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

DONALD BREN SCHOOL OF INFORMATION AND COMPUTER SCIENCES
Report No. 2011-109

June 29, 2011

Prepared by:

Helen Templin
Senior Auditor

Reviewed by:

Michael Bathke

Michael Bathke
Campus Audit Manager

Prepared by:

Evans Owalla

Evans Owalla
Principal IT Auditor

Approved by:

Bent Nielsen

Bent Nielsen
Director
UC Irvine Internal Audit Services

IRVINE: INTERNAL AUDIT SERVICES

June 29, 2011

HAL STERN
DEAN
DONALD BREN SCHOOL OF INFORMATION AND COMPUTER SCIENCES

RE: Donald Bren School of Information and Computer Sciences Audit
Report No. 2011-109

Internal Audit Services has completed the review of the Donald Bren School of Information and Computer Sciences 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: Audit Committee
William Cohen, Director of Computing Support
Cassandra Jue Low, Director of Finance
Deanna Nunez, Director of Administrative Operations

DONALD BREN SCHOOL OF INFORMATION AND COMPUTER SCIENCES
Report No. 2011-109

I. EXECUTIVE SUMMARY

In accordance with the fiscal year 2010-11 audit plan, Internal Audit Services (IAS) reviewed the adequacy of internal controls, policy compliance, and information technology (IT) operations for the Donald Bren School of Information and Computer Sciences (ICS) within the University of California, Irvine (UCI) campus. Business risks and control concerns were identified. Specifically, we noted the following.

Employee Management – IAS was unable to locate documentation supporting the background check clearance for five sampled employees with critical elements in their job description. Performance evaluations were not completed on an annual basis for all staff employees. Details are discussed in section V.1.

Key Deposits – The internal controls over record keeping and reconciliation of key cash deposits needs improvement. This observation is discussed in section V.2.

Non-Payroll Expenditures – The internal controls over authorizing, documenting, and processing PALCard transactions and travel expenses needs improvement. The observation regarding PALCard transactions included lack of timely approvals of internal requisitions, lack of packing slips, and lack of appropriate reviewer documentation. The Travel expense reimbursement observation included untimely submittal to Accounting and lack of adequate supporting documentation. Additional details are discussed in sections V.3 and V.4.

Information Technology – IT operations can be improved upon in the following areas: physical and environmental security of the server room, change management, business continuity and disaster recovery planning, and user account management. The observations are discussed in sections V.5-V.8.

II. BACKGROUND

ICS enrolls approximately 1,200 students, including 400 graduate students. As an independent school focused solely on the computer and information sciences, ICS has a unique perspective on the information technology disciplines that allows a broad foundation from which to build educational programs and research initiatives that explore the many applications of the computing discipline; from circuits and systems to software engineering and human aspects of computing.

For fiscal year 2009-10, ICS employed approximately 40 full time equivalents (FTEs) and has an annual operating budget of approximately $28 million.

III. PURPOSE, SCOPE AND OBJECTIVES

The purpose of the audit was to review internal controls, policy compliance, and IT operations for the fiscal year 2009-10. Based on IAS's risk assessment of ICS, the following objectives were established:

1. Evaluate the following aspects for unit employee management: personnel files, background checks, written job descriptions, performance evaluations, overtime approvals, payroll ledger reconciliations, and sick and vacation balance tracking for appropriateness and completeness;

2. Review non-payroll expenditures for approval and appropriate documentation to determine compliance with University policy;

3. Evaluate equipment inventory procedures and sample inventoried items to ensure UCI tagging and location;

4. Review cash handling and cash receipt procedures to determine evidence of controls and that assets are properly safeguarded;

5. Evaluate whether there are adequate controls over budgeting and financial reporting;

6. Evaluate the controls related to extramural funding;

7. Review IT operations such as: change management, business continuity and disaster recovery planning, physical and environmental security, and user account management for appropriateness.

IV. CONCLUSION

In general, the selected ICS processes reviewed appear to be functioning as intended. However, business risks and control concerns were identified in employee management, cash handling, non-payroll expenditures, and IT controls.

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

V. OBSERVATIONS AND MANAGEMENT ACTION PLANS

1. Employee Management

Background

UCI Human Resources (HR) provides guidance to hiring managers on recruiting, screening, and interviewing prospective staff. The department will select candidates for interviews and decide on the final candidate for hiring. Once an employee is hired, the ICS Personnel Manager is responsible for ensuring that all completed documents are placed in the employee personnel file. ICS has one central personnel manager position and one personnel analyst position.

