UCIrvine | Internal Audit Services

Institute for Memory Impairments and Neurological Disorders (UCI MIND)

Internal Audit Report No. I2014-206

December 30, 2013

Prepared By
Helen Templin, Senior Auditor & Evans Owalla, IT Principal Auditor
Reviewed By
Julie Chung, Senior Auditor
Approved By
Mike Bathke, Interim Director

UNIVERSITY OF CALIFORNIA, IRVINE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

INTERNAL AUDIT SERVICES
IRVINE, CALIFORNIA 92697-3625

December 30, 2013

FRANK LAFERLA, PH.D.
DIRECTOR
INSTITUTE FOR MEMORY IMPAIRMENTS AND NEUROLOGICAL DISORDERS (UCI MIND)

RE: UCI MIND Audit
Report No. I2014-206

Internal Audit Services has completed the review of UCI MIND 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.

Mike Bathke

Mike Bathke
Interim Director
UC Irvine Internal Audit Services

Attachment

C: Audit Committee
Sinqui Musto, Assistant Vice Chancellor – Office of Research
Andrea Wasserman, Chief Administrative Officer – UCI MIND

I. MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2013-2014 audit plan, Internal Audit Services (IAS) reviewed business operations of the Institute for Memory Impairments and Neurological Disorders (UCI MIND). In general, internal controls and processes reviewed appear to be functioning as intended. However, certain internal controls could be improved to ensure compliance with University policies and procedures and/or best business practices. The following concerns were noted.

Non-payroll Expenditures – PayQuest transactions were sometimes incorrectly classified and consequently, required exceptional approvals or host certifications were not always obtained. This observation is discussed in section V.1.a.

Concerns were also noted with PALCard purchases. For some purchases, required PALCard documentation and/or other support documentation were not always retained. This observation is also discussed in section V.1.b.

Risk Assessment and Security Plan – Formal information security risk assessments for the information technology (IT) environment have not been completed. Also, a documented information security plan has not been completed. Performing periodic formal risk assessments, either on a regular basis or as part of an ongoing operational process, will help detect unidentified or unmanaged risks while a security plan helps lay out a path for addressing those risks. This observation is discussed in section V.2.

Access Control and Server Security – Some concerns were noted with one shared administrator account and a host-based firewall configuration for a web server. This observation is discussed in section V.3.

Collection, Management, and Analysis of Audit Logs – A formally documented process is not in place for the logging, aggregation, review, and retention of audit logs. Robust logging and monitoring functions enable the early detection and/or prevention of potential security issues. This observation is discussed in section V.4.

II. BACKGROUND

UCI MIND is an organized research unit "dedicated to investigating the causes of Alzheimer's disease and related dementias and to improving the quality of life and promoting successful aging." UCI MIND was established in 1995 and is one of 29 Alzheimer's disease centers (ADC) supported by the National Institute for Aging (a branch of the National Institutes of Health) and one of 10 California Alzheimer Disease Clinical Centers (CADC) funded by the California Department of Public Health.

Currently, UCI MIND has more than $22 million in restricted and unrestricted funds, including $18 million in grants to support clinical studies, research, and training programs.

The UCI MIND Director reports to the Vice Chancellor, Research. Administrative processes are managed by a Chief Administrative Officer (CAO) who reports to the Director. The CAO is assisted by a Chief Financial Officer (CFO). The CFO oversees financial operations and payroll.

III. PURPOSE, SCOPE AND OBJECTIVES

The scope of the audit focused on FY 2012-2013 UCI MIND business operations. The primary purpose of the audit was to assess whether the internal controls currently in place are adequate and sufficient to prevent or detect fraudulent or non-compliant transactions, while ensuring the overall efficiency and effectiveness of business operations. IT general controls were also reviewed.

