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

THE HENRY SAMUELI SCHOOL OF ENGINEERING
Report No. 2012-105

May 21, 2012

Prepared by:
Julie Chung
Senior Auditor

Reviewed by:
Mike Bathke
Audit Manager

Reviewed by:
Bent Nielsen
Director

IRVINE: INTERNAL AUDIT SERVICES

May 21, 2012

GREGORY WASHINGTON
DEAN
THE HENRY SAMUELI SCHOOL OF ENGINEERING

RE: The Henry Samueli School of Engineering
Report No. 2012-105

Internal Audit Services has completed the review of The Henry Samueli School of Engineering 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: Carol Jun, Assistant Dean
Katherine Gallardo, Director of Finance
Audit Committee

I. EXECUTIVE SUMMARY

In accordance with the fiscal year 2011-12 audit plan, Internal Audit Services (IAS) reviewed the adequacy of internal controls, policy compliance, and information technology (IT) operations for The Henry Samueli School of Engineering (HSSoE) within the University of California, Irvine (UCI). Business risks and control concerns were identified. Specifically, the following issues were noted.

Cash Handling Procedures – Based on a review of three out of eight departments, we noted some instances where funds greater than $500 were collected and accumulated over a period of time and not deposited in a timely manner. In addition, adequate physical security measures, control procedures, and separation of duties were not maintained. These observations are discussed in section V.1.

Sales and Services Revenue – Sales and services agreements were not obtained when departments rendered a service or provided goods to a non-University entity. This observation is discussed in section V.2.

Non-Payroll Expenditures – Proper supporting documentation was not maintained for some transactions reviewed. Most transactions were not authorized/approved prior to purchase, some purchases were reviewed/approved by a subordinate, in some instances the reimbursement payee also prepared (but did not approve) the reimbursement, and travel reimbursements were not submitted on a timely basis as required by policy. These observations are discussed in sections V.3 and V.4.

Payroll Certification – Some payroll certifications were past due and had not been submitted to Contracts and Grants Accounting in a timely manner. These observations are discussed in section V.5.

Equipment Management – Some inventorial equipment was not identified with the UCI property tag, stored in the reported location, or accurately reported to the Equipment Management Office. In addition, not all departmental custodians performed an annual physical inventory of the equipment or updated the equipment information in the Equipment Management System (EQS) to accurately report their observations. These observations are discussed in sections V.6.

IT Operations – The IT environment in two research departments, that maintain their own IT structure separate from HSSoE, could be strengthened by developing and implementing a formal process for updating software, installing anti-malware software, ensuring physical and environmental security of servers and documenting disaster recovery plans. These observations are discussed in sections V.7, V.8, and V.9.

II. BACKGROUND

HSSoE at UCI was founded in 1965. The school is home to five academic departments, and affiliated with two dozen research centers and state-of-the-art experimental facilities. In fiscal year 2010-2011, there were 2,579 undergraduate students and 720 graduate students enrolled in the HSSoE. The U.S. News & World Report ranked HSSoE as the 39th best engineering graduate school in its national rankings for 2012.

III. PURPOSE, SCOPE AND OBJECTIVES

The purpose of the audit was to review internal controls, policy compliance, and IT operations from July 2010 to present. Based on the assessed risks the following objectives were established:

1. Verify if the required general, confidential, payroll, and medical documents are properly maintained and filed in personnel records;

2. Determine whether the following aspects of employee time reporting: overtime approval, payroll ledger reconciliations, and sick and vacation balance tracking, comply with University policy;

3. Review non-payroll expenditures for proper approval and supporting documentation in compliance with University policy;

4. Evaluate inventory tracking procedures and sample inventorial items to ensure appropriate UCI tagging and location;

5. Evaluate whether there are adequate controls over budgeting and accounting and confirm if ledgers are reconciled;

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

7. Verify whether the Budget Office, Material & Risk Management, and Office of Research Administration (ORA) reviewed and approved agreements where departments/units received income from sales and services to external entities and determine if the rates charged properly accounted for costs;

8. Review appropriateness of cost transfers, completion of payroll certifications, and federal award overdrafts; and

9. Review selected IT operations.

IV. CONCLUSION

Business risks and control concerns were identified in cash handling procedures, sales and services, non-payroll expenditures, payroll certifications, human resources, equipment management, key controls, and IT operations.

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. Cash Handling Procedures

Observation

Several units and departments within the HSSoE receive cash for services such as the copy center for photocopies and departments for key deposits. IAS selected three cash handling entities to determine if each complied with the established policies and procedures. The following is a summary of the observations.

