UCIrvine | Internal Audit Services

School of Biological Sciences

Internal Audit Report No. I2014-109

November 20, 2013

Prepared By
Julie Chung, Senior Auditor & Evans Owalla, IT Principal Auditor
Reviewed By
Helen Templin, 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

November 20, 2013

BRANDON S. GAUT, PH.D.
INTERIM DEAN
SCHOOL OF BIOLOGICAL SCIENCES

RE: School of Biological Sciences Audit
Report No. I2014-109

Internal Audit Services has completed the review of the School of Biological Sciences and the final report is attached.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. If you have any questions or require additional assistance, please do not hesitate to contact me.

Mike Bathke
Interim Director
UC Irvine Internal Audit Services

Attachment

C: Audit Committee
Albert Bennett, Dean Emeritus
Benedicte Shipley, Assistant Dean
Yuanshun Chen, Finance Director

I. MANAGEMENT SUMMARY

In accordance with the fiscal year 2013-2014 audit plan, Internal Audit Services (IAS) reviewed the business operations, internal controls, and policy compliance for the School of Biological Sciences (SBS) at the University of California, Irvine (UCI). 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.

Cash Handling – Cash collection and depositing processes are not adequately separated. Improvement is also needed in safety measures for UC Irvine employees transporting cash/equivalents. Furthermore, a receipt is not always completed and/or retained for each collection. In addition, employees with cash-handling responsibilities are not receiving required training. The details related to these issues are provided in section V.1.

Non-payroll Expenditures – Concerns were noted with PALCard purchases. Pre-authorizations were not always obtained for purchases and PALCard dollar limits were occasionally exceeded. For some purchases, required PALCard documentation and/or other support documentation were not always retained. In addition, adequate descriptions of purchased items and/or the business purpose for purchases were not always provided. This observation is discussed in section V.2a.

Concerns were also noted with PayQuest reimbursements. Official University travel was not properly authorized, reported, or reimbursed in accordance with G-28. Travel expenditures were sometimes improperly/incorrectly reimbursed, or the required exceptional approvals were not obtained, and reimbursements were sometimes requested for purchased goods/services that should have been acquired with a PALCard. This observation is discussed in section V.2b.

Payroll–Overtime – Internal controls were not established to ensure that overtime for staff was accurate and valid. Prior approvals for overtime were not documented or reviewed to verify that reported overtime was correct prior to payment. These observations are discussed in section V.3.

Human Resources – Some individuals reviewed had not completed background checks. Also, some necessary records were not maintained as required per policy. In addition, written performance evaluations were not completed on an annual basis for all staff employees, and the performance evaluation code was not entered into the Payroll Personnel System (PPS). These observations are discussed in section V.4.

Risk Assessment and Security Plan – SBS Computing performs informal ad-hoc information security risk assessments; however, formal information security risk assessments specifically for the Biological Sciences IT environment have not been completed on a regular basis. In addition, a documented information security plan has not been completed. These observations are discussed in section V.5.

Access Control – A review of the Biological Sciences domain controller[1] group policy indicated that account policies and password policies need to be strengthened. Also, some opportunities for improvement were noted in managing user access and accounts. These observations are discussed in section V.6.

Management and Analysis of Log Data – Opportunities for improvement noted include implementing a formally documented process for log management practice. These observations are discussed in section V.7.

Faculty Computing Assessment – Most faculty members in SBS host their own data and maintain their own endpoint devices (e.g. servers, desktops, laptops etc.). Consequently, some of the key concerns noted are the risk of data loss, inventory and classification, and systems and application security. These observations are discussed in section V.8.

II. BACKGROUND

SBS is comprised of four departments focused in the following areas of biological research and education: Developmental & Cell Biology, Ecology & Evolutionary Biology, Molecular Biology & Biochemistry, and Neurobiology & Behavior.

[1] The domain controller is a server that responds to security and authentication requests within a Windows Server domain.

All of these programs are ranked in the top 20 percent or higher of national institutions according to National Research Council data. Each department has a comprehensive series of core courses for undergraduates that reflect the ever-expanding and developing field of biological sciences.

SBS also collaborates with many other units on campus to help further research in important fields. The research centers and institutes that have significant participation from SBS faculty are school centers, campus organized research units, system-wide centers, and state-wide centers.

III. PURPOSE, SCOPE, AND OBJECTIVES

The scope of the audit focused on fiscal year 2012-2013 SBS 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.