Observation

Background Checks

UCI Administrative Policy Sec. 300-10 states that background checks be completed on critical positions. The University believes that background checks provide a safer environment for people, property, and information at the University. Background check procedures are part of the pre-employment process. HR works with the new employee to get the background check completed, then notifies the hiring manager via email whether the employee has cleared the background check. This email should be filed in the employee's personnel file to acknowledge background check clearance. IAS was unable to locate the email confirmation of a cleared background check for five of the sampled critical positions in ICS. HR confirmed that three of these employees had cleared a background check. However, no documentation was found for the other two employees and it is uncertain if they had cleared a background check.

Performance Evaluations

UCI Personnel Policy 23 states that "The performance of each employee shall be appraised at least annually in writing by the employee's immediate supervisor, or more frequently in accordance with local procedures." Written performance evaluations provide a means of communicating between the supervisor and employee on how job performance and expectations are being met. Performance evaluations provide a framework for setting objectives, identifying goals, providing feedback, and evaluating results. Currently, six out of 42 eligible employees (14 percent) have not had a performance evaluation for the period ending June 30, 2010.

Management Action Plan

Background Checks

When UCI began doing background checks on staff employees about ten years ago, HR advised the departments not to keep materials related to these background checks as HR was the office of record for these documents. However, in order to maintain the integrity of the employee's personnel history, it is now necessary for this office to keep a copy of the email notification sent by HR once an employee has passed their background check. This process will be implemented immediately.

Performance Evaluations

The ICS Personnel Manager sends the first reminder to supervisors and managers regarding annual performance evaluations in July and follows up every other month to remind supervisors of their responsibility. This practice will continue until all annual performance evaluations are completed.

2. Key Deposits

Background

ICS maintains a locked cash box within a keyed safe to store cash deposits required for department keys (a deposit of $10 per key). When the keys are returned to ICS, the deposit is returned. ICS has not established a change fund to help track cash deposits and withdrawals for keys.

IAS was informed by ICS management of the potential issues surrounding the key deposits at the start of the review.

Observation

IAS noted that the record keeping to properly account for the key deposits is lacking and there has been no reconciliation performed between cash accepted and keys that have been distributed and/or returned. There is no assurance that all cash deposits are being accounted for and reconciled against the key inventory.

Insufficient control over cash deposits and lack of reconciliation weakens the control structure and reduces the ability to detect theft and/or inaccuracies.

Management Action Plan

To address these issues, ICS will integrate into the current key procedures steps which will allow the reconciliation between keys and deposits. These steps would include creating a change fund (has already been established), providing receipts for key deposits, expanding the key spreadsheet, and separate cash handling duties between the custodian and the alternate custodian. The improved procedures will be in place within six months.

3. PALCard Review

Background

University of California (UC) purchasing policies require purchases to be pre-approved through either a purchase requisition or some other form of documentation, such as an email. In addition, a reviewer must review the PALCard supporting documentation and account/fund for appropriateness in a timely manner and attach appropriate reviewer documentation.

Appropriate reviewer documentation includes the TOEP (screen print) with user identification and Financial System (FS) send date or a reviewer signature on the PALCard notification email. The cardholder must forward documentation to the reviewer within 4-6 days so that the transaction can be reviewed in a timely manner. The reviewer then has 14 days to review the transaction for appropriateness and make changes, if necessary. If the transaction is not reviewed within 14 days, the transaction will be approved automatically and the default account/fund and taxes, if any, will be sent to the general ledger. After the automatic submission or "auto send" takes place, the reviewer can still provide a signature on the PALCard notification email which can be used when transactions post to FS automatically and an electronic signature is not present. The preferred method is to review the PALCard purchase before the automatic submission so the FS sender field contains the reviewer's name.

Observation

IAS performed an analysis on a sample of 15 PALCard transactions during fiscal year 2009-10, and noted the following during the review:

- Six of the 15 had an approved internal requisition dated after the purchase was completed;
- One of the 15 did not have a receipt;
- Four of the 15 did not have a packing slip;
- Two of the 15 did not have appropriate reviewer documentation attached to the PALCard supporting documentation packet;
- Two of the 15 were conducted by the PALCard holder who was also the requestor; and
- One of the 15 did not appear to have a justifiable business reason for purchase.

IAS compiled a report with PALCard purchases dated from July 2009 through June 2010 that were automatically approved through the PALCard review system. IAS identified 294 transactions or $40,748.72 (13 percent) in PALCard purchases that were not reviewed in a timely manner.

