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

# OFFICE OF ADMISSIONS & RELATIONS WITH SCHOOLS INFORMATION TECHNOLOGY

**Report No. 2012-106**

**January 31, 2012**

Prepared by:
Evans Owalla
IT Principal Auditor

Reviewed by:
Bent Nielsen
Director

IRVINE: INTERNAL AUDIT SERVICES

January 31, 2012

**ERIC PUCHALSKI**
**DIRECTOR, ENROLLMENT SERVICES**
**OFFICE OF INFORMATION TECHNOLOGY (OIT)**

**RE: Office of Admissions & Relations with Schools Information Technology**
**Report No. 2012-106**

Internal Audit Services has completed the review of core Office of Admissions & Relations with Schools Information Technology (IT) systems and the final report is attached.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. 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: Brent Yunek, Assistant Vice Chancellor, Enrollment Services
Scott Brinkerhoff, Programming Manager, University Registrar, OIT
Dana Roode, Chief Information Officer and Assistant Vice Chancellor, OIT
Audit Committee

**OFFICE OF ADMISSIONS & RELATIONS WITH SCHOOLS**
**INFORMATION TECHNOLOGY**
**No. 2012-106**

**CONFIDENTIAL**

## I. EXECUTIVE SUMMARY

In accordance with the fiscal year 2011-12 audit plan, Internal Audit Services (IAS) reviewed the adequacy of internal controls, policies, and procedures over core Office of Admissions & Relations with Schools (Admissions) Information Technology (IT) systems in protecting the confidentiality, integrity, and availability of sensitive applicants' information. Based on the audit work performed, opportunities for improving and strengthening internal controls were identified. Specifically, the following issues were noted:

**Patch and Software Updates –** Admissions has not implemented a formal process to ensure consistency and predictability in patch, malware, and other software updates. Details are discussed in section V.1.

**Passwords –** Admissions requires use of strong passwords, however, control improvements are needed to ensure passwords remain confidential, periodically changed and appropriate lockout enabled. Details are discussed in section V.2.

**User Account Management –** Admissions has a process to establish new user accounts and access controls to systems. However, improvements are needed in periodic review of user access based on least privilege. Details are discussed in section V.3.

**Change Management and Separation of Duties –** Admissions has not implemented adequate change management and separation of duties controls to their IT environment. Details are discussed in section V.4.

**Auditing and Monitoring –** Admissions has implemented detailed logging that can provide effective monitoring, but improvements are needed to ensure the audit logs are managed in a manner that facilitates these benefits. Details are discussed in section V.5.

**Information Security Program –** Some key components of the information security program have either not been formalized or need improvement. These components include asset inventory and classification, risk assessment, security plan, and security awareness training. Details are discussed in section V.6.

**Contingency Planning –** Admissions has not developed contingency plans, including business continuity and disaster recovery plans for its systems. Details are discussed in section V.7.

## II. BACKGROUND

Admissions provides prospective students with the information needed to apply to University of California (UC), University of California Irvine (UCI), implementing fair evaluation to applications and coordinating a campus-wide effort of assisting students with the necessary information and resources to imagine themselves as a student at UCI and to accept their offer of admission.

In 2010-11, Admissions received nearly 60,000 applications from new freshman and new transfer applicants. Admissions collects and maintains a significant amount of personal information on each applicant. Admissions understands that protecting the confidentiality of this sensitive information is paramount; otherwise, applicants could be potentially exposed to loss of privacy and to financial loss and damages resulting from identity theft. While Admissions core systems are older COBOL-based systems, they have also developed and implemented web based application systems to better facilitate recruitment and yield efforts.