Deposits

IAS noted some instances when cash collections were not deposited in a timely manner. In addition, the cash was not maintained in a secure manner. Appropriate lockable receptacles or burglarproof/fire resistant safes were not used to store cash based on the appropriate cash limits.

IAS also noted that in some instances deposits were not validated and prepared in dual custody. IAS found that some deposits lacked support or did not match the supporting documentation and no explanation was noted for the differences.

Failure to validate deposits and prepare them in a timely manner as well as to properly safeguard cash, weakens the control structure and may lead to theft of cash.

Separation of Duties

Control procedures that ensure an adequate separation of duties is maintained over HSSoE cash handling processes need improvement. In some instances, separation of duties and individual accountability for cash were not being

maintained throughout the receiving, processing, and depositing of the funds collected. Failure to maintain adequate separation of duties over cash related functions may result in a diversion of University funds.

Refunds

Refunded transactions were not adequately documented. IAS reviewed a sample of transactions and noted that refunds were not explained and the transactions were not adequately reviewed/approved in writing by the supervisor. Inadequate management of refunded transactions increases the risks of fraudulent transactions being processed subjecting the University to unnecessary financial loss.

Management Action Plan

Managers of HSSoE units that collect cash will be involved in a review of BUS-49 and will establish procedures and systems to comply with policy by June 2012. Steps will be taken to ensure that receipts are provided for cash deposits, funds are secured in an appropriate locked receptacle, accumulations of funds are deposited before locked receptacle limits are reached, deposit amounts are validated, separation of duties is achieved (where no single person is responsible for collection, handling, depositing, and accounting for funds), funds are reconciled on a quarterly basis, and refunds are documented and approved.

2. Sales and Services Revenue

Background

A Sales and Services Agreement is initiated when a campus unit wishes to render a service or provide goods to a non-University user for which revenue is collected. This transaction is appropriate when the furnishing department incurs expense to make available a product or service which is sold to the non-University user for an established price, or at a price based on an established standard pricing method.

UCI Administrative Policy Sec. 703-14 establishes a mechanism for requesting, reviewing, and approving Sales and Services Agreements between the University community and a non-University entity. Under the policy, the campus unit should establish charges for the sale of goods and services provided to non-University users to ensure that University costs, both direct and indirect, are fully recovered.

Observation

IAS reviewed a sample of sales and services deposits and noted that most of the transactions lacked sales and services agreements. In addition, analyses and/or justifications for rates charged to non-University entities were not documented and maintained on file so it is uncertain if the rates charged fully recover University costs. Further discussion with department administrative management revealed that many of them were unaware of the goods/services rendered until they were asked to invoice a non-University entity.

The University may be subject to legal and financial exposure without a clearly stated sales and services agreement outlining the entire scope of the goods/services (i.e., relationship of the parties, rates charged, indemnification, etc.).

Management Action Plan

By June 2012, HSSoE managers will conduct a review of the UCI policy 703-14: Sales and Services Income Guidelines; Materiel and Risk Management policies and guidelines pertaining to Sales and Service Agreements and Business Contracts; and UCI policy 703-13: Recharge Accounts and Rate Review Procedures. Efforts will be made to communicate with faculty about the need to establish authorized sales and services activities in advance, with documented rates, and properly executed contracts before the start of any work for services being provided to outside entities. HSSoE administrative management will ensure that indirect costs are included in the rates being charged and that indirect costs are charged appropriately

HSSoE managers will also conduct an internal review of the documentation for all existing sales and services accounts to ensure that future use of the accounts is consistent with the activities being conducted and that rates are documented and authorized. New accounts will be requested for each new activity.

3. PALCard Purchases

Background

UC purchasing policies require purchases to be pre-approved either through 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.

Observation

IAS analyzed PALCard processes and selected a sample of 26 transactions for review, and noted the following:

- For five of 26 (19 percent) transactions reviewed, an internal requisition was not submitted. In addition, two other internal requisitions were dated after the purchase dates.
- For eight of 26 (31 percent) transactions reviewed, an appropriate authorization signature was not obtained. For six of the eight transactions, the PALCard holder authorized their own purchase or did not submit an internal requisition, and the PALCard reviewer is a subordinate. In addition, the majority of internal requisitions reviewed were not dated by the individual authorizing the transaction. Therefore, IAS was not able to determine if the purchase requests were properly authorized prior to the purchase date.
- For five of 26 (19 percent) transactions reviewed, a receipt was not maintained on file and available at the time of PALCard transaction review.

