

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

**WILLED BODY PROGRAM  
Report No. I2013-203**

**January 10, 2013**

Prepared by:

Evans Owalla  
IT Principal Auditor

Helen Templin  
Senior Auditor

Reviewed by:

Gregory Moore  
Health Sciences Audit Manager

Bent Nielsen  
Director

January 10, 2013

**MARK BROOKS  
PROGRAM DIRECTOR  
WILLED BODY PROGRAM**

**RE: Willed Body Program Audit  
Report No. I2013-203**

Internal Audit Services has completed the review of the Willed Body Program 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  
Director  
UC Irvine Internal Audit Services

Attachment

C: Audit Committee

Greg Ackerman, Director of Technology, Health Affairs Information Services Administration  
Ralph Clayman, Professor and Dean of the School of Medicine  
Jim Murry, Chief Information Officer, Health Affairs Information Services Administration  
Brandi Schmitt, Director, Anatomical Services

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

**I. MANAGEMENT SUMMARY**

In accordance with the fiscal year (FY) 2012-2013 audit plan, Internal Audit Services (IAS) reviewed the adequacy of internal controls, policies and procedures of the business and information security (IS) processes in the UC Irvine Health Willed Body Program. Based on the audit work performed, opportunities for improving and strengthening internal controls were identified. Specifically, the following issues were noted.

**Risk Assessment and Security Plan** – The Digital Donor Library (DDL) System did not have a documented risk assessment and a security plan to ensure compliance with The UC Business and Finance Bulletin, Electronic Information Security (IS-3) requirements. Details are discussed in section V.1.

**Log Data Management** – A formal process was not in place to document the DDL history of activity logs review. In addition, there is no solution to easily retrieve or present the activity logs for review by management. Also, DDL server logs are reviewed periodically; however, documentation of the log review is not maintained. Details are discussed in section V.2.

**Separation of Duties** – A review of the DDL user roles and permissions determined that some users have unrestricted access to change and/or update all screens in the DDL application. Details are discussed in section V.3.

**Contingency Plan** –A comprehensive contingency plan had not been documented to ensure business continuity and disaster recovery for the DDL systems. However, regular DDL system backups are performed and sent to an offsite storage location. Details are discussed in section V.4.

**DDL System Management Reports** – Currently the DDL has limited system management reports available to the Willed Body Program users to effectively manage and monitor program activities. Details are discussed in section V.5.

**Outside Bank Account** – An authorized signer on the Willed Body Program checking account is no longer with the UC Irvine Health School of Medicine (SOM) and needs to be removed from the account. In addition, a new signer needs to be added to ensure adequate controls over the account. Details are discussed in section V.6.

**Non-Payroll Expenditures** – Not all supporting documentation for PayQuest, travel, and PALCard reimbursements/transactions were maintained on file as required by policy. Details are discussed in section V.7.

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

**II. BACKGROUND**

The Willed Body Program was established within the SOM. The primary purpose of this program is to serve as the central repository for the procurement, processing, systematic tracking, use, storage, and final disposition of anatomical materials used for the research, experimentation, and educational needs of the University. The Willed Body Program obtains these anatomical materials through donations. In addition, UC Irvine Health houses and maintains the server and program application for the systemwide Willed Body Program.

The program is managed by the SOM Dean's office and currently consists of three full-time employees (Program Director, Associate Director, and Administrative Analyst). The program is also supported on a part-time basis by the SOM Finance Operations Manager and the SOM Payroll Manager. The Program Director has a dual reporting relationship to the SOM Dean and the UC Systemwide Anatomical Services Director.

Oversight and advice to the program is provided by the Anatomical Materials Review Committee (AMRC) and the Anatomical Advisory Board (AAB). The AMRC is a management team with operational expertise who are responsible for reviewing and recommending action on requests for use of anatomical materials. The Assistant Dean of the SOM is the Responsible Executive Officer (REO) and is a member of this committee that provides management oversight of the Willed Body Program. The AMRC meets monthly or at least ten times per year. The AAB also consists of the REO and individuals representing the faculty, staff, and other users of anatomical materials. The AAB provides broad input from the community by advising the campus on policy and making recommendations regarding program activities. The SOM Dean serves as chair of the AAB and appoints the members of this committee. The AAB meets at least annually or as necessary.