## III. PURPOSE, SCOPE AND OBJECTIVES

The purpose of this audit was to evaluate controls over core Admissions IT systems in protecting the confidentiality, integrity, and availability of sensitive applicants' information. Based on assessed risk at Admissions, the following objectives were established:

1. Determine whether key servers, workstations, laptops and netbooks were installed with up-to-date critical patches and anti-virus software;

2. Determine whether effective identification and authentication mechanisms including password confidentiality, complexity, expiration and lockout were implemented;

3. Analyze users' access to selected systems to determine whether access was appropriately based on the least privilege principle;

4. Determine whether sensitive data were securely transmitted using appropriate encryption protocol and stored separately from publicly accessible servers;

5. Determine whether incompatible functions have been separated among IT staff and change management policies and procedures established;

6. Evaluate whether policies and procedures for management and monitoring of log data for security events were implemented;

7. Determine whether an asset inventory exists and was current and accurate;

8. Determine whether risk assessments have been conducted on core systems and risks and threats have been documented;

9. Determine whether management, operational, and technical controls have been tested periodically (at least annually) with an actionable test plan and results documented, including vulnerability scans of network, hosts and web applications;

10. Determine whether systems security plans including management, operational, and technical controls have been documented and are up-to-date;

11. Determine whether a formal user security awareness training program has been implemented for IT staff and users;

12. Determine whether contingency plans have been established, tested or updated including backup and recovery procedures and capability to recover and reconstitute the system's original state after a disruption or failure.

## IV. CONCLUSION

Business risks and control concerns were identified with patch and critical software updates, passwords, user account management, change management and segregation of duties, and log monitoring. In addition, key components of the information security program had either not been formalized or required improvement. These components include, conducting of risk assessments, documentation of security plans, and user security awareness training.

Observations detail and suggestions were discussed with management, who formulated action plans to address the issues. These details are presented below.

## V. OBSERVATIONS AND MANAGEMENT ACTION PLANS

### 1. Patch and Software Updates

**Background**

Software should be scanned and updated frequently to guard against known vulnerabilities. In addition to periodically looking for software vulnerabilities and fixing them, security software should be kept current by establishing effective programs for patch management, virus protection, and other emerging threats.

Also, software releases should be adequately controlled to prevent the use of noncurrent software. Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack.

### Observation

Admissions has not implemented a formal process to ensure consistency and predictability in patch, malware, and other software updates. Consequently, Admissions had not patched some of its Unix servers and ensured that operating and application software were up-to-date. This was attributed to limited IT staffing and servers not being part of the established Office of Information Technology (OIT) centralized Unix patch management support.  Examples of elements of software update deficiencies observed include:

- Admissions managed laptops and netbooks are not part of the centralized OIT desktop support services and were therefore not periodically updated;

- Admissions managed laptops and netbooks have outdated antivirus software that is not supported;

- Unix servers are not protected by anti-malware software. While Unix operating systems are generally regarded as very well-protected, they are not immune, from malware. Anti-malware software could provide an additional layer of protection against risk of viruses, trojans, worms, and attacker tools (e.g. rootkits).

Software vulnerabilities that are not patched or outdated software increases risk that data and information systems (IS) could be compromised.

### Management Action Plan

Admissions will address these observations in the following ways:

- We will work with OIT to implement a process to ensure consistency and predictability in patch, malware, and other software updates for servers;

- We will implement a process to ensure consistency and predictability in patch, malware, and other software updates for Admissions managed laptops and netbooks, including installing up-to-date antivirus;

- We will assess the risk of malware on our Unix servers and consider appropriate anti-malware tools.

- We expect to be able to complete the remaining items by the end of June 2012.

## 2. Passwords

### Background

Appropriate identification and access management strategies should be in place for establishing individual accountability so that activities on the system can be linked and traced to a specific individual and for controlling access to the system. This is typically achieved by assigning a unique account to each user (identification). The system should also establish the validity of a user claiming identity by requesting information, such as a password, that is known only by the user (authentication).

### Observation

Admissions requires the use of a strong password for authentication (minimum length of eight characters with at least one numeric and one special character). However, Admissions has not implemented best practices on certain elements that help ensure passwords remain confidential and are only known by the user. For example:

- Admissions Easier system stores user passwords in clear text within the system user access management file. While this file is limited to two IT staff, passwords should not be in clear text to maintain their confidentiality and minimize risk of disclosure in case of a breach;

- Admissions Unix servers are not configured to enforce password complexity. Therefore, the system administrator generates user passwords and provides them to users in person. While the system can allow users to change the initial passwords provided by the system administrator using the Unix “passwd” command, the system does not force password change and users typically don’t know how, and therefore don’t change the initial passwords;

- Servers are not configured to enforce periodic and regular password changes; and

- Unix servers are not configured to disable user accounts after a limited number of failed logon attempts.

