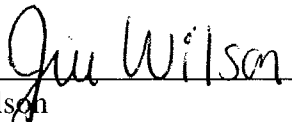UNIVERSITY OF CALIFORNIA, IRVINE
ADMINISTRATIVE AND BUSINESS SERVICES
INTERNAL AUDIT SERVICES

FACILITIES MANAGEMENT
Report No. 2011-107

May 31, 2011

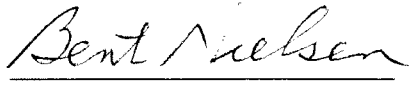Prepared by:

Jill Wilson
Jill Wilson
Senior Auditor

Reviewed by: Reviewed by:

Mike Bathke   _Bent Nielsen_
Mike Bathke   Bent Nielsen
Campus Audit Manager   Director

May 31, 2011

MARC A. GOMEZ
INTERIM ASSISTANT VICE CHANCELLOR
FACILITIES MANAGEMENT

RE: Facilities Management
     Report No. 2011-107

Internal Audit Services has completed the review of Facilities Management and the final report is attached.

Please let me know if you have any questions regarding this document.

Bent Nielsen
Director
UC Irvine Internal Audit Services

Attachment

C: Alan Smith
   Audit Committee

I.   EXECUTIVE SUMMARY

In accordance with the fiscal year 2010-2011 audit plan, Internal Audit Services (IAS) reviewed the adequacy of internal controls, policy compliance, and IT operations for Facilities Management (FM) within the University of California, Irvine (UCI) campus. Business risks and control concerns were identified. Specifically, we noted the following.

FACserv - FACserv navigation, work order completeness, and job reporting and monitoring need improvement to ensure essential information is captured and to measure job cost performance and productivity against established work measurements. The observation is discussed in section V.1.

Equipment Management, Trades Material Inventory and Yard Security – The updating of equipment inventory into UCI's Equipment Management System (EQS) and an official procedure for entering and removing equipment needs to be established. A physical inventory of shop trades materials and supplies has not been performed since 2007. Yard security needs to be improved to control theft sensitive items and protect assets from the environment. The observations are discussed in sections V.2, V.6 and V.7.

Payroll and Personnel – Payroll ledger review and reconciliation is not being performed. Also, FM Human Resources does not have a system in place to ensure employees clear a background check.   This process creates the risk of background checks being failed or not taken by the employees since employees are allowed to start working before the background check clearance is received. The observations are discussed in sections V.3 and V.4.

Non-Payroll Expenditures – The internal controls over authorizing, documenting, and processing PALCard transactions needs improvement. The observations included lack of proper approval of internal requisitions, lack of packing slips, and lack of appropriate reviewer documentation. Additional details are discussed in section V.5.

Contractors Working Without a Contract – Contractors are starting work before a contract has been prepared. This creates a risk to the University since if a contract was not in place, it is unlikely that the licensing and insurance requirements were finalized before the work started. Additional details are discussed in V.8.

Updating of Policies – Policies have not been updated on a regular basis. A few policies have not been updated since 1997.   Keeping policies current helps individuals to remain compliant and to follow consistent practices. Additional details are discussed in V.9.

Information Technology (IT) – IT operations can be improved upon in the following areas: user account management, separation of duties, change management, risk assessment, security plans, continuity and disaster recovery, and FACnet. The observations are discussed in sections V.10-V.15.

II. BACKGROUND

FM is responsible for the maintenance of all buildings, grounds, and utility systems on the UCI campus. FM has approximately 226 employees with an annual operating budget of $65 million in fiscal year 2009-10. The FM staff works on more than 170 buildings and 1,475 acres of land and provides general maintenance, operation and renovation of buildings, grounds, utility systems, custodial care, landscaping, fleet services, and engineering support.