IAS also compiled a fiscal year 2010-11 report with PALCard purchases that were automatically approved through the PALCard review system. IAS identified 2,018 transactions totaling $116,981 (5 percent) in PALCard purchases that were not reviewed in a timely manner or not reviewed at all.

Controls over PALCard transactions, such as proper authorization of transactions and timely reviews, needs improvement to reduce the risk of error or misuse. Proper authorization and timely review of transactions reduces the risk of inappropriate costs or unauthorized use of University funds.

Management Action Plan

HSSoE managers and supervisors of PALCard holders will review the following expectations with card holders in their units by July 2012.

- An internal requisition will be generated in a timely manner, preferably on the same day of purchase, by each PALCard holder to document the purchase.
- Authorization for each PALCard purchase will be documented on the internal requisition. Authorization will be from the person assigned responsibility for overseeing expenses on the account being charged (e.g. unit manager, director, chair, PI). The approver will be someone other than the PALCard holder, and should not be a subordinate.
- Purchase authorizations will be obtained before or immediately after the purchase. Procedural expectations for the timing of the authorization (before

or after) can be determined at the discretion of the unit manager responsible for the account.

- Original receipts will be attached to internal requisitions for all transactions, and documentation will be provided to reviewers in a timely manner (ideally within 5 business days of the charge being processed). Documentation should be provided well before the reviewer deadline to ensure adequate time for review and processing, and to minimize the administrative burden of tracking down outstanding paperwork.

Compliance with these expectations will be emphasized and enforced by PALCard reviewers effective immediately.

4. PayQuest Reimbursements

Background

IAS reviewed a sample of PayQuest reimbursements for appropriateness and compliance with University polices.

A. Travel Authorization & Untimely Submission of Travel Vouchers

Observation

HSSoE does not have an adequate mechanism in place to properly authorize and monitor travel for academic appointees. Most of the PayQuest travel transactions reviewed lacked pre-authorization and many had been submitted late, including one that was submitted over two years after the travel date.

IAS recommends that HSSoE require academic personnel to complete AP-76 forms for all travels/leaves of more than seven days and to complete a travel authorization form for travels/leaves less than seven days. These forms can then be used as authorization for travel of certain categories of leave as well as to monitor travel to ensure compliance with University policies.

B. Payee Prepared or Approved Reimbursement

Observation

IAS noted over 50 PayQuest transactions totaling approximately $23,500 had been prepared by the same individual that was the payee. Additional review revealed that most of these PayQuest reimbursements contained the appropriate approval signature. However, IAS noted several instances when the department had used a signature stamp to approve these PayQuest transactions so it is uncertain if some reimbursements had been properly reviewed/approved by a

separate individual. In addition, IAS noted several examples when the payee had approved their own reimbursement.

Allowing the payee to prepare or approve their own reimbursement weakens the control structure and increases the potential for errors/inaccuracies and fraud to go undetected.

C. Lack of Travel's Signature on PayQuest Cover Sheet

Background

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. UC policy (G-28) states that internal departmental expense claim forms are not an acceptable alternative for obtaining the traveler's signature on the travel expense voucher (or electronic equivalent), unless approved as an exception to this policy.

Observation

Most of the travel reimbursements reviewed lacked the traveler's certification on the PayQuest cover sheet. The non-compliant PayQuest cover sheets contained "see attached" notations on the traveler certification signature line, which then referred to/relied upon the signature noted on the internal request for reimbursement as the traveler's certification.

Allowing preparers to use "see attached" notations on the traveler certification line weakens the control structure and reduces the ability to detect inaccuracies.

Management Action Plan

HSSoE faculty and unit management will be reminded about the requirement to submit form AP-76 in advance of travel lasting more than seven days.

A discussion has already taken place to emphasize the need for separation of duties. HSSoE managers were explicitly informed to make sure that the preparer and approver are different people, and that the approver has delegated authority to sign. They were also strongly encouraged to avoid being the preparer and payee. Units will be discouraged from using signature stamps.

Regarding the lack of signatures on the travel voucher cover page, HSSoE management acknowledges this compliance issue. The HSSoE Director of Finance is working with the UCI Managers of Academic and Administrative Business Offices (MAABO) group and UCI Controller to propose a change to the

G-28 policy language that explicitly disallows internal department forms. This language was news to many financial managers on campus, who were continuing to function in compliance with prior guidance by UCI Accounting that internal forms with certification language identical to PayQuest were acceptable. To achieve immediate compliance represents a significant workload issue and will impact the timeliness of travel submission. Therefore, steps are being taken to either modify the policy in a way that addresses risk but that also does not create undue administrative work, or to identify systems/procedures that will facilitate electronic certification.

5. Payroll Certification

Background

The Department of Health and Human Services approved the implementation of the Payroll Certification System, a pilot program which substantiates salaries charged directly to federally funded projects, as an alternative to Personnel Activity Reporting (PAR).

Under the new process, payroll certification will occur at the end of a budget year or other reporting schedule as identified by an award's terms and conditions for every federal or federal flow-through project. The departments are required to send a copy of the signed Certification Report, with a copy of the Payroll Expense Report attached, to Contracts & Grants Accounting (C&G) and maintain the original documents.

Departments have 70 days from the budget or project end date to submit a copy of the signed payroll certification forms to C&G. Timeliness is a key factor in the payroll certification process.

Observation

IAS reviewed the C&G report on the current payroll certification status as of November 30, 2011, which showed that a total of 84 payroll certifications were due. The following is a summary of IAS review:

- Payroll certifications for 17 contracts/grants were past due and had not been submitted to C&G;
- Payroll certifications for five contracts/grants that were initially submitted to C&G required recertification due to corrections. However, all five recertifications had not been submitted to C&G as of November 30, 2011;
- Six payroll certifications were submitted late; and
- Fifty-six payroll certifications were submitted timely.

IAS selected five payroll certifications from the C&G report (two payroll certifications submitted timely and three that were not submitted per the status report) for further review. For the two timely submissions, IAS confirmed that the original copy of the payroll certification was maintained on file and that the Principal Investigator (PI) signed and dated the payroll certifications as required. For the three that were not submitted, one payroll certification was submitted to C&G on December 2, 2011 upon IAS inquiry, the second payroll certification was received by the department analyst from the PI on November 30, 2011 (one day prior to IAS review), and the last payroll certification was initially submitted to C&G but was rejected due to correction to reflect cost sharing and the recertification report has not been submitted because the PI is out of the country.

Management Action Plan

Actions are currently underway to achieve a near 100 percent completion of outstanding payroll certification forms. This is still a relatively new process and HSSoE is working to improve timely generation of forms, internal tracking, and adequate follow-up. In addition, HSSoE management is working with C&G to improve notifications and reminders that would be helpful to achieve timely submission.

6. Equipment Management

Background

For Equipment Management purposes, UCI equipment is defined as any equipment with an acquisition cost of $5,000 or more and a useful life of one year or more. UCI policy requires an acceptable property control system which includes affixing property tags to items, inventory of items, reporting changes, and reporting lost or stolen property.

Annually, the Equipment Management Office provides departments/units with a copy of its current equipment list. The department should then review the report, confirm the location of the equipment, add new equipment, delete sold equipment, and return a signed copy of the report to Equipment Management. The department should then update these changes by entering the information into the EQS.

Observation

IAS selected inventorial equipment items to determine if each item was identified with the UCI property tag, stored in the reported location, and accurately reported to the Equipment Management Office. The following is a summary of the observations:

- Nine of the 15 items were not identified with the UCI property tag;
- Three of the 15 items reviewed were not found in the designated location as reported to the Equipment Management Office; and
- Not all departmental custodians performed an annual physical inventory of the equipment by verifying each item on the equipment management report to the property tag or serial number on the equipment, and the room location. One department custodian did perform an annual physical inventory, but did not update the equipment information in EQS to accurately report his observations.

Failure to maintain an accurate equipment inventory weakens the control structure and reduces the ability to detect inaccuracies and theft.

Management Action Plan

Equipment management responsibilities within HSSoE are decentralized to each unit. Detailed action plans for each unit have been developed and will be reviewed by IAS during the follow-up process.

In general, HSSoE units will make an effort to affix property tags to equipment that are missing tags. In addition, units will perform annual physical inventories and will update EQS as part of the inventory review process.

7. Patch Management and Protection Against Malware

Background

Information system (including servers, workstations, and mobile computing devices) should implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam). Virus-scanning software should be provided at critical entry points, such as remote access servers and at each desktop system on the network.

Observation

A. Patch Management and Malware Protection

Discussion with the Research Engineer for Advanced Power and Energy Program (APEP) indicated that there is no process to automatically scan and update third party software (i.e. flash, adobe, java, MS Office etc.) on end user computers they manage. Third party software patches are manually applied to the servers on a

monthly basis and Windows Server Update Services performs automatic updates to the operating systems. Software vulnerabilities that are not patched or outdated software increases risk that data and information systems could be compromised.