As a result of these weaknesses, increased risk exists in user accountability in case of inappropriate access and compromise of sensitive data. In addition, compromise of Easier passwords by individuals with malicious intentions could be used to potentially gain elevated privileges to compromise other systems.

**Management Action Plan**

While the Easier passwords are stored in plain text, they are embedded within a proprietary file system that is only accessible to two senior IT staff and is not readily decoded without a very high level of expertise in an outdated technology. The likelihood of a random attacker gaining access to the file system and being able to extract the passwords is very remote. The nature of the VSAM file system and the COBOL application programs used to access it is such that it is not possible to encrypt the passwords within the current file structure.

Given the low risk of exposure of the passwords stored for Easier access, the difficulty involved in reconfiguring the file system to accept encrypted passwords, and the fact that all Enrollment Systems are currently being reviewed for possible replacement with newer technology, no plans are in place to encrypt Easier passwords.

To address the other issues, we will as of March 2012:

- Arrange training for end users in using the Unix passwd command to change login passwords;

- Enable the feature of the system that forces periodic change of login passwords; and

- Enable the lockout feature to disable accounts after three sequential failed login attempts.

## 3. <u>User Account Management</u>

**Background**

User account management addresses requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. A key component of granting or denying individual access rights is the concept of “least privilege.” Least privilege means that a user is granted only those access rights and permissions needed to perform official duties. Management should also perform regular reviews of all accounts and related privileges.

## Observation

Admissions has implemented a formal process to establish new user accounts and implemented access controls to systems. For example, access to application systems are approved by the requestor’s supervisor and identification and authentication are required. However, deficiencies with the user account management process were noted as follows:

- There are no procedures for regular reviews of user access rights and privileges. For example, some users with access to web applications had never logged on since their accounts were created, others had not used the applications for at least two years, and a few no longer worked for UCI. Web application user access was resolved during the audit;

- The Easier system does not provide a report that indicates user access rights and privileges that can be reviewed for continued appropriateness especially for users with access to sensitive transactions;

- The Web applications access control list does not match the unique user account to a user name, making it difficult to identify the account owner for a potential reviewer; and

- There were two users with administrative access at the server level who no longer needed the elevated permission.

As a result of these deficiencies, there is increased risk that a user could potentially gain inappropriate access to computer resources, and deliberately or inadvertently read, modify, or delete sensitive information.

## Management Action Plan

We will review login accounts for all systems and eliminate unnecessary accounts and also generic accounts wherever possible. We will ensure that all systems enforce minimum standards that meet UC, Business and Finance Bulletin IS-3: Electronic Information Security (IS-3) requirements. To the extent possible we will also do so for application programs. Although the primary responsibility for reviewing staff status and data access requirements resides in the Admissions business office and not the IT group, we will conduct regular reviews of privileged access to systems, at least quarterly and will assist Admissions operations staff in conducting their review of other access levels. In addition, we will also add user name information to the access web applications access control list to facilitate easy and accurate review of access and privileges. We expect to start this by March 2012 and should be complete by the end of June 2012.

## 4. Change Management and Separation of Duties

### Background

Establishing separation of duties over the modification of IS components and related documentation helps to prevent unauthorized changes and ensure that only authorized systems and related program modifications are implemented. IS-3 states that changes should be performed according to authorized management procedures that ensure recording of all changes. This is accomplished by instituting policies, procedures, and techniques that help ensure all hardware, software, and firmware programs and program modifications are properly authorized, tracked, tested, and approved.

### Observation

Admissions has not implemented adequate change management and separation of duties controls to their IT environment. Although Admissions has implemented Concurrent Versions System (CVS) software in the UNIX environment, the software was not utilized for all the business applications development life cycle. Admissions also uses JIRA[1] to track issues including change request, however changes cannot always be tracked to CVS and vice-versa. Examples of other deficiencies related to change management and separation of duties include:

- Policies and procedures have not been documented and established to assure that all changes are approved, appropriate and tested to ensure that they do not compromise security controls; and that unauthorized changes are detected and reported promptly;

- The technical staff with programming responsibilities can, and do, independently write, test, and approve system software program changes to production without evidence of supervisory authorization;

- Application security policies and procedure test plan have not been developed; and

- There is no process to properly document, test, and approve emergency changes.