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

1. Reviewed cash handling processes for conformance with UC/UCI policies and procedures and for assurance that collected funds are properly recorded, secured, reconciled, and deposited;

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

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

4. Verified whether the required general, confidential, payroll, and medical documents are properly maintained and filed in personnel records;

5. Assessed and reviewed selected information technology (IT) general controls.

IV. CONCLUSION

In general, internal controls and processes reviewed appear to be functioning as intended. However, select internal control/compliance concerns were identified in the areas of cash collection and depositing, non-payroll expenditures, overtime compensation, human resources, risk assessment and security plan, access control, collection, management and analysis of log data, and faculty computing.

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. Cash Handling

Background

Business and Finance Bulletin 49 (BUS – 49) establishes the University's policies related to handling and processing of cash and cash equivalents, and defines roles and responsibilities related to receipt, safeguarding, reporting and recordkeeping for all University cash and cash equivalents. Its purpose is to ensure that University assets are protected, accurately and timely processed, and properly reported. The bulletin also establishes basic internal control principles (accountability, separation of duties, security, and reconciliation) in regards to collecting and accounting for cash and cash equivalents.

Observation

Three units in SBS (ImageWorks, Copy Center, and the Arboretum) were selected for review to determine if each unit complied with the established policies and procedures. The following is a summary of the observations.

a) Deposits

In two units, collections were not deposited either in a timely manner weekly, or when collections exceed $500 as required by policy. IAS noted instances when thousands of dollars were collected and accumulated for one month and then deposited. For example, in one unit, IAS noted that on April 26, 2013, almost $5,000 was deposited, which included a total of 50 checks and money orders dated March 22, 2013 through April 24, 2013. In the following month, on May 30, 2013, over $4,000 was deposited, which included 42 checks and money orders dated April 24, 2013 through May 20, 2013. In another unit, 18 checks (totaling $765), some dating back to August 2007, had not been deposited.

IAS also noted that checks were not restrictively endorsed immediately upon receipt, but at month end and/or during preparation for deposit. Also, deposits were not validated and prepared in dual custody, and deposits in one unit lacked appropriate supporting documentation, such as invoices, receipts, or tickets, or the cash collections did not correspond to the expected revenue from the sale of admissions and no explanation was noted for the variances. Only verbal justifications, such as discounts to some donors or free admission for high donors, were given to explain the variances in the collection of Arboretum admissions.

In addition, cash deposits were not transported securely by employees in dual custody in compliance with policy.

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

b) Separation of Duties

Internal control procedure that ensures an adequate separation of duties was not always maintained. For example, an individual who reconciled the deposits to the general ledger also prepared deposit advice forms and transported cash to the Cashier's Office for deposit. Also, one supervisor who accepted checks from customers also prepared deposits.

BUS-49 states that the business unit head is responsible for establishing procedures that ensure that no single individual is responsible for the collection, handling, depositing and accounting for cash received by that unit. At least two qualified individuals must be assigned to carry out key duties of the cash handling process. Failure to maintain adequate separation of duties over cash related functions may result in the diversion of University funds.

c) Securing Collections

In two units, checks were not securely stored but kept in a plastic basket which was placed on a countertop. Two weeks prior to IAS review, a lockable receptacle was purchased, but it had not yet been installed for use. In addition, the cash and checks collected in the third unit reviewed were also not maintained in a secure manner. An appropriate safe as stated in the policy was not used to store cash and checks overnight.

d) Receipts/Invoices

In two units, invoices were maintained and given to customers as required by policy. However, reviews were not performed to verify that there were no missing/lost/stolen invoices and that all invoices were accounted for sequentially. In the third unit, receipts or invoices were not given to customers nor were tickets given to customers for admission as required by policy.

e) Change Fund Verification

In one unit, unannounced cash count and verification of the change fund ($100) for which cash handling employees are accountable was not performed and documented. Unannounced cash count and verification are required on a periodic basis, at least quarterly, by someone other than the fund custodian to

comply with the policy. When the unit supervisor went on leave, her supervisor found over $300 in the change fund.

f) Voids/Refunds

Transactions that were voided were not explained and documented. In addition, voided transactions were not adequately reviewed or approved in writing by the supervisor as required by policy.