Based on the assessed risks, the following audit objectives were established:

1. Reviewed non-payroll expenditures for proper accountability and separation of responsibilities, adequate documentation, assurance of valid, properly pre-authorized and approved transactions, timely reconciliations, and compliance with UC/UCI policies and procedures;

2. Determined whether the following aspects of employee time reporting: overtime approval, leave accrual tracking, and payroll reconciliation comply with established policies and procedures;

3. Evaluated whether there are adequate controls over budgeting and accounting and verified whether general ledgers are reviewed and reconciled in a timely manner;

4. Reviewed payroll certification processes for timely completion and submission;

5. Determined whether extramural fund expenses were appropriate, allocable, and reasonable, especially with subcontracts;

6. Evaluated whether there are adequate controls over the management of the "Brain Bank;"

7. Verified that inventorial equipment is properly tagged and monitored in accordance with UCI policies and procedures; and

8. Assessed and reviewed selected IT general controls.

IV. CONCLUSION

In general, internal controls and processes reviewed appear to be functioning as intended. No issues were noted related to the payroll/personnel processes, budget and accounting, extramural funds, the "Brain Bank," or equipment inventory. However, select internal control/compliance concerns were identified in the area of non-payroll expenditures, risk assessment and security plan, access control and server security, and collection, management and analysis of audit log data. In some of these specific areas, control measures may not always be optimal to prevent or detect fraudulent transactions.

Observation details 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. Non-Payroll Expenditures

A review was performed of PayQuest reimbursements and PALCard purchases in UCI MIND.

a. PayQuest Transactions

Background

The UCI PayQuest system is used to reimburse employees for expenses incurred while conducting University business. The documentation and purpose must be compliant with various policies. UC Business and Finance Bulletin G-28 discusses the policy and regulations that apply to all official University business travel and BUS-79 UC Expenditures for Business Meetings, Entertainment, and Other Occasions discusses the manner in which the University may provide hospitality. UCI's PayQuest guidelines contain documentation requirements for entertainment, travel, and other types of reimbursements. IAS reviewed a sample of PayQuest transactions to determine compliance with local and UC policies.

Observation

On a sample basis, IAS reviewed UCI MIND's FY 2012-13 PayQuest transactions. The following is the summary of the observations.

Travel Reimbursements

- A traveler was reimbursed for alcoholic beverages on a federal fund.

- There are numerous instances where travel dates listed have days before and/or after a conference. An explanation should be given to account for these days.

Other Reimbursements

- Of the transactions sampled, most were incorrectly classified. Because of the incorrect classification, these transactions lacked the necessary exceptional approval signatures and/or host certifications.

Lack of proper classification and subsequent lack of approvals and certifications of PayQuest reimbursements increases the risk of improper costs or unauthorized use of University funds.

Management Action Plan

1. To ensure compliance, effective immediately UCI MIND distributed an updated checklist to reiterate allowable and unallowable travel reimbursement expenses. Alcoholic beverages are listed as an unallowable travel expense.

2. Effective immediately, for UCI MIND staff, we will require a signed note from the employee and the employee's supervisor approving any personal/vacation days taken prior to or following a conference/meeting to account for extra travel days. This documentation will be used to ensure that the proper personal/vacation time is recorded on the employee's timesheet.

3. The PayQuest preparer has been retrained on how to classify transactions to the correct category to ensure that the proper approval signature is obtained. The UCI MIND CFO will follow up to ensure compliance and to provide additional training as necessary.

IAS will follow up on this management action plan in March 2014.

b. PALCard Transactions

Background

The UCI PALCard is used by University employees who are authorized to purchase low value supplies and services. Purchasing policies and procedures require that all purchases must be documented and reviewed.

IAS reviewed a sample of PALCard transactions to determine compliance with local and UC policies.

Observation

On a sample basis, IAS reviewed UCI MIND's FY 2012-13 PALCard transactions. The following is a summary of the observations.

- Approximately half of the applicable PALCard transactions reviewed did not have packing slips included with the supporting documentation. This weakens the control that the items ordered were actually received and at the proper location.

- Two of the PALCard transactions reviewed were for FedEx. These transactions had no supporting documentation submitted with the journal.

Proper pre-authorization, review, approval, documentation, and timely submission for PALCard purchases reduce the risk of improper costs or unauthorized use of University funds.

Management Action Plan

1. UCI MIND will communicate with all principal investigators and lab personnel regarding the importance of collecting and turning in all packing slips to the business office within three business days of receiving packages. In the event that a packing slip is unavailable, the business office will make every effort to provide the recipient lab an invoice corresponding to the delivery. The invoice will be used to document the receipt of the delivered items, will be initialed by lab personnel, and will be used in lieu of a packing slip.

2. Effective October 2013, UCI MIND will download the monthly FedEx statement and will use this information as supporting documentation to verify all FedEx transactions.

IAS will follow up on this management action plan in March 2014.

2. Risk Assessment and Security

Background

UC Electronic Information Security policy, IS-3, requires that a risk assessment be formally documented to identify vulnerabilities and threats to departmental informational resources, as well as major enterprise systems. Risk assessments should take into account and prioritize potential adverse impact on the University's reputation, operations, and assets. In addition, it should be conducted by units or departments on a periodic basis by teams composed of appropriate campus administrators, managers, faculty, and IT and other personnel associated with the activities subject to the assessment. Additionally, IS-3 requires that an information security plan should be developed that takes into consideration the acceptable level of risk for systems and processes.

Observation

UCI MIND IT performs informal ad-hoc risk assessments; however, formal information security risk assessments for the UCI MIND IT environment have not been completed. Also, a documented information security plan based on a risk assessment has not been completed.

Performing periodic formal risk assessments, either on a regular basis or as part of an ongoing operational process, will help detect unidentified or unmanaged risk to UCI MIND informational resources. In addition, a security plan helps lay out a path for addressing identified risks and also describes the controls that are in place or planned to ensure an acceptable level of risk for systems, processes or the IT environment.

Management Action Plan

UCI MIND IT will open a dialogue with the Office of Information Technology (OIT) security team and use their Security Risk Assessment Questionnaire (SRAQ) tool to identify vulnerabilities. The anticipated completion date is by the end of March 2014. UCI MIND IT will complete and document actionable items from the risk assessment as a basis to

develop an information security plan. The expected completion date is May 2014.

3. Access Control and Server Security

Background

IS-3 requires that procedures for providing individual authenticated access to resources are performed such that only authorized individuals are granted access. It also indicates that when readily available for specific operating systems, a host-based firewall shall be running and appropriately configured to limit access to systems that host restricted or essential resources.

Observation

IAS discussions and inspection of documents noted some concerns with one shared administrator account and the host-based firewall configuration for a web server as outlined below.

- The domain administrators were sharing the same administrative account; however, UCI MIND IT resolved this issue by creating individual administrative accounts.

- IAS ran Microsoft Baseline Security Analyzer (MBSA) on a sampled UCI MIND file and web server, and noted that the Windows host-based firewall on the file server was disabled. This configuration was enabled during the review.

The use of generic administrative accounts could increase the risk of improper use of the account or unauthorized operations and also create accountability issues. Host-based firewalls can block network traffic that is not explicitly allowed and thus protect the system from being exploited.

Management Action Plan

UCI MIND IT created unique individual accounts for each of the two system administrators during the review. Also, UCI MIND IT enabled the host-

based firewall during the review. UCI MIND IT will also implement procedures to run security configuration tools periodically, e.g., MBSA, Nessus vulnerability scanner, etc., on current and each new Windows server instance that is initialized. No further action is required for this observation.

4. Collection, Management and Analysis of Audit Logs

Background

IS-3 requires the implementation of audit logging policies defining the use, review, and retention of audit logs. Audit logs can capture detailed information that aids in the enhancement of security, system performance, and resource management. Audit logs should be managed in a manner that facilitates these benefits while protecting the confidentiality and integrity of the information contained in these logs.

Observation

Inspection of the UCI MIND audit logs for a sampled server indicated that logs are enabled to capture events such as logon/off, failed logon, and access attempts among others. However, IAS noted opportunities for improvement of the log management practice in the following areas:

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

- There is no central audit log management and logs are stored only on the individual systems generating the data. The server event logs are overwritten once the 205 megabytes limit has been reached, beginning with the oldest events.

Robust logging and monitoring functions enable the early detection and/or prevention of potential security issues. Additionally, audit logs can aid with the subsequent inspection of unusual and/or abnormal activities that may need to be addressed.

Management Action Plan

UC MIND IT will review, document, and adjust log management practices where feasible to align with the IS-3 guidelines (i.e., logging, aggregation, review, and retention of audit logs). In addition, UC MIND IT will consider implementing a log management solution, contingent on available budget, to provide automated monitoring and alerts for the most sensitive logs. The process of looking at feasible log management systems will commence at the beginning of the year 2014. The estimated implementation date is May 2014.