III. PURPOSE, OBJECTIVES, AND SCOPE

The purpose of the audit was to review internal controls, policy compliance, and IT operations for the fiscal year 2009-2010 to present. Based on IAS's risk assessment of FM, the following objectives were established:

1. Evaluate the following aspects for employee management: personnel files, background checks, overtime approval, payroll ledger reconciliations, and sick and vacation balance tracking for appropriateness and completeness;

2. Review Payquest reimbursements and PalCard transactions for approval and appropriate documentation to determine compliance with University policy;

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

4. Review and verify that labor charges are accurate in the FACserv system;

5. Evaluate budget and accounting control;

6. Discuss and review cash handling, cash advance, and cash receipt procedures to determine evidence of controls and that assets are properly safeguarded;

7. Review IT operations including FACserv and FACnet.

IV. CONCLUSION

Business risks and control concerns were identified in the FACserv system, material and supply inventories, human resources, payroll reconciliation, non-payroll expenditures, equipment management, physical security, contract and project accounting, and information technology.

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. FACserv Work Order Detail, Monitoring, and Reporting

Background

FACserv is an Enterprise Resource Planning (ERP) application that integrates several of FM business processes, such as work order management, inventory management, customer service, and trade's billings.

Observation

FACserv

As part the payroll/overtime review, IAS reviewed timesheets and work orders with overtime in the FACserv system. IAS was able to confirm that the overtime reviewed was valid and properly approved. However, during the FACserv work order review process, IAS discovered that FACserv data capturing is limited.

Work Order Completeness

IAS examined the work order screens (resolutions, notes, and procedures) and found many of them to be blank or lacked essential information. The work order data entry screens reviewed did not contain a clear scope of work performed, an estimated budget to indentify a basis for assigning personnel, number of hours, or completion of tasks necessary to manage the performance of work, expectations, and obligations. It appears this could be caused by FM staff not entering detailed information. Also, FM may want to work with Office of Information Technology (OIT) to create new fields in FACserv in order to display essential information as determined by management.

According to the FM Business Office Manager, customers often complain that there is not enough information on their bill. If a customer complains, the FM

Business Office Manager has to follow-up with the trades to determine a complaint resolution. These complaints are frequent, time consuming, and cause poor customer relations. In some cases, the bill is reduced to satisfy the customer. Work order information is essential and standard operating procedures in most similar public and private trades.

Job Reporting and Monitoring

IAS discussed the FACserv system and reporting capabilities with the OIT programmer/analyst who supports the system for FM. The programmer/analyst stated that the FACserv system can report on just about all of the data contained in the system. If OIT gets a request from FM for a FACserv report, it can generally be created with relative ease. Currently, OIT can provide reports or spreadsheets of this kind on an adhoc basis but "canned" user reports are limited.

The programmer/analyst provided IAS with three adhoc production reports (active work order with zero charges, closed or completed work orders with zero charges, and closed or completed work orders where the job status is showing in progress). The reports had numerous discrepancies between work order status and job status, many dating back to 2007. Some work orders listed as active had the job status as closed and completed. Other work orders listed as closed or completed were displaying a job status as in progress. The OIT programmer/analyst explained that the old transactions cannot be deleted from FACserv since there would be no history. In addition, the programmer/analyst believes that most of these discrepancies have a valid explanation. If one work order number is active, then the other work orders could accurately be listed as closed or completed while showing job status as in progress since one work order has yet to be completed.

Another report had work orders listed as closed or completed and had over 10,000 closed job orders with zero charges. The OIT programmer/analyst believes that some of these transactions could be legitimate but they still should be reviewed. Currently there is no process in place to determine if they are legitimate transactions. IAS discussed the observations with the FM Business Office Manager who agreed this is an area of concern and that funds could be lost since the jobs may not have been billed for labor and materials in a timely manner. The closing of a job, rather than the job completion, affects accounts not being billed since FM must bill prior to the close-out taking place. FM must recharge departments or complete transfers of expense within 90 days.

Failure to properly monitor transactions to ensure that all charges are accurately and timely posted and billed may result in lost revenues and inflated job costs, and reduces the ability to accurately measure productivity and detect inaccuracies. Failure to properly document the work orders to ensure the work performed is

clear and complete, in addition to other essential information necessary to manage the performance of work, expectations, and obligations could result in poor customer service and complaints, and reduces the ability to measure job cost performance and productivity against established work measurements or criteria.