Without adequate change management control to systems and programs, increased risk exists that changes may not work as intended, or may result in unintentional disruption of business, loss of data or program integrity or

[1] A proprietary tool commonly used for bug tracking, issue tracking, and project management.

exploitation of weaknesses introduced to gain access to sensitive systems and data.

### Management Action Plan

We currently have a project under way to set up a development environment that will allow us to implement proper change control procedures. The infrastructure and version control utilities are in place and are already being used for most development done on the core business applications. In conjunction with OIT we are developing a formal Systems Development Life Cycle (SDLC) to manage the development of new systems and maintain existing ones. We expect the details of the SDLC to be worked out and implemented no later than the end of April, 2012.

Along with this, we have started an effort to collect and formalize Standard Operating Procedure (SOP) used throughout Admissions and Enrollment Services. When complete, a library of production and emergency processes and procedures will be available online. The SOP library was completed before the end of 2011 but we do not expect to have all processes and procedures completely documented until the end of 2012.

## 5. Auditing and Monitoring

### Background

Effective auditing and monitoring requires a system that can establish individual accountability, monitor compliance with security policies, be used to investigate security violations, and the capability to determine what, when, and by whom specific actions have been taken on a system. Audit logs should be managed in a manner that facilitates these benefits while protecting the confidentiality and integrity of the information contained in these logs.

### Observation

Discussions with the Admissions technical staff and review of supporting documentation indicate that logs are enabled on Admissions servers to capture events such as access attempts, file transfers, messages, and other events. Also, the Easier system is configured to collect and maintain detailed audit logs. However, deficiencies on audit logging and the monitoring process were noted as follows:

- A formally documented process is not in place for the logging, aggregation, analysis and retention of audit logs;

- Except for email notification sent to IT staff when a social security number is modified in Easier system, there are no monitoring and alert functions or mechanisms set up to notify of other reportable security exceptions and violations as they occur, for example multiple failed log in attempts;

- There is no process for regular review of logs, reviews of the logs are done on an as need basis; and

- Logs are only stored in the systems generating the data and IT staff have write access to the logs. Logs should also be stored on a dedicated repository that protects the confidentiality and integrity of the information.

Robust logging and monitoring functions enable the early detection and/or prevention and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

**Management Action Plan**

We will review, document, and adjust our logging practices to conform with the recommendations where feasible and applicable to our situation. We will work with OIT security to employ the automated monitoring and alert functions of Splunk for the most sensitive logs. This should be complete by the end of June 2012.

## 6. Information Security Program

Some key components of the information security program have either not been formalized or need improvement. These components include asset inventory and classification, risk assessment, security plan and security awareness training.

### A. Asset Inventory and Classification

**Background**

An up-to-date inventory and classification of computing assets (hardware and software) helps to identify and determine the nature of campus electronic information resources. In addition, an accurate and up-to-date inventory is critical for the management of IS and implementation of an effective security program. Furthermore, the inventory is necessary for effective monitoring, testing, and evaluation of IS controls.

### Observation

Documentation obtained from OIT Desktop Support Services (DSS) indicates that an inventory of Admissions assets exists (hardware and software). However, the inventory listing was not complete based on observation and Nmap scan (Network Mapper). Examples are as follows:

- Management of Admissions assets is decentralized between the OIT DSS and Admissions IT staff. Therefore, while OIT DSS provided a LANDesk report of the desktops they manage, Admissions did not have a readily available listing of laptops and netbooks that they administer. Admissions also did not have a listing of all of their applications and interfaces;

- Admissions has not documented a current baseline inventory of hardware, software, and firmware of their servers; and

- While Admissions has identified their sensitive data and documented it in the Electronic Information Resources Inventory System (EIRIS), information assets have not been classified in terms of criticality.