Controls over PALCard transactions, such as timely authorization of charges before purchase, needs improvement to reduce the risk of error or misuse. Proper approval of transactions reduces the risk of inappropriate costs or unauthorized use of University funds.

Management Action Plan

The ICS Business Office will remind PALCard holders that approvals for all purchases must be obtained prior to purchase and that all required documentation must be submitted with each PALCard packet to the reviewers within 4-6 days. The reviewers will be reminded to review all PALCard packets for completeness and justification. For those PALCard holders who requested and purchased their own items, the ICS Business Office will require purchase requisitions be approved by another individual prior to purchase. The ICS Business Office will monitor PALCard packets to ensure the above is carried out.

4. Travel Expense Review

Background

Official University travel must be properly authorized, reported, and reimbursed in accordance with UC Business and Finance Bulletin, G-28. Authorization is to be obtained prior to undertaking University travel. Travel expenditures must be submitted to the campus accounting office within 21 days of the end of the trip. The traveler must sign the travel expense voucher certifying that the amounts claimed are a true statement of the expenses incurred and that the original of all required receipts has been submitted.

Observation

IAS judgmentally selected a sample of 13 travel vouchers during fiscal year 2009-10, and noted the following during the review:

- Five of the 13 were not submitted to the campus accounting office within 21 days of the end of the trip; and
- Two of the 13 did not include appropriate supporting documentation for expenses listed.

Insufficient control over timely submission of travel expenses and lack of proper support for expenditures weakens the control structure and reduces the ability to detect fraudulent activities and/or inaccuracies.

Management Action Plan

For those travel reimbursements that are submitted well beyond the 21 day policy, a memo is now required from the traveler to the Dean of ICS stating why the submission is late. The memo is also signed by the department chair or unit director/manager.

An email will be sent out by the ICS Director of Finance at least once each fiscal year to all staff, faculty, and graduate students as a reminder of the 21 day policy as well as other travel or reimbursement policies or procedures that may require attention.

All PayQuest processors will be reminded that they are required to have the necessary supporting documents for reimbursements. The ICS Business Office will review all PayQuest packets for completeness.

5. Physical and Environmental Security of the Server Room

Background

Protection for computer equipment and personnel requires well-designed and well-managed facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel. Such controls include guards, gates, and locks, and also environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies.

Observation

IAS performed a walkthrough of the ICS server room (machine room). IAS noted that the server room required improvement on physical, safety, and environmental controls in the following areas:

- The air conditioning (AC) unit was condensing and leaking water which collected under the elevated floor where electric cables (insulated) are installed. The pooling of water near electrical power cables may create a potential electrocution or fire hazard; and

- Entry to the server rooms was secured via a standard key lock. The room has an alarm system, but the alarm was normally disarmed during normal business hours and there is no video surveillance of the server room. Also the alarm code is shared among eight IT personnel. As a result, there may be accountability issues in case of a breach to the server room.

Management Action Plan

UCI Facilities Management's plumbers have worked on the AC unit and replaced the condensate pump and will install a new humidifier tank. Since the pump was replaced, ICS has not seen any water in or under the AC unit.

Regarding entry to the server room, ICS Computing Support (ICS CS) does not see a significant need to change from a standard lock and key or to install video surveillance. In addition, UCI Facilities Management Systems shop could not reprogram the alarm system. ICS CS is currently working to set up a contract with Unique Security to take over programming and maintenance. These changes will include deleting all "old" or existing codes, and replacing with unique codes to be assigned to each individual who needs to enter alarmed spaces. These will be reviewed at least once per quarter, and changes made as often as needed to keep the system secure. The estimated completion date is July 2011.

6. Change Management

Background

The goal of the change management process is to ensure all changes, including emergency maintenance and patches relating to infrastructure and applications within the production environment, are formally managed in a controlled manner. Changes, including those to procedures, processes, and systems, are logged, assessed, and authorized prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of risks that may negatively impact the stability or integrity of the production environment.

Observation

Discussions with the Director of ICS CS indicated that they do not have a documented change management process. However, ICS CS was able to provide evidence of requested changes, tracking, and version control of system level changes made in the UNIX environment. Request for changes are tracked using the "Request Tracker" (RT) ticketing system. Version control in the UNIX environment is managed using the Git version control system. IAS suggests that ICS CS consider strengthening change management processes in the following area:

- Set up formal change management policies and procedures to handle, in a standardized manner, all requests (including emergency changes) for changes to applications and systems within the production environment. This should include logging, assessing and authorizing prior to implementation, and reviewing against planned outcomes. Also, when possible, different people should perform the following tasks: implementation, review, and migration to production.