FM management should work with OIT programmers to create additional and regularly used FACserv reports to improve monitoring and tracking of work orders. In addition, this could help to ensure that all information is accurate and entered timely. IAS recommends that FM management review the discrepancy reports noted above and develop a plan to monitor and resolve these issues in the future.

Management Action Plan

Work Order Completeness

FM management agrees that the ability to capture and report on data in FACserv is under-utilized. It is an ongoing process to improve the functionality of the system while still maintaining a balanced work load for FM shop supervisors. In FY2009-10, there were over 29,000 work orders created. FM management does not think it is an efficient or effective use of supervisor time or FM resources to enter detailed information on every work order.

FM and OIT have plans to simplify and standardize information entry and reporting capabilities with the next software upgrade. In the meantime, FM management will continue to work closely with the OIT team to create improvements to FACserv that will allow supervisors to capture additional reportable data in a simpler, more efficient manner.

Estimated implementation is May 2012.

Job Reporting and Monitoring

FM management and OIT agree that FACserv transactions should be reviewed for appropriateness. Currently, OIT can create FACserv reports once they are requested by FM. However, since February 2010, OIT has been working with FM management on various productivity reports that are available to FM employees through UCI's SNAP website. This is an ongoing process with three new reports currently available and complete. The new reports show employee productivity, shop workload, and work completed without charges. In addition, OIT is working on a report that can be used by management to monitor FACserv activity. The estimated completed date for this report is December 2011.

During the past year, FM management has made concerted efforts to increase accountability and improve customer services across the department. With this effort, there has been considerably more interest in the ability to review and report on various metrics, thus more reporting tools have been, and will continue to be, created.

2. Trades Materials Physical Inventory

Background

Nearly $4 million of inventorial materials and supplies are procured and managed by FM Shop Stores each year, which represents the vast majority of material and supply purchases for FM. Stock supplies and materials are drawn down by the crafts and trades and charged to work order numbers within their shops. In most cases, parts and materials are not expensed or used entirely on one job. Usually they are stored for later use in shops, on service vehicles, or in building supply closets. The craft and trade shops receive approximately $350,000 of craft materials from Shop Stores. These inventories are relatively small compared to the total cost of inventory reported from Shop Stores, however the risk and exposure remain the same. These materials and supplies should be inventoried on an annual basis.

In a previous IAS audit report of FM Craft Shops (2003-104), it was noted that physical inventories of craft and trade shop materials and supplies had not been performed since 1999. As part of FM corrective action, the FACserv system was implemented in 2007 to integrate several of FM business processes including inventory management.

IAS performed a follow-up review to verify that FM management had taken corrective action to address the trades inventory reporting. The follow-up review determined that FM management had performed a physical inventory in Summer 2007 and implemented an adhoc inventory reporting mechanism, which satisfied the management corrective action requirements in the previous IAS audit report.

Observation

Based on discussions with the FM Business Office Manager, the Shop Store Manager, and an OIT programmer/analyst who supports inventory management in the FACserv system, physical inventories of shop trades materials and supplies have not been performed since the last physical inventory in 2007.

Not performing the routine inventories weakens the internal controls over inventory levels and supply usage, which reduces the likelihood of detecting errors and omissions in the event of a loss, theft, or product waste when items

become obsolete. University policy states that supply inventories are to be verified by physical count at least annually.

Management Action Plan

FM management agrees that physical inventories should be conducted on an annual basis. Currently, FM is in the process of reviewing their current business practices with regard to inventory monitoring and has started to expand the number of inventory locations within FACServ.

The Sign Shop will serve as the initial physical inventory test site. A requirements document is in the process of being developed and reviewed. Implementation is scheduled to begin before June 30, 2011. If the test proceeds well, FM will add inventory locations for the other shops. Once a shop has been added as an inventory location, the shop will be responsible for performing an annual physical count.