Without an accurate and up-to-date asset inventory and information asset classification, Admissions cannot effectively manage IS controls across the department. For example, that all systems are effectively configured and updated as intended.

### Management Action Plan

We will bring our hardware asset inventory up to date and document the reasons why the LANDesk scan performed by OIT Security as part of this audit does not correspond exactly to the inventory. We will also review our software inventory and update as necessary. We believe that our information assets are adequately documented in the campus Electronic Information Resource Inventory system but will review them with respect to criticality of the data assets. We will review this on a regular basis, at least annually. We expect to be done with the update of EIRIS by the first quarter of 2012.

## B. Risk Assessment

### Background

IS-3 requires that units and departments understand and document risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption modification, or destruction of information and IS. Risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization’s mission, including the effect on sensitive and critical systems and data. Identifying and assessing information security risks are essential to determining what controls are required.

### Observation

Based on discussions with Admissions IT, none of the four Admissions systems reviewed had a formal risk assessment performed, either on a regular basis or as part of an ongoing operational process. Without periodic risk assessments, potential risks to systems may not be fully known and associated controls may not be in place.

### Management Action Plan

We will conduct a risk assessment for Admissions’ IT assets. We believe that the participation of someone trained in risk assessment methodology will be required to assist in the assessment and to ensure the quality of the results. This will be a major project that will take several months to complete. Expected completion would be in the third quarter of 2012.

## C. Security Plans

### Background

An objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system’s security requirements and describes the controls (i.e. management, operational, and technical controls) that are in place or planned to meet those requirements. According to IS-3, the security plan should account for the management, use, and protection of information that has some level of confidentiality, and identify the procedures and controls that will be implemented to enhance security for information assets.

### Observation

Admissions has not documented security plans describing the management, operational, and technical controls in place for the Easier system and three other web applications that we reviewed.  However, Admissions has documented some high level technical controls of their systems in the EIRIS. Without risk based security plans for key systems, Admissions cannot ensure that appropriate controls are in place to protect the sensitive information in their systems.

### Management Action Plan

Admissions will prepare documentation for security controls, operational procedures, and technical controls for all core business applications. This documentation will be prepared as part of an Enrollment Services-wide initiative to document existing systems and processes. Initial work will be completed early in 2012 and should be complete by the end of 2012.

## D. Security Awareness Training

### Background

Security education and awareness training is essential to ensure that IT staff and users are provided with sufficient training to understand system security risks and their own roles in implementing related UCI, and departmental policies to mitigate those risks. IS-3 states that department heads and supervisors shall ensure that appropriate security awareness training is routinely conducted for all members of the University community. In addition, the training program should include regulatory requirements and security reminders regarding current threats to technical environments in which individuals are working.

### Observation

Admissions has not established a formal process to provide regular user security awareness training to IT staff and general users. However, Admissions has a process in place for providing training for newly-hired employees and returning contract workers. For example, user security training provided includes the California Information Practices Act (IPA). Admissions also maintains user training and reader expectation agreement records to comply with their policies. Lack of adequate security training for users could create a weak link that could limit the ability of Admissions to effectively implement security measures.

### Management Action Plan

We will require current and future IT staff assigned to our group to complete the campus security training available through the UC Learning Center in addition to the FERPA training administered by UCI Registrar. We will take advantage of any future training opportunities that may become available. Expected completion of this task would be March 2012.

## 7. Contingency Planning

### Background

Business continuity and disaster recovery plans involve the identification, selection, implementation, testing, and updating of processes and specific actions necessary to prudently protect critical business processes from the effect of major system and network disruptions and ensure that when unexpected events occur, essential operations can continue without interruption or can be promptly resumed, and that sensitive data are protected.

### Observation

Although Admissions performs backups of their systems, it has not developed contingency plans, including business continuity and disaster recovery plans. Without developing and implementing a comprehensive contingency plan, Admissions may not be able to effectively recover their systems, data and normal operations after a disruption.

### Management Action Plan

We will work with the Admissions management team to finalize Admissions' contingency plan using UC Ready and additional resources as required. A business continuity plan will be in place before the end of 2012 and implementation of the plan before the end of 2013.