**III. PURPOSE, SCOPE AND OBJECTIVES**

The purpose of this audit was to review the internal controls of the business and IS processes in the Willed Body Program for the FY 2011-2012. Specifically, the operational review focused on the areas of billing and revenue collection for willed body services, expenses, inventory controls, and tracking of anatomical material used in research. The information technology (IT) review focused on determining whether the DDL system IS controls were adequate to protect the confidentiality, integrity, and availability of the information and system.

The objectives of our review were as follows:

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

1. Verify that non-payroll expenditures are properly authorized and are processed in accordance with University policies and procedures;
2. Determine whether adequate controls are in place to ensure Willed Body Program services are billed, revenue is collected, and recorded in the general ledger in accordance with University policies and procedures;
3. Evaluate whether there are adequate controls over budgeting and accounting and verify whether general ledgers are reviewed and reconciled in a timely manner;
4. Evaluate controls related to inventory acquisition, preparation, management, tracking, and disposal of anatomical material;
5. Verify that inventorial equipment is properly tagged and monitored in accordance with UC Irvine policies and procedures;
6. Determine whether adequate system and application level general controls were implemented in areas of security management, access control, configuration management, separation of duties, and contingency planning; and
7. Evaluate whether adequate application business controls are in place in the areas of data input, processing, and output.

**IV. CONCLUSION**

In general, the Willed Body Program's internal controls are operating effectively in the areas of equipment inventory, budgeting and accounting, anatomical material inventory acquisition, preparation, tracking, and disposal. However, business risks and control concerns were identified in the areas of risk assessment and security plan, log data management, separation of duties, contingency plan, DDL management reports, outside bank account, and non-payroll expenditures.

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

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

**V. OBSERVATIONS AND MANAGEMENT ACTION PLANS**

**1. Risk Assessment and Security Plan**

**Background**

IS-3 requires appropriate risk assessments or business impact analyses to be conducted to understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources, and to identify the level of security necessary for the protection of the resources. The policy states that after a risk assessment is completed, an IS plan should be developed that takes into consideration the acceptable level of risk for systems and processes.

**Observation**

The DDL system does not have a documented risk assessment although system security vulnerability assessments of the DDL servers are performed periodically using scanning tools to identify potential vulnerabilities that could be exploited. In addition, the DDL system does not have a documented security plan. A system security plan provides an overview of the systems' security requirements and describes the controls that are in place or planned to meet those requirements. Without complete and periodic formal risk assessments, either on a regular basis or as part of an ongoing operational process, there may be unidentified or unmanaged risk to the DDL data. Also, a security plan is required to provide assurance that controls are effectively implemented.

**Management Action Plan**

DDL risk assessments are regularly performed on the servers and application. A new risk assessment process for the department has formalized the documentation procedure. A newly updated risk assessment was completed on October 1, 2012 and documents have been placed onto the Data Security portal on the departments SharePoint site. An updated DDL security plan is in progress and completion is expected by July 1, 2013.

**2. Log Data Management**

**Background**

IS-3 requires that each campus develop a log management infrastructure. Audit logs can capture detailed information that aids in the enhancement of security, system performance, and resource management. Audit logs should be managed in

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

a manner that facilitates these benefits while protecting the confidentiality and integrity of the information contained in these logs.

**Observation**

The DDL application has the capability to track the history of activities, for example, changes and updates of DDL data within the application itself. In addition, the DDL servers (application and SQL hosts) log system events such as security audit logs that could provide insight on policy violations, internal threats, and regulatory compliance. However, the following opportunities to improve DDL application logs and server event logs were noted:

DDL Application

- A formal process is not in place for the review of the DDL history of activities ('logs'). The Willled Body Program Systemwide Director stated that the 'logs' are reviewed as needed. In addition, no evidence of DDL activity log review is currently maintained.
- DDL 'logs' are maintained within the application itself, but there is no solution to easily retrieve or present the logs for review by management.

DDL Server

- The server logs are overwritten locally instead of being archived in accordance with IS-3 log retention guidelines. Also, management stated that server logs are reviewed on a periodic basis, but the process has not been documented and evidence of log review is currently not maintained.

Without comprehensive logging and monitoring functions for the DDL systems, Health Affairs Information Services (HAIS) may not be able to promptly detect and/or prevent and timely report security and/or non-compliance activities that may need to be addressed.

**Management Action Plan**

The log files for our Virtual Private Network (VPN) and applications servers are reviewed on a regular basis, however, a documented process and findings report does not exist. A new syslog server has been created to store the logs from the servers. The logs from the servers (application and SQL hosts) will be sent and stored on the syslog server before they are overwritten locally. The log file review is performed at least monthly and findings are reviewed during data security team meetings, which include the security officer for the campus. Any action items that come out of the review are logged into the HAIS help desk

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

system for remediation or corrective action. The new process for log file storage and review will begin January 2013. The DDL Application activities are logged in the SQL database and a new function within the application will be created to review the historical activities. The goal is to complete this function by June 2013.