3. Human Resources

Background

Once an employee is hired in FM, FM Human Resource Department (FMHR) is responsible for ensuring that all completed documents are placed into the employee's personnel file. On occasion, Central HR may participate in the hiring process. This will occur when the new hires are of sensitive nature and this usually involves unions.

FMHR will conduct reference checks and request that a background check be completed by UCI Police (UCIPD) for all new hires. The results are reported and recorded at Central HR, who will then contact the department via email with job-related results. A background check should be performed for both internal and external hires in critical positions. Critical positions include some of the following functions: master key access, direct contact with minors, access to confidential files, and responsibility or access to cash, check or University disbursements or receipts.

Observation

Personnel Files

Personnel files for all employees are kept in a locked cabinet in FM Interim Office Building. IAS sampled ten personnel files for completeness.

- Two of the ten did not have a completed I-9 form.

- Three of the ten did not have a signed job description.

- Five of the ten did not have a signed job application.

- Two of the ten did not have a witness for the Oath/Patent Acknowledgement.

IAS discussed personnel files with the Director of Employment Services. It was confirmed that the completed I-9s and Oath/Patent Acknowledgements must be on-file in the employee's personnel record even if the originals were sent to the Payroll department. UCI Policy for Staff Members, Personnel Records Procedure 80 and UCI's SNAP website provides a checklist of the required and necessary personnel file documents.

Background Checks

FMHR allows individuals to start working before they are given a background check clearance. FMHR relies on Central HR to inform them via email that a background check has cleared. FMHR does not have a system in place in case Central HR does not notify them. In other words, if an employee does not go to UCIPD to initiate a background check, Central HR would not have an email to send regarding the results and FMHR would not know that the individual was not given a background check. FMHR does not have an email archive of the background check clearance emails and a paper copy of the email is not routinely being placed into the personnel file. Seven of the ten personnel files sampled did not have a copy of Central HR's background check clearance email. IAS also sampled an additional 16 employees to confirm whether a background check was completed and of the ones sampled, Central HR confirmed a background check was given and passed. 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.

Management Action Plan

FMHR recognizes the requirement to comply with University of California (UC) established guidelines for new hires and to comply with all applicable state and federal employment laws.

FMHR is a new department and is currently setting up internal controls and processes for improved compliance. FMHR is on the road to creating a new hire procedure and process manual and should have it completed by December 2011.

4. Lack of Reconciliation of Payroll Ledgers

Background

UCI policy states that each activity manager, who is directly responsible for the financial affairs of that activity, should maintain procedures that monitor and verify transactions in order to reconcile balances monthly to the General Ledger. Departments have a responsibility to ensure the appropriateness and accuracy of all financial transactions applied to their department's ledger. In addition, the department has the obligation of maintaining signed documentation of this review to ensure that they adhere to internal control procedures.

Observation

IAS and the FM Payroll Coordinator (PC) discussed payroll processes. The Payroll Coordinator position was created due to the complicated nature of time keeping in FM.

PC stated that the payroll ledger review and reconciliation to the General Ledger was performed in Central Payroll but since this position was re-assigned to FM, the review/reconciliation is not being performed. Reconciliations are integral to ensure that financial information is complete, accurate, and valid. Failure to perform payroll reconciliations may result in undetected payroll errors.

Management Action Plan

In January 2011 FM hired an individual for the Timesheet/Payroll Coordinator position. This position is now responsible for payroll ledger review and reconciliation to the General Ledger. IAS will follow-up in approximately six months.

5. PALCARD Review

Background

UCI PALCard policies require supporting documentation for each transaction. 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.

Appropriate reviewer documentation includes the TOEP (screen print) with user ID and 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 the transaction can be reviewed. 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 43 PALCard transactions during fiscal year 2009-10, and noted the following during the review:

- Twenty-nine of the 43 did not have an approved internal requisition or some other form of pre-approval for the purchase;

- Twelve of the 43 did not have either an internet confirmation screen or credit card receipt, if applicable;

- Ten of the 43 did not have a packing slip; and

- Nine of the 43 did not have appropriate reviewer documentation attached to the PALCard supporting documentation packet.

IAS also compiled a report with PALCard purchases dated from July 2009 to present that were automatically approved through the PALCard review system. IAS identified 264 transactions or $559,248 (11 percent) in PALCard purchases that were not reviewed in a timely manner or not reviewed at all.

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

FM will follow-up with the specific units identified in the IAS sample to ensure that PALCard and purchasing policies are understood and adhered to for future processes. In addition, FM will conduct a training class for all users to review the related policies and procedures and to clarify that all transactions are to be

reviewed by the assigned reviewer within the 14-day calendar period. Estimated implementation is December 2011.

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, UCI Equipment Management provides FM with a hard 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 Equipment Management system (EQS).

Observation

IAS sampled 60 pieces of equipment. Six of the 60 items or 10 percent could not be located. In addition, seven of the 60 items could not be confirmed to be the correct item due to missing UCI property tags or limited information from the equipment list. Some vehicles on the equipment list did not have any identifying details such as plate# or UCI's four digit vehicle identification number.

FM has been updating, signing and returning equipment lists to UCI's Equipment Management in a timely manner; however the updates are not being entered into EQS. The last inventory was in July 2009 and the updates were not entered at that time. Currently they are working on the new annual equipment list received and plan to enter any updates into EQS.

FM does not have official procedures for entering or removing equipment from inventory. Removing equipment from the inventory lists such as for disposal or salvage/surplus sale is not clearly defined or documented.

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

Management Action Plan

FM was able to find all six items that were not located during the review. The current locations of these items have now been updated into FM's EQS inventory by the Shop Stores Supervisor. FM also researched the seven items that could not be confirmed due to missing UCI property tags or limited information from the equipment list. UCI property tags will be placed on the items and documentation of vehicles will be complete. We will also stress to Unit Heads the importance of making sure that equipment inventory changes are properly reported. IAS will follow-up in December 2011.

7. **Yard and Equipment Security**

Background

FM oversees several yards which are used to house FM trade areas, fleet services, grounds and maintenance, and scrap metal storage. IAS walked the North Campus and Grounds Maintenance and Building Services yards on five days in October and November 2010, and January 2011 during business and non-business hours.

Observation

North Campus Yard

IAS observed the following issues at the North Campus Yard:

Yard Physical Security

- IAS sampled 40 vehicles and found 9 or 22 percent to be unlocked. This includes both vehicle doors unlocked and /or truck toolboxes unlocked.

- Gate opening and closing procedures are not clearly documented or defined. IAS received various responses as to how the process works. It is not clear how FM shares the responsibility with others with closing of the yard.

- Gates, when locked, are locked with old, low-grade chains.

- FM's response to our departmental questionnaire states that there are cameras in place to safeguard theft sensitive items but IAS could only locate one. The Shop Store Supervisor confirmed this.

- IAS walked the yard five times and was only questioned by one person as to what we were doing.

Protecting Theft Sensitive Items

- Power tools were found outside in the metal shop area after-hours.

- Refrigeration supply cabinets were not organized and inventory usage lists were dated as of 2007.

- Brand new pliers and other tools/screws were left out in rain in the back of a UCI truck.

- Multiple Weather Guard tool boxes were located outside and not protected from theft.

Failure to secure the yard, control theft sensitive items and protect assets from the environment increases the risk for loss of University resources.

Grounds Maintenance and Building Services Yard

Grounds Maintenance and Building Services business offices and vehicles are locked nightly to prevent theft and unauthorized access and craft/trade supply containers (used shipping containers used as storage) are kept locked with limited access to those in the trades. However, the remaining yard facility is left unlocked 24 hours a day with easy access to landscape materials (gravels, rocks, mulch, ground cover etc.), plants and trees inventory, masonry bricks, utility flatbed trailers, and other high value equipment around the yard.

In addition, the yard has been used as a dump site in which used mattresses, couches, and construction demolition material are dumped. We were advised that on several occasions, hazardous waste and materials (paints, solvents, VGA monitors and tires) have been dumped on the property. IAS performed a physical inspection of the area and confirmed several of these materials on site.

Management Action Plan

The North Campus Yard is the responsibility of multiple parties. UCI Parking and Transportation and UCI Police along with FM take a part in the securing of the yard. FM only controls some of the yard gates so even if FM locks their gates, other gates could still be left open by other responsible parties. Only if a unified effort takes place can FM ensure that the yard is secured. FM believes the focus should be and is on securing trade areas, vehicles and other supplies from theft. New gates and/or security are not an option at this time due to lack of

resources. FM management distributed a memo to remind staff of the importance of securing the yard and its materials and will continue to notify employees on an annual basis.

In March 2011, the FM Assistant Director, Building & Ground stated that the gates in the Grounds Maintenance and Building Services areas are now closed and locked from 5:30 pm to 4:30 am each day. IAS has since confirmed this practice so additional follow-up for this observation is deemed unnecessary.

8. **Contractors Working Without a Contract**

Background

FM Contracts fulfills requirements set forth by UCI and regulators in regards to construction contracts. The process starts with contractor selection and the preparation of a contract along with verifying any required documentation such as licenses or insurance. FM Contracts compiles the contracts and related verifications. The process ends with a separate unit, Project Accounting, paying the contractors for work completed. Project managers interact between the two units and work directly with contractors. They will assign work to be started after the contract is in place. A contract and appropriate documentation must be in place before the work can be started.

Observation

IAS identified a few cases where contractors are completing work before a contract has been written. Since the contract was not in place before the work was started, it is likely the licensing and insurance requirements were not checked or were not finalized before the work started.

IAS also obtained information that change order approval documentation was not always approved in advance. In some cases, Project Accounting was contacted by project managers to verify if funds were available to pay the contractor, after the work had already been completed. The proper process would be for change order documentation to be submitted and approved in FM Contracts prior to any additional work being started. If the additional funds are not secured in advance, it is not guaranteed that the funds will be available to pay the contractor. However, the contractor must still be paid so it takes extra time and creates internal conflict to find available funds in order to pay in a timely manner.

Contractors performing work before a contract is in place or before a change order is approved creates a risk to the University. Contractors may not have the required licensing and insurance requirements which creates a liability to the University. When change orders are not pre-approved, UCI is at risk of not

having available funds to pay the contractor. In addition, not pre-approving change orders creates the risk of missing new contractor requirements, such as being bonded, since this may be required if the new contract total exceeds a particular threshold.

Management Action Plan

A field order process exists that can be used by FM project managers to authorize additional work to be performed by the contractor in advance of an executed change order. There are several instances in which this process is employed. These include: eliminate safety or quality issue, maintain critical construction schedule and avoid cost increases. Project managers must be aware of the funding status of their projects to prevent project overruns.

Refresher training on contracting requirements and procedures will be conducted with all Project Managers. Training will cover the requirement to have a construction contract or contract change order in place prior to the start of construction activities. Contracts and Project Accounting groups will be included in the training on this approximate schedule:

- Prepare and have approved form to be signed by all Project Managers acknowledging participation in the training;
- Refresher training on the requirement to have construction contract, or contract change order, in place prior to start of construction;
- Refresher training on the use of field orders and change orders.

The estimated implementation date is June 2011.

9. Updating of Policies

Background

Policies and procedures should be updated and maintained on a regular basis. Without the use of current policies and procedures, the department increases its risk of being non-compliant and decreases the likelihood of following consistent practices in the department.

Observation

IAS noted that six FM policies had not been updated on a regular basis. Four of the six have not been updated since 1997. The other two policies have not been updated since 1998 and 2004.

Management Action Plan

The FM Administrative Coordinator agreed that the policies need updating. FM has made several attempts in the past few years to update the policies but it was not possible due to operational reasons. FM still considers this a priority and will work on updating the policies by December 2011. The Director of Administration and Budget stated that the process is already in place to conduct the updating of policies and procedures.

10. User Account Management

Background

UC Business and Finance Bulletin, Electronic Information Security (IS-3) requires that management implement policies and procedures to address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges. This should include an approval procedure outlining the Resource Proprietor (data or system owner) granting the access privileges. Procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. In addition, the Resource Proprietor should perform regular management review of all accounts and related privileges.

Access authorizations should be documented on standard forms and maintained on file. A formal process for transmitting these authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings.

Observation

Policies and Procedures

IAS interviewed FM individuals and found that specific procedures on suspending, modifying and closing user accounts and related user privileges had not been completed. During the fieldwork of this audit, FMHR was documenting new employee orientation procedures, which they stated will address requesting, establishing, and issuing of user accounts and related user privileges to FM systems.

Management Review of User Accounts

User account management controls should be enhanced in the areas of periodically performing reviews of user accounts and related privileges to ensure

access rights remain commensurate with user job responsibilities. Specific issues identified and corrected included:

- There were an excessive number of administrator user access accounts (nine). Only four accounts in OIT support FACserv and need administrator access. FM approved the removal of the five excess accounts;

- Seventeen out of the 144 active accounts belonged to terminated employees. FM worked with OIT to delete these accounts during this review; and

- Five employees no longer worked for FM but still worked at UCI. FM worked with OIT to delete these accounts during this review.

Standardized Formal Authorization Required

IAS sampled eight employees who were granted access to FACserv in 2010 to determine if creation of their FACserv accounts was appropriately approved. Specific observations included:

- Three accounts were for OIT employees but there was no evidence of access approval by supervisor or data owner;

- Five accounts were for FM employees created by the Resource Proprietor, but no access evidence of approval by their supervisors.

We suggest that FM should:

- Finish documenting and implement specific procedures on suspending, modifying and closing user accounts and related user privileges;

- Work with OIT to obtain access rule reports and perform periodic reviews of user accounts and related privileges; and

- Establish standardized access request forms for user provisioning and de-provisioning.

Management Action Plan

- FM will define user account and privilege lifecycle, encompassing all user account usage, not just FACserv.

- Establishment of standardized access request forms in FACserv, to be managed by FM.

- OIT will generate a report of user access and security groups in FACserv, accessible on demand, and reviewed by FM.

The estimated implementation date is December 2011.

11. Separation of Duties Review

Background

Effective separation of duties is designed to prevent the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner, in the normal course of business processes. Although separation of duties alone will not adequately assure that only authorized activities occur, inadequate separation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

Observation

Formal Review of Duties

Access to FACserv is assigned by group based on job duties. IAS review of FACserv found that 21 employees were assigned to multiple groups ranging from two to 10. While having individuals assigned to multiple groups may not be indicative of segregation of duties issue, there has not been a formal effort to identify incompatible tasks within these groups.

We suggest that FM should:

- Review all roles for conflict of duties;

- Remove conflicting roles for those individuals assigned multiple roles.

Management Action Plan

OIT will provide a report of user access and roles in FACserv. The report will be available on demand and managed by FM. FM will assign a FM employee to review roles and remove conflicting roles if found.

The estimated implementation date is December 2011.

12. <u>**Change Management**</u>

Background

Authorizations for system and application software modifications should be documented and maintained. Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing system changes; however, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective.

The use of standardized change request forms helps ensure that requests are clearly communicated and approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected.

Observation

Authorizations for system and application software modifications were generally followed for the FACserv system. However, we observed some areas that needed enhancement to strengthen internal controls and/or effect compliance with change management procedures in the areas of:

- Documenting all phases of change management tasks as required by procedures, for example, code reviews and test procedures;

- Maintaining separation of duties such that no single person can complete all phases of change management (i.e. code review, production approval, and production turnover); and

- Maintaining clear documentation of authorization or need for change from the application user.

Without adequate change management procedures, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.

Management Action Plan

- The change management process will be modified so documentation is consolidated and readily viewable.

- Separation of duties is currently being implemented for common skill set turnovers (Java code). FACserv requires a specialized skill set and the turnovers are manual, prohibiting the use of the QA team. Currently the turnovers are done by a different team member than the developer of the change, and will be enforced in the future.

- Requests for product changes and reports will be implemented in FACserv and managed by FM. It will provide the clear documentation and lifecycle of the request, including all needed approvals. This was implemented as of March 2011 but old requests have not yet been backfilled into FACserv.

The estimated implementation date is December 2011.

13. Risk Assessments and Security Plans

Background

IS-3 requires appropriate risk assessments or business impact analyses to be conducted periodically. The risk assessment and validation and related management approvals should be documented and maintained on file.

After completing a risk assessment, an information security plan should be developed that takes into consideration the acceptable level of risk for systems and processes. An application security plan serves as a roadmap during the entire security development and maintenance lifecycle of the application.

Observation

Risk Assessment

FM had not performed periodic risk assessments or business impact analysis of their systems including, FACserv as required by IS-3.

Without implemented risk assessment or business impact analysis, FM may not be able to:

- Determine the nature of their electronic information resources;

- Understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources; and

- Identify the level of security necessary for the protection of the resources.

Information Security Plans

FM should document security plans for their systems including FACserv as required and defined by IS-3.

The lack of a comprehensive, documented security plan increases the risk of inappropriate system access and compromised data confidentiality, integrity, and availability.

We suggest FM consider using the resources provided by OIT security to perform a risk assessment and develop a security plan.

Management Action Plan

- OIT currently provides comprehensive IT security to known FM applications. This is done in close collaboration with the OIT security, network, and DBA teams. OIT will provide FM with a review of the current mechanisms and policies in place.

- OIT is currently assessing security policies and risks associated with FACnet, file servers, and shadow systems of FM.

- OIT will provide a consolidated view of the security mechanisms in place for the FACserv system.

The estimated implementation date is December 2011.

14. **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.

Continuity plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

Observation

FM was in the process of documenting business continuity plans (UC Ready) during this review, including their IT systems. However, we noted enhancement was needed in the areas of disaster recovery planning. We suggest FM should document a disaster recovery plan that addresses items such as:

- List of hardware (servers, networks, etc.) necessary for the operation of FACserv;

- Specific restore instructions for each FACserv server. (hardware, network, OS, application, data);

- List of media necessary for the restoration of each system;

- Sequence that servers must be brought up in (if applicable);

- List of server connections that must be established, such as ODBC connections between applications and databases;

- Requirement for management review, approval and testing of the disaster recovery plan on a periodic basis;

- Requirements for documentation and reporting of test results to senior management; and

- Requirements to adjust any deficiencies identified during testing.

Management Action Plan

- Business continuity related items already exist, but need documentation to be consolidated and easily accessible.

- Complete UC Ready questionnaire to determine actual criticality of FACserv. The results of the questionnaire will dictate next steps.

The estimated implementation date is December 2011.

15. FACnet

Background

FACnet is a FM network physically separate from the UCI network that allows FM users to share resources and use key systems. The FM business continuity plan has identified the level of criticality of FACnet as 2. Critical level 2 is described as systems whose "failure will lead to imminent and very serious consequences". Examples of the FM groups that depend on key systems within FACnet include HVAC and Refrigeration, Fire and Lock, Building, Central Plant, and Energy and Utility Management among others. For the past several months, OIT has been working with FM to upgrade the FACnet infrastructure and take over support of the network.

Observation

FM has not documented implementation of control policies and procedures of FACnet systems and applications in the following areas:

- Security management;

- Access control;

- Segregation of duties;

- Configuration management; and

- Business continuity, disaster recovery planning.

Because of the overall criticality level of FACnet and interconnected systems, IAS recommends that OIT and FM consider providing additional resources to expedite implementation of appropriate controls and security measures of FACnet and the systems within it.

Management Action Plan

- OIT has performed a risk assessment of FACnet and has begun implementing some of the action plan for access control and security management.

- A FACnet committee has been created, composed of OIT and FM personnel, to begin driving the effort for addressing the current needs and directing the future of FACnet.

The estimated implementation date is December 2011.