UNIVERSITY OF CALIFORNIA, IRVINE
ADMINISTRATIVE AND BUSINESS SERVICES
INTERNAL AUDIT SERVICES

UNIVERSITY OF CALIFORNIA, BUSINESS AND FINANCE BULLETIN IS-3
ELECTRONIC INFORMATION SECURITY

Report No. 2011-114

June 30, 2011

Prepared by:

Evans Owalla
IT Principal Auditor

Reviewed by:

Bent Nielsen

Bent Nielsen
Director
UC Irvine Internal Audit Services

IRVINE: INTERNAL AUDIT SERVICES

June 30, 2011

SHERYL VACCA
VICE PRESIDENT/CHIEF COMPLIANCE & AUDIT OFFICER

RE: University of California, Business and Finance Bulletin IS-3 Electronic Information Security
Report No. 2011-114

Internal Audit Services has completed the assessment of the campus compliance with the control objectives defined in the University of California, Business and Finance Bulletin 1S-3, Electronic Information Security, and the final report is attached.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting the assessment. If you have any questions or require additional assistance, please do not hesitate to contact me.

Bent Nielsen

Bent Nielsen
Director
UC Irvine Internal Audit Services

Attachment

C: Audit Committee
Dana Roode, Chief Information Officer and Assistant Vice Chancellor, Office of Information Technology

COMPLIANCE WITH UC ELECTRONIC INFORMATION SECURITY POLICY IS-3
Report No. 2011-114

I. EXECUTIVE SUMMARY

University of California, Irvine (UCI) Internal Audit Services (IAS) conducted an assessment of selected computing environments for compliance with the 17 control objectives defined in the University of California (UC), Business and Finance Bulletin IS-3 Electronic Information Security (IS-3) at the request of the UC Office of the President (UCOP). The assessment was performed predominately by Protiviti under the direction of IAS. The number of unique computing environments, coupled with a high degree of decentralization lead to a sample approach. Specifically, a representative sample of the computing environments was selected to represent the entire campus. However, we were not in a position to determine whether the results of the audit could be extrapolated to represent the entire campus. Each computing environment selected was assessed using a two-step approach consisting of an initial risk assessment, to assess its inherent risk level and control environment, followed by multi-level testing of IS-3 control objectives for controls determined to present a high and medium inherent risk in each environment. Inherent risk is the risk that exists in each area without consideration of the level of management control in place (risk before controls).

The results of the audit are representative of a fragmented environment, with relatively few standard, "horizontal", operational processes and limited effectiveness of the central technology governance model. Specifically, despite the ongoing consolidation and standardization effort in the UCI computing environments, there is a significant difference in the level of compliance with IS-3 requirements among the computing environments assessed as part of the audit. Nonetheless, our observations lead us to believe that ongoing standardization and consolidation plans, once fully implemented, will lead to a significant improvement in the consistency of the computing environments as well as overall level of compliance with IS-3 requirements.

While it was determined that none of the computing environments audited are fully compliant with IS-3 mandated control objectives, the controls implemented in several of them adequately mitigate the majority of the applicable threats in that environment.

Of the 17 control objectives defined in IS-3, information assets classification, designation of information security roles, incident response planning and notification, third-party agreements, and network security controls were generally consistent among all the computing environments sampled. Systemic issues were identified in the areas of third party risk assessment and management, information systems event management, risk assessment, physical security controls, security planning, and operational contingencies.

The differences between the control environments in the computing environments assessed were determined to be significant, the results are presented in Table 1 and Figure 1, below.

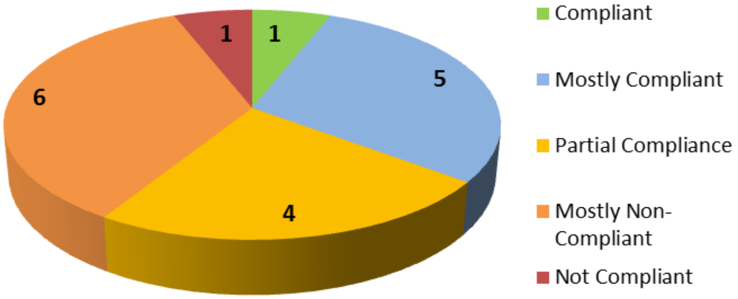
Table 1: Overall UCI Results

IS-3 Control Area	***Overall Status (UCI)***
Information Security Officer	***Compliant***
Security Awareness & Training	***Partial +***
Asset Inventory & Classification	***Partial +***
Risk Assessment	***Partial -***
Information Security Plan	***Not Compliant***
Workforce Administration	***Partial +***
Physical & Environmental Controls	***Partial -***
Incident Response Planning and Notification	***Partial***
Third-Party Agreements	***Partial -***
Identity & Access Management	***Partial***
Access Controls to Authentication & Authorize User	***Partial +***
Systems & Application Security	***Partial -***
Application Systems Management	***Partial -***
Collection, Analysis, and Mgmt. of Log Data	***Partial***
Data Protection & Encryption	***Partial +***
Risk Mitigation Measures	***Partial -***
Network Security Tools & Practices	***Partial***

Table 1 Legend:

Compliant	Most (>80%) of IS-3 controls have been implemented
Partial +	A majority (60%-80%) of IS-3 controls have been implemented
Partial	Some (40%-60%) of IS-3 controls have been implemented
Partial -	Few (20%-40%) of the IS-3 controls have been implemented
Not Compliant	Most (less than 20%) IS-3 controls have not been implemented

Figure 1: UCI Audit Findings



II. BACKGROUND

IAS conducted an assessment of selected computing environments for compliance with the 17 control objectives defined in IS-3 at the request of UCOP. IAS used a standard system-wide audit program that was developed by UCOP for use at all campuses.

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

In 2007, 2008, and 2009, the University'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 to 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). Responses from the ten campuses, five medical centers, Agriculture and Natural Resources, and UCOP were distilled to develop the overall assessment of IS-3. After three years of self-assessments, this audit was conducted by IAS to provide an independent assessment of IS-3 compliance.

Although UCI has a central computing environment, the Office of Information Technology (OIT), a significant number of distributed, autonomous or semi-autonomous, computing environments continue to operate. As such, a representative sample of the UCI centrally supported, autonomous, or mixed (autonomous consuming central services and infrastructure) computing environments were selected for the audit.

III. PURPOSE, OBJECTIVES, AND SCOPE

The purpose of the audit was to determine whether the internal controls currently implemented satisfy applicable control objectives defined in IS-3. The audit consisted of an initial risk assessment, to determine inherent risk for each control objective in each computing environment, followed by testing activities focused on areas determined to be of high and medium inherent risk. The scope of the audit consisted of the following computing environments:

- University Extension
- Registrar Office in Enrollment Services
- Counseling and Health Services in Student Affairs
- Office of Research Administration
- Legacy Systems & Client Support (PAL)
- University Advancement
- OIT

Each environment selected was initially assessed using a qualitative risk assessment approach aimed at identifying the inherent risks for the environment and the relevance of each of the 17 control objectives contained in IS-3 for mitigating the inherent risk identified. A rating of high, moderate, and low was used to categorize the level of mitigation offered by each control objective against the relevant inherent risks in the environment.

Subsequently, control objectives determined to provide high and moderate mitigation against inherent risks were audited through a multi-level testing approach. The first level of testing involved a review of relevant formal processes and management controls; a majority of the control objectives categorized moderate were audited using the first level of testing. In addition, controls categorized as high were audited through a second level of testing that involved validation of the level of adherence and the level of effectiveness of the controls. A third level of testing was to be used in the event inconclusive results were obtained using the first two levels; however, the use of the third level of testing was not required during the audit. The assessments were predominately performed by Protiviti during the months of April and May 2011.

IV. CONCLUSION

The results of the audit are indicative of an overall distributed computing environment with varied levels of IS-3 compliance. While areas of non-compliance and control deficiencies were identified in each computing environment, the differences between the computing environments in scope were significant. A number of systemic areas of non-compliance were identified; in most cases, non-compliance and control deficiencies were a direct result of ad-hoc operational processes and absence of an enforceable central governance model.

Observation details are presented below.

V. OBSERVATIONS

A summary of observations is presented below, along with the inherent and residual risk level. Inherent risk is the risk that exists in each area without consideration of the level of management control in place (risk before controls). Residual risk is the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk (risk after controls).

Table 2, below, presents the inherent risk level associated with each IS-3 control objective for each computing environment in scope for the audit. The results are based on the initial risk assessment performed for each environment.

Table 2: UCI Computing Environments Inherent Risk

Assessment Categories (IS-3 Control Objectives)	University Extension	Central Computing Environment (OIT)				
		Registrar	Counseling & Health Services	Office of Research Admin	Legacy Systems	Advancement
Management Measures: People						
1.Designation of Information Security Officer	***Low***	***Low***	***Low***	***Low***	***Low***	***Low***
2.Security Education & Awareness Training	***Moderate***	***High***	***High***	***Low***	***Low***	***Moderate***
Management Measures: Processes						
3.Asset Inventory & Classification	***High***	***High***	***Moderate***	***Moderate***	***Moderate***	***Moderate***
4.Risk Assessment	***Moderate***	***High***	***Moderate***	***Moderate***	***Moderate***	***Moderate***
5.Information Security Plan	***Low***	***Moderate***				
6.[Workforce] Administrative	***High***	***High***	***High***	***Moderate***	***Moderate***	***Moderate***
7.Physical/Environmental Controls	***Moderate***	***Moderate***	***Moderate***	***Moderate***	***Unknown/ OP***	***Moderate***
8.Incident Response Planning & Notification Procedures	***High***					
9.Third Party Agreements	***High***					
Technical Measures						
10.Identity and Access Management	***High***	***High***	***High***	***Moderate***	***Moderate***	***Moderate***
11.Access Controls to Authenticate & Authorize Users	***High***	***High***	***Moderate***	***Moderate***	***Moderate***	***High***
12.Systems and Applications Security	***High***	***High***	***High***	***Low***	***Low***	***Moderate***
13.Application Systems Management	***High***	***High***	***High***	***Low***	***High***	***Moderate***
14.Collection, Management and Analysis of Log Data	***High***	***High***	***High***	***Moderate***	***High***	***Moderate***
15.Data Protection and Encryption	***High***	***High***	***High***	***Low***	***Low***	***High***
16.Risk Mitigation Measures	***Moderate***	***Moderate***	***Moderate***	***Moderate***	***Moderate***	***Moderate***
17.Network Security Tools & Practices	***High***	***High***	***High***	***Moderate***	***Moderate***	***Moderate***

Table 3, below, presents the residual risk for each IS-3 control objective for each computing environment, based on the results of the inherent risk previously determined and testing activities conducted as part of the audit.

Table 3: UCI Computing Environments Residual Risk

Assessment Categories (IS-3 Control Objectives)	University Extension	Central Computing Environment (OIT)				
		Registrar	Counseling & Health Services	Office of Research Admin	Legacy Systems	Advancement
Management Measures: People						
1.Designation of Information Security Officer	***Low***	***Low***	***Low***	***Low***	***Low***	***Low***
2.Security Education & Awareness Training	***Low***	***Low***	***Low***	***Low***	***Low***	***Low***
Management Measures: Processes						
3.Asset Inventory & Classification	***Moderate***	***Moderate***	***Moderate***	***Moderate***	***Low***	***Moderate***
4.Risk Assessment	***Low***	***High***	***Moderate***	***Moderate***	***Low***	***Moderate***
5.Information Security Plan	***Low***	***Low***				
6.[Workforce] Administrative	***Moderate***	***Moderate***	***Low***	***Moderate***	***Low***	***Moderate***
7.Physical/Environmental Controls	***Moderate***	***Moderate***	***Moderate***	***Moderate***	***Unknown/ OP***	***Moderate***
8.Incident Response Planning & Notification Procedures	***Moderate***					
9.Third Party Agreements	***High***					
Technical Measures						
10.Identity and Access Management	***Moderate***	***High***	***Low***	***Moderate***	***Low***	***Moderate***
11.Access Controls to Authenticate & Authorize Users	***Moderate***	***High***	***Low***	***Moderate***	***Low***	***Moderate***
12.Systems and Applications Security	***Moderate***	***Moderate***	***Moderate***	***Low***	***Low***	***Moderate***
13.Application Systems Management	***Moderate***	***High***	***Moderate***	***Low***	***Moderate***	***Moderate***
14.Collection, Management and Analysis of Log Data	***Low***	***High***	***Low***	***Moderate***	***Moderate***	***Moderate***
15.Data Protection and Encryption	***Moderate***	***Moderate***	***Low***	***Low***	***Low***	***Moderate***
16.Risk Mitigation Measures	***Low***	***Moderate***	***Moderate***	***Moderate***	***Moderate***	***Moderate***
17.Network Security Tools & Practices	***Low***	***Moderate***	***Moderate***	***Moderate***	***Moderate***	***Moderate***

Key Issues Identified

The following control issues were identified in more than one of the computing environments assessed. IAS will also be following up on these control issues and preparing reports for the individual computing environments.

1. Asset Inventory and Classification

We noted inconsistent and informal information asset inventory processes and limited use of the inventory information during ongoing operational processes, including but not limited to risk, change, and contingency management. In most cases, information assets inventories consisted of spreadsheets updated on an ad-hoc or annual basis. Asset classification was not, generally, stored with the asset inventory; the campus Electronic Information Records (EIR) system was used to document systems processing or storing Personal Identifiable Information (PII) and other sensitive information.

2. Risk Assessment

Ad-hoc or informal risk assessment processes yielding, in most cases, limited or inconsistent actionable information were observed in many of the environments assessed.

3. Information Security Plan

OIT has a high level security plan and draft information strategic plan at the campus level; however, a lack of a formal security plan that includes recommendations for administrative, technical, and physical security measures to address identified risks relative to their sensitivity or criticality was noted in many of the environments.

4. Physical and Environmental Controls

Inconsistent physical security and environmental controls, and, in some cases, limited operational effectiveness were observed.

5. Incident Response Plan

Although steps for information security incident management are documented, no formal plan is currently approved; however, we noted that UCI is currently reviewing and plans to adopt the UC Incident Response Plan.

6. Third Party Agreements

We noted a fairly consistent inclusion of information security contractual terms in major third-party contracts; however, we also noted a lack of a formal management process and third party risk assessments are performed on only an ad-hoc basis for a very limited number of third-parties, both within each computing environment and campus-wide.

7. Identity and Access Management

Inconsistent controls for user authentication across multiple platforms, especially in applications and non-standard infrastructure components were noted in several computing environments. While centrally managed authentication solutions, such as Active Directory and Kerberos, have generally been implemented, consistent password control settings, applications and systems not using these solutions have varying degrees of compliance with password and authentication control requirements.

8. IT Contingency Plans

Contingency plans have not been implemented in most of the computing environments assessed. Although some computing environments participate, or participated, in UC Ready, no actionable contingency plans have been created or implemented.

9. Collection, Management and Analysis of Log Data

Inconsistent and often operationally ineffective management of systems and network event data (logs) were noted in several computing environments; in addition to uneven event generation settings across multiple platforms, event information is often not monitored, reviewed, and stored according to IS-3 requirements.

10. Network Access Controls

While certain computing environments have segmented their systems from the campus-wide network to provide addition access control and risk mitigation, network access controls are not fully effective in all environments audited. Additionally, the wireless network does not use encryption for both guest and authenticated user access, leading to potential exposure of authentication and other sensitive information.