**3. Separation of Duties**

**Observation**

A review of user roles and permissions limited to the Willed Body Program personnel and the Systemwide Director noted that some users have full access to change/update all screens in the DDL which may present risks associated with lack of separation of duties. For example, some users have permissions to initiate, modify, and then approve their own entries. While the DDL application maintains a detailed history of user activities such as entries, changes and updates to data, management should still consider separating these incompatible duties. Adequate separation of duties can prevent or detect errors and irregularities by ensuring that no one individual controls all critical stages of a work flow process.

**Management Action Plan**

Staffing levels in the UC Anatomical Materials Programs do not allow for single role assignments. We will undertake a review and re-assignment process to redistribute permissions that will reduce or eliminate full access wherever possible by July 1, 2013.

**4. Contingency Plan**

**Background**

Contingency planning measures is a critical component of information protection. It protects information resources and minimizes the risk of unplanned interruptions and provides for recovery of critical operations should interruptions occur. Contingency plans detail emergency response measures, backup operations, and disaster recovery for information systems. To mitigate service disruptions, these plans should be clearly documented, communicated to potentially affected staff, updated to reflect current operations, and periodically tested.

**Observation**

There is no documented contingency plan for the DDL system. However, DDL system backups are created on a daily basis and sent to an offsite storage location.



**WILLED BODY PROGRAM**  
**Report No. I2013-203**

Without comprehensive business continuity and disaster recovery plans for the DDL system, the UC is at risk of loss of critical services and data relied on for academic and administrative operations for an unacceptable duration.

**Management Action Plan**

A contingency plan is being created for DDL currently and is expected to be completed by February 1, 2013. We will operate under the draft contingency plan until approved by the Office of the President (UCOP).

**5. DDL Management Reports**

**Observation**

The DDL application needs improvement on standard and useful management reports. For example, DDL users cannot generate reports of the case summary, specimen summary, or inventory by storage location in a logical order directly from the DDL and have to use the print screen function and paste to WordPad to obtain these reports. The absence of meaningful reports and printing capabilities has led to the use of other external documents, for instance the use of Microsoft Word and Excel to track outside specimen allocation. DDL's lack of standardized reports and printing limitations could limit management's effort to track sensitive Willed Body Program material and review operation activities.

**Management Action Plan**

Willed Body Program management is aware of this limitation. The DDL is a new application and certain features have been prioritized ahead of reporting capabilities. We are currently engaged in a discovery process to determine a reporting solution within the DDL. Through the discovery process we will determine a plausible implementation date timeline. However, until the discovery process has been completed an expected date of implementation is set for July 2013. In the interim, a secure web accessible reporting mechanism has been provided to staff members, which allows access to systemwide approved reports including the Inventory by Location, Available Specimens, and Vital Statistics reports. We will re-educate staff regarding the approved systemwide reports and discourage them from creating shadow reports in another application.

**6. Outside Bank Account**

**Background**

The Willed Body Program has the responsibility for arranging transportation of the deceased donor and obtaining death certificates and other legal documents to

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

comply with federal and state regulations and University policy. These activities require the Willed Body Program personnel to work with county health services and/or county coroner's offices. These entities require payment on demand and in most cases will only accept cash and/or check payments for their services. As a result, the Willed Body Program established an outside bank account in order to accommodate the payment for these services. The Systemwide Director of Anatomical Services stated that utilizing an outside bank account is a common business practice for willed body programs.

According to the UC Irvine Accounts Payable Supervisor, reimbursements are normally made "after the fact" by using invoices or receipts collected by the payee to justify payment. Since invoices or receipts would not be available prior to the transaction of the services, these transactions would then be defined as cash advances. Due to the frequency of these requests, a petty cash checking account was determined by UC Irvine Accounts Payable to be the best method in handling these payments.

**Observation**

IAS reviewed a sample of the activity in the outside bank account and matched the disbursements from the account supporting documentation to the requests for replenishing the account through the PayQuest process and found no exceptions. However, through a review of the authorized signers and the reconciliation process of the bank account, IAS determined the following.

- A. The authorized signers on the account are the Willed Body Program Director, the Willed Body Program Analyst, and the former Finance Operations Manager for the SOM Dean's Office. However, this Finance Operations Manager, who is no longer with the SOM, had not been removed from the signatory list on the account.
- B. The former Finance Operations Manager was the individual responsible for the monthly reconciliation of the bank statement. Currently, the Willed Body Program Analyst is now responsible for the use, monitoring, reconciliation, and replenishment of the account.

To maintain an adequate internal control structure and separation of duties, the former Finance Operations Manager's name needs to be removed and another person, preferably from the SOM Finance department, should be added to the account. That person should conduct the monthly reconciliation of the bank account to remove that process from the Willed Body Program Analyst.

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

**Management Action Plan**

The Willed Body Program Director has removed the prior Finance Operations Manager from the signatory authorization list. The Director will add the Senior Finance Analyst (currently recruiting), in January 2013. Additionally the individual will reconcile the bank statement along with the current monthly reconciliation of Willed Body Program revenue and expense account/funds.

**7. Non-Payroll Expenditures**

**Background**

UC Irvine PayQuest is used to reimburse others for expenses incurred during University business. The documentation and purpose must be compliant with various policies.

**Observation**

**A. PayQuest Reimbursements**

IAS sampled 26 PayQuest reimbursements for appropriateness and compliance with policy. The following is the summary of the observations:

1. Seven of the 26 (27 percent) PayQuest transactions reviewed for employee reimbursements for supplies did not have any purchase requisitions attached. A purchase requisition should state the actual business purpose of the expense and show each item requested for purchase. This will allow the account approver the ability to verify a purchase for appropriateness before reimbursing funds; and
2. One of the PayQuest transactions reviewed was for a reimbursement of registration fees. Since there was travel associated with this registration fee, it should have been claimed through the travel voucher procedures.

**B. Travel Documentation**

IAS sampled ten travel vouchers for appropriateness and compliance with policy. The following is the summary of the observations:

1. None of the ten travel vouchers sampled contained any documentation for travel authorization prior to travel;
2. There were two instances of multiple travel vouchers claiming expenses for a single trip; and

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

3. Three of the ten (30 percent) travel vouchers sampled had either missing or incomplete supporting documentation. This includes the lack of an agenda or other notes that would more clearly explain and support the business purpose or event.

Proper review, documentation, and compliance with local and UC policies for travel reimbursements reduces the risk of improper costs or unauthorized use of University funds.

C. PALCard Transactions

IAS sampled five PALCard transactions for appropriateness and compliance with policy. Three of the five (60 percent) PALCard transactions reviewed did not have packing slips included in the supporting documentation packet. Packing slips provide proof of delivery. Lack of this documentation weakens the control that the items ordered were actually received at the proper place.

Proper documentation for PALCard transactions reduces the risk of inappropriate expenses or unauthorized use of University funds.

**Management Corrective Action**

PayQuest Reimbursements

- Willed Body Program employees will comply with policy by submitting an approved purchase requisition, including the business purpose of purchase(s) for future reimbursements. The process was discussed with Willed Body Program personnel.
- Registration fees that have other travel related expenses will be processed together on one travel voucher. We have discussed this with Willed Body Program personnel and will adhere to policy.

IAS has verified with SOM Finance that this corrective action has been implemented.

Travel Documentation

Management has provided copies of UC Irvine Policy and Procedures Section 715-01 and UC Travel Policy G-28 to staff, as well as implementing new business practices and procedures to ensure compliance, as follows.

**WILLED BODY PROGRAM**  
**Report No. I2013-203**

- Future travel authorizations will either be documented in the “travel notes section” that travel was approved by authorized personnel with date or by an attached email providing approval.
- Willed Body Program management discussed the necessity of preparing and processing all business related travel expenses on one travel voucher; multiple vouchers for the same trip is not acceptable and is not within campus and UC policies.
- Willed Body Program management discussed the importance of providing a business meeting agenda or other documentation that will clearly support the business purpose of the event when submitting travel reimbursements.

IAS has verified with SOM Finance that this corrective action has been implemented.

PALCard Transactions

- Most PALCard purchases that are made have appropriate documentation and packing slips. Due to the different locations of the Willed Body Program and delivery of purchases, packing slips were not received. Packing slips are now received and attached to PALCard documentation to complete the transaction.
- There was one incident when a vendor split the purchase into two shipments, therefore creating two invoices for one purchase. If this occurs again, we will document detail notes of such on the appropriate forms.

IAS has verified with SOM Finance that this corrective action has been implemented.