Additional discussions indicate that while workstations are installed with Microsoft Security Essentials antivirus, the virtualized servers do not have real-time malicious software protection installed. Without up-to-date malicious software protection software, APEP is at risk that their computers cannot prevent, detect, and remove malware which could lead to exposure of sensitive information. In addition, the University network could also be affected and suffer the same consequences by malicious code through APEP systems.

Management Action Plan

We are currently evaluating Security/Patch management products. We have installed the software on a test environment, and we are currently working to compare the functions, ease of deployment, and effectiveness on reporting and preventing latest security threats. We plan to implement this by June 2012.

B. Protection against Malware

Discussion with the Computer Resource Specialist for Integrated Nanosystems Research Facility (INRF) indicate that while the servers are installed with malicious software protection software, the workstations and other end user computers do not have real-time malicious software protection. Without up-to-date malicious software protection, INRF is at risk that their computers cannot prevent, detect, and remove malware which could lead to exposure of sensitive information. In addition, the University network could also be affected by malicious code through INRF systems.

Management Action Plan

INRF management agrees with the need to protect their systems from malware. The current browsers running on the machines are Internet Explorer 9 and Google chrome. These two browsers already implement malware website detection and malware download prevention. Both of these browsers also implement sandboxing which prevent malware from getting access to the operating systems. OIT mail servers run malware detection for all emails routed and received through their servers. At the same time, the mail client software automatically implements spam and malware protection. This mitigates the malware coming through email.

However, most malware come through the browser which cannot be all stopped. There is also risk of users running unauthorized scripts and executable files from CDs, USB flash drive and internet downloads. Therefore, INRF management has

already taken the initiative to implement real time scanning via PANDA. In addition, they are evaluating user training options with probable completion by the end of June 2012.

8. Server Physical Security

Background

Protection for computer equipment and personnel requires well-designed and well-managed physical 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, video surveillance, 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 room where the INRF four servers are located and noted that adequate physical and environmental controls were not in place to detect and contain potential physical and environmental threats. Discussion with the Computer Resource Specialist also indicated that in the past there have been water leaks from the ceiling by the servers and a computer monitor theft. Without adequate physical and environmental controls, there is increased risk of damage and theft that could cause interruption to INRF operations.

Management Action Plan

INRF management agrees that their servers should be secure. They have initial planning stages for relocating the servers to the OIT Academic Data Center or through Virtual Server Hosting. An option is also available to relocate the server to the Calit2 server room. They also need to verify with OIT whether Cisco vlan ipx could be implemented since it is necessary for the INRF facility server to facilitate relocation. INRF management will assess the above available options and implement the steps to ensure physically and environmental security of their servers. At the earliest, the probable completion date is end of June 2012.

9. Disaster Recovery Plan

Background

A disaster recovery plan is a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. The plan enables the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.

Observation

Discussion with the research engineers for APEP and INRF indicated that while there are no formal contingency plans, APEP and INRF performs backup of their data on a defined schedule. In addition, APEP and INRF does not utilize offsite backup storage. Currently, backup is stored in alternate servers and other storage media in the same vicinity as the production servers. Without a plan for offsite storage, APEP risks not being able restore critical business information in the event of a significant disruption.

Management Action Plan - APEP

APEP management is currently evaluating off-site backup solutions as well as looking into off-site backup storage at the UC San Diego Data Center.

APEP will test disaster recovery plans on restoring the server in emergency bare-metal restore process. They also plan to regularly test backup data for data integrity and will have documentation on the type of servers and data backups. Servers include Domain Controller, Windows Servers, Exchange, and SQL. The type of data includes critical, non-critical, and archived. The plan for implementation is by the end of June 2012.

Management Action Plan - INRF

INRF is currently evaluating disaster recovery plan solutions. A server can be restored from backup or rebuilt and configured in a day which is an option currently available since the servers were upgraded a couple of times. Running a server from a remote site or through virtual hosting allows new options to be available. They will review the UC Ready documentation to find out the requirements for proper planning, staging, and implementation of a formal contingency plan.

Since part of the requirement is securing the servers, this is tied to the physical security of the servers. The servers for INRF are composed of the business side

and the facility side. For the business side, INRF will plan to relocate backup data offsite to OIT through virtual hosting or by physically moving. The facility side is a different matter since the server for the facility could be easily restored and relocated, but most of the equipment are specialized and located onsite. Only the server equipment could be easily relocated offsite. Probable completion date for implementing a contingency plan and storing backup offsite is the end of June 2012.