University policy requires that voids and refunds to be fully documented and explained as well as approved in writing by the supervisor. Inadequate management of voided and refunded transactions increases the risks of fraudulent transactions being processed subjecting the University to unnecessary financial loss.

g) Background Checks

As far back as February 2004, background checks were not performed prior to employing cash handlers and individuals in other critical positions.

Management Action Plan

Managers of units that collect cash and cash equivalents will review BUS-49, establish procedures and internal controls to comply with the policy by December 2013, and train current and new employees accordingly. To comply with the policy, steps will be taken to ensure that sequentially numbered receipts/invoices are provided to customers and used internally to support deposits, checks are endorsed immediately, funds are secured in an appropriate locked receptacle, funds collected are deposited before the established maximum limits are reached, deposit amounts are validated in dual custody, appropriate separation of duties is established (where no single person is responsible for the collection, handling, depositing, and accounting for funds), change funds will be verified periodically, all voids/refunds are documented and approved, and all employees involved in the cash handling process are required to complete a background check.

Also, students and staff have completed and received a clear background check. The Arboretum is no longer in the plant sale business, and an Advisory Ad Hoc Committee has been established to give recommendations

regarding operations and directions for the Arboretum. If it is decided that the Arboretum should be in the plant sale business in the future, we will establish cash collecting and cash equivalent procedures that comply with policy BUS-49.

2. Non-Payroll Expenditures

A review was performed of PALCard purchases and PayQuest reimbursements in the SBS academic departments and other units.

a. PALCard Transactions

Background

The UCI purchasing card (PALCard) is used by faculty and staff members responsible for purchasing University equipment, supplies and services. UC purchasing policies require purchases to be pre-authorized either formally through an internal requisition or informally, such as an email. In addition, UCI PALCard policies require an administrative reviewer to review PALCard supporting documentation and account/fund for appropriateness for each transaction in a timely manner.

Observation

IAS selected a sample of 64 PALCard transactions from July 1, 2012 through present for review, and noted the following:

- Internal requisitions were not properly approved or documented. Examples of the observations include the requestor/PALCard holder approved the purchase, the approver did not sign the internal requisition, the requisition was not completed prior to purchasing, or a requisition was not completed. In addition, the business purpose for the purchase was not documented to properly determine if the expense is allowable and allocable.

- PALCard holders made personal purchases; one in particular made personal purchases on four occasions. Another PALCard holder purchased a membership with her PALCard but also submitted and

received a PayQuest reimbursement for the same expense. However, it should be noted that the PALCard holders did pay back the University.

- One PALCard holder's spouse was the designated approver for purchases.

- Administrative reviews were not performed in a timely manner. It should also be noted that administrative reviewers approved some transactions although not all of the required supporting documentation was retained and/or filed as required by policy and necessary for proper review.

- Invoices were not maintained on file for review as appropriate supporting documentation.

- The proper tax amounts were not posted to the general ledger.

- Packing slips were not maintained on file for review as appropriate supporting documentation.

In addition, a few transactions exceeded the PALCard purchase limit (total order $5,000 or less, including tax and shipping), but an exceptional approval was not obtained prior to purchase as required by policy. Also, PALCard holders paid for transactions involving service agreements without proper review or approval of the agreements by Risk Management or the Office of Research.

Implementation of internal controls, such as obtaining authorized requisition prior to purchase, appropriate separation of duties, maintaining proper documentation, and timely administrative review, minimizes the risks of error, waste, and inappropriate or unauthorized use of University funds.

Management Action Plan

By March 1, 2014, policy requirements will be communicated to all PALCard holders, reviewers, and approvers to ensure compliance in acquiring prior approvals with the required signature and date, documenting business purpose, filing necessary supporting documentation, and properly reviewing transactions in a timely manner. In addition, the Dean's Office will follow-up with the specific departments and unit to ensure compliance with University

policies. If deemed necessary, additional training will be provided to individuals.

b. PayQuest Transactions

Background

UC Irvine employees utilize the PayQuest automated system to request reimbursement for various expenditures and certain other payments. Reimbursement requests pertaining to travel expenditures must comply with UC Business and Finance Bulletin G-28; expenditures for business meetings, entertainment, and other occasions must comply with UC Business and Finance Bulletin BUS-79. Reimbursement requests must also comply with all applicable UC Irvine policies.

Observation

IAS reviewed a select sample of PayQuest transactions in the Dean's Office, the academic departments, and one unit from July 1, 2012 to present for appropriateness and compliance with policy. The following is a summary of the observations:

