit logging and review; and the data center fire suppression - sprinkler system.

We would like to express our appreciation to the Director, Client Services and Security for assistance and cooperation throughout this review.

Sincerely,

Barry Long

Barry Long, Director
Internal Audit & Advisory Services

Attachment

Distribution:

Director Roeth
Principal Auditor Dougherty

UCSC Audit Committee:

Special Assistant Beaston
Vice Chancellor Delaney
Vice Chancellor Doyle
Assistant Vice Chancellor Lew
Vice Chancellor Margon
Vice Chancellor McGinty
Assistant Vice Chancellor Moreno
Vice Chancellor Murphy
Assistant Chancellor Sahni
UCOP SVP Vacca
Vice Chancellor Valentino
Vice Chancellor Vani

INTERNAL AUDIT
IAS
ADVISORY SERVICES

IS-3 COMPLIANCE

Report No. SC-11-05

June 2011

Approved:

James Dougherty

James Dougherty
Principal Auditor

Barry Long

Barry Long, Director
Internal Audit & Advisory Services

UC SANTA CRUZ

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Internal Audit & Advisory Services (IAS) has completed a review of campus compliance with Business and Finance Bulletin IS-3 *Electronic Information Security* (IS-3) by examining controls to ensure the security of ITS-managed information technology (IT) resources.

In general, we found that systems we reviewed were in compliance with IS-3 and that practices for compliance were adequate. We did not recommend modifications to IS-3.

The following items represent opportunities for improvement when supporting conditions become available:

A. ***There were systems with sensitive data that could not technically enforce campus standards for strong passwords. Consequently, system administration relied on user training and reminders (administrative controls) to strengthen passwords. Periodic identification of weak passwords was not done on these systems.***

B. ***There are systems with restricted data that do not have encrypted data in the live database. The security of this data depends on mitigating controls.***

C. ***Audit logging and review was inconsistently managed.***

D. ***The use of a wet pipe sprinkler system in the Data Center is not recommended for the protection of computing systems and represents a high risk condition.***

Our observations and related management corrective actions are described in greater detail in section III of this report.

II. INTRODUCTION

A. Purpose

The purpose of this audit was to assess compliance with Business and Finance Bulletin IS-3 *Electronic Information Security* (IS-3) on a sample basis, identify areas to improve compliance, and identify recommendations for modifications to the IS-3 policy.

B. Background

Internal Audit & Advisory Services (IAS) was requested by the Office of Ethics, Compliance and Audit Services at the Office of the President to participate in this systemwide audit.

IS-3 was first published in 1998 with the purpose of establishing guidelines for achieving appropriate protection of university electronic information resources and to identify roles and responsibilities at all levels in the University of California (UC) system. The provisions of IS-3 apply to all UC campuses and medical centers, the Office of the President (OP), UC managed national laboratories, and other UC locations regarding management of its information assets.

In 2007, 2008, and 2009, UC's chief information officers and the information security community undertook a self-assessment of compliance with IS-3 to gauge the strength of information security activities across the system. The self-assessment instrument condensed nearly 50 IS-3 requirements and points of guidance into 17 activity categories for assessment. Each location was asked to provide responses from two distinct perspectives: that of the central/campus-wide information technology organization and that of the location as a whole but excluding central/campus-wide IT (the decentralized view). Medical center responses focused primarily on the central perspective. Responses from the ten campuses, five medical centers, Agriculture and Natural Resources, and OP were distilled to come up with the overall assessment of IS-3, which was presented to the Regents each year.. The current review was conducted by IAS to provide an independent assessment of IS-3 compliance.

In 2010, UCSC Information Technology Services (ITS) requested IAS to provide an advisory service by validating the 2009 IS-3 self-assessments. We provided a validation by determining the reasonableness and reliability of responses to the IS-3 self-assessments completed by participating campus units. Our validation included a cursory review of all 56 self-assessments submitted; a review of a number of specific activity categories chosen for detailed analysis; and a review of the self-assessment process employed by ITS. Further, we chose a judgment sample of self-assessments to verify their responses. We concluded that the 56 self-assessments submitted were completed with due diligence and professional care; identified opportunities for improvements to the process; and when appropriate identified risks that required further action.

C. Scope

The scope of this review included the 17 activity categories used in the previous IS-3 self-assessments and the respective IS-3 sections. We started with the 56 self-assessments we already had, which included descriptions of improvements projected for 2010. We then obtained a list of recent systems that were not included in the last self-assessment and assessed them for possible inclusion in our risk universe. For a risk assessment, we identified 18 systems that had highly sensitive data and were essential to completing the campus mission. We conducted a risk assessment of the 17 activity categories of these 18 systems by assigning risk levels (high, medium, and low) using maturity levels recorded in the self-assessments: 0-1 equaled high risk; 2-3 equaled medium risk; and 4-5 equaled low risk. We then refined the risk levels based on our knowledge of the systems from previous audits and advisory services, and those activity categories that represented the greatest risk to security. We then conducted more detailed analysis of remaining high risk activity categories to determine how management controlled these risks. Detailed analysis included:

- Data Center: consolidation of access control lists of new firewalls and physical security
- Unix systems administered by Data Center Operations
- Windows systems administered by Data Center Operations
- Telecommunication Services: database access controls
- Campus Curriculum and Leave Planning System
- Financial Information System and Academic Information System: data-at-rest encryption

We limited the extent of testing because a focused review of logical security controls of high risk systems is planned for FY12. Further, as the audit plan for FY12 includes a review of mobile device security, we did not include this IT environment in our risk analysis for this review.

Concurrent with this review, IAS provided its annual review of campus documentation of HIPAA entities' implementation of practices for compliance with the HIPAA Security Rule. We therefore did not include an assessment of HIPAA security risks in addition to IS-3 security risks.

D. <u>Observations of Noteworthy Practices</u>

IS-3 Self-Assessment Process
ITS took advantage of the OP-requested IS-3 self-assessment process to further its own understanding of campus IT security activities and compliance with that policy. Consequently, ITS took care to identify systems to be assessed and instructed assessors on their duties. The result was a body of knowledge updated during the three year period of self-assessment that added to ITS's monitoring of IT security activity over a wide range of systems and identified opportunities for improvements. IAS was exposed to this body of knowledge in FY10 when ITS requested it to provide a validation of this process. This cooperation has provided IAS with a greater understanding of campus IT systems, processes, and security activities.

Firewall Access Control List Consolidation
Consolidation of the thousands of accumulated access control lists (ACL) assumed by the Data Center's new firewalls is a major project. We were satisfied with management's plan to obtain a firewall management application (within a comprehensive plan for consolidation) to identify and remove ACLs that are erroneous, no longer in use or providing unnecessary access.

Wincore

- When privileged access is required for system administration, sys-administrators use individually identifiable logons. These are Active Directory user IDs, which are also Cruz IDs. This assures individual accountability.
- Security logs are turned on and assures that a record of access is available for review; review of logs is incident driven.

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

In general, we found that systems we reviewed were in compliance with IS-3 and that practices for compliance were adequate. The items listed below represent opportunities for improvement when supporting conditions become available.

A. Access Controls – Password Strength

There were systems with sensitive data that could not technically enforce campus standards for strong passwords. Consequently, system administration relied on user training, campus password policy, and reminders (administrative controls) to strengthen passwords. Periodic identification of weak passwords was not done on these systems.

When feasible, password strength should be enforced systematically. When administrative controls are relied on for strong passwords, there are applications that can be used to test for weak passwords.

Comments:
In addition to administrative controls, system administrators told us of plans to technically implement strong passwords. For example:

- Unix systems: there is a project proposal for a campus LDAP for campus systems to authenticate with hardened Kerberos passwords. In the meantime, users with privileged access to Unix systems are required to set strong passwords.

- Campus Curriculum and Leave Planning System (CCLP): administrators intend to migrate this entire application from FileMaker Pro into a PHP format - a general purpose scripting language. This will enable the use of Shibboleth authentication, resolving the password strength issue.
- Telecomm databases (2): administrators are researching how to move to LDAP and Shibboleth passwords. In the meantime, administrative controls are being setup for one system. As an interim control for the other system, administrators are researching the possibility of allowing users to reset their passwords.

The only sensitive information in the CCLP and the Telecomm systems appears to be specific personal directory information that the campus decided to restrict access to.

Agreements:

1. The Campus Information Security Officer will approve all exceptions to password policy by newly deployed ITS systems with sensitive data, encouraging the development of logical controls for strong passwords by July 15, 2011.

2. The Campus Information Security Officer will partner with ITS resources to test for weak passwords on CCLP and Telecomm databases as budget considerations allow by June 1, 2012.

B. Encryption of Data at Rest

There are systems with restricted data that do not have encrypted data in the live database. The security of this data depends on mitigating controls.

The strongest security for data is encryption. If PII and/or ePHI data is encrypted the university is relieved of reporting requirements if these systems are compromised.

Comment:

Campus systems such as FIS and AIS do not have the ability to handle encrypted data. There are mitigating controls in place that reduce the risk of unencrypted data at rest, such as firewalls, physical security, server/application account management, etc.

Even if encryption for data at rest is developed for these applications, its effect on performance and a cost/benefit analysis would need to be assessed before a decision to deploy could be made.

Agreement:
The Campus Information Security Officer will partner with resources within ITS to provide guidance regarding encryption to data stewards of restricted data systems (as identified through IS-3 self-assessments) by June 1, 2012.

C. Audit Log Management

Audit logging and review was inconsistently managed.

Practices to ensure compliance must be monitored to assess their effectiveness in achieving the security goal of identifying attempted/actual unauthorized access and activity.

Comments:
During the last IS-3 self-assessment process, ITS management observed that audit logging and review was inconsistently practiced. There were applications without logging capability; systems with access logging did not have activity logging; logging capability was not necessarily turned on; log review was either event-driven, periodic, or automated. ITS took steps to improve audit logging and review by developing a draft campus log policy and procedures soon to be finalized. Once issued, the implementation of this policy and procedures must be monitored to assess their effectiveness in achieving the security goals of log management.

Agreements:

1. The Campus Information Security Officer will finalize the logging policy and procedures and submit them for review and approval as campus policy and procedures by December 15, 2011.

2. The Campus Information Security Officer will ensure that audit log management is included in review of newly deployed ITS systems with sensitive data and managed desktop deployment by October 15, 2011.

D. Data Center Fire Suppression System

The use of a wet pipe sprinkler system in the Data Center is not recommended for the protection of computing systems and represents a high risk condition.

The campus should consider replacing the current wet pipe sprinkler system with a pre-action sprinkler system.

Comments:
A sprinkler system in the Data Center adds risk that contents could be damaged in the event of a discharge. Since the Data Center is located in a multiuse facility, it is

required to have a sprinkler system installed. The recommended best practice for a sprinkler system in a Data Center is a pre-action/dry pipe system.

For several years, the Data Center manager has listed the costs for implementing the new system on his annual spending projections submitted to ITS senior managers for funding approval. ITS senior managers have chosen to assume the risk of maintaining the current system for the time being, while keeping it on their list of high risk items. Given the reliability of the current sprinkler system, low likelihood of causes of accidental discharge, and other mitigating factors, such as the additional gaseous system in place, this decision is understandable in the current budget climate.

However, with so many essential systems in the Data Center, the high loss of accidental discharge weighs against the low likelihood of such an event. As long as the Data Center is located inside a multiuse facility, it is imperative that ITS considers installing a pre-action sprinkler system as soon as funding can be made available.

ITS has taken steps and continues to mitigate the risks of physical damage to the Communications Data Center through use of alternative facilities such as the San Diego Supercomputer Center; improved disaster recovery such as a warm site for the critical enterprise system AIS, and increased use of shared service providers, e.g. Google SlugMail, rSmart eCommons, Kuali UCReady.

Agreement:
The Campus Information Security Officer will ensure the Data Center sprinkler system and other related risks are captured in the campus enterprise risk management process, and report on progress for this or other mitigation actions by October 15, 2011.

***