Management Action Plan

To accomplish this successfully, ICS CS needs to research best practices from others in the UCI community. ICS CS plans to talk to representatives of the UCI Office of Information Technology (OIT) and other units on campus. ICS CS will then define procedures to capture requests, get approval, define testing needed, track testing, get customer signoff, and track who migrated to production.

At this time, with limited staff resources, it is very difficult to fully implement a complete change management policy. The amount of documentation which results from requests could add significant time to any request. Separation of duties with reduced staff (e.g. one programmer and loss of two people in the systems administration group) will be difficult to implement. ICS CS does not fall under any regulatory restrictions to keep strict documentation for all systems.

ICS CS plans to have policies and procedures in place by January 2012.

7. Business Continuity and Disaster Recovery

Background

UC Business and Finance Bulletin, Continuity Planning and Disaster Recovery (IS-12) states that the overall goal of continuity planning should be to reduce risk and minimize disruption of campus research and academic programs and of supportive campus business functions. Risk assessments or business impact analyses should be conducted to identify all critical functions of the organization or unit and their supporting information systems. The impact of loss or disruption of functions should be identified, evaluated, and categorized according to the time frames required for recovery of each function.

Observation

ICS CS has completed a business continuity plan using the UC Ready tool; however, IAS noted some key areas in the IT part of the UC Ready plan on applications and systems were not complete - for example, backup information, offsite storage, etc. In addition, while the IT business continuity/disaster recovery plans are not limited to the below, the following should be considered:

- Alternative processing location;
- List of hardware, software, media and network components necessary for the operation of critical systems. Also, document specific restore instructions and restore order for each critical server; and
- Periodic testing of the disaster recovery plan.

Management Action Plan

ICS CS has a good start on disaster recovery (DR) planning. They will continue to update their DR with the UC Ready planning tool. This process will take considerable effort and time to accomplish as described in the preliminary report due to the complex nature of the ICS environment and reduced personnel. They work in a very fluid environment and the DR plan will need constant attention. They will add a section to the change management policies and procedures to include updating the DR plan for bringing new systems online and when updating existing systems.

ICS CS currently tests the DR during actual failures. They also regularly restore items from backup due to disk failures or accidental deletions. ICS CS will periodically test portions of the DR plan on a quarterly basis.

ICS CS will identify an alternative location, by contacting other departments and UC campuses. As time allows, ICS CS will assign staff/students to document the critical servers, hardware requirement, network connections necessary for operation, and specific restore instructions for each critical server including a list of media needed. ICS will also periodically test the ability to restore specific systems should a disaster occur.

ICS CS plans to implement by June 2012.

8. User Account Management

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. This also includes an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Management should perform regular review of all accounts and related privileges.

Observation

Discussions with ICS CS and the ICS Personnel Manager indicate that specific procedures on suspending, modifying, and closing user accounts and related user privileges have not been fully documented. In addition, IAS found and discussed with ICS CS the account administrative deficiencies in the areas of Active Directory accounts (including dormant accounts), terminated accounts, and other accounts that did not align with ICS procedures.

ICS CS provided some documentation on the creation of UNIX-based group accounts and the method to expunge expired accounts from the Lightweight Directory Access Protocol (LDAP) directory. In addition, IAS noted that ICS user accounts are mostly set to expire automatically to help with user account management. For example, student accounts are extended if they are taking classes; staff and faculty accounts are extended with the approval of their supervisors.

IAS suggests that ICS CS consider strengthening user account management in the following areas:

- Establish, document, and implement a standard user access request for approving, suspending, modifying, and closing of user accounts and related privileges procedures;
- Establish, document, and implement a procedure for periodic review of all accounts and related privileges for departmental applications.

Management Action Plan

ICS CS will create policies and procedures for request and approval of accounts, changes to accounts, and access permissions. They will also create a way to show what access to departmental applications a user has. ICS CS also plans to work with the ICS Personnel Manager to create or modify a checklist for when a person separates from ICS. This will include having the supervisor or the personnel office contact ICS CS to receive a list of applications to which the user has access and who to contact regarding removal of rights.

ICS CS will also define procedures for reviewing accounts/privileges for departmental applications and Active Directory on a quarterly basis. They will need to work with the ICS Personnel Manager and the application administrators to determine which account accesses are valid.

ICS CS policy has been to expunge accounts annually after an account has been expired for over a year. With the reduced staffing levels, this policy has not been followed. Other, more critical, items have kept ICS CS from expunging accounts for quite a while.

ICS CS plans to have the above in place by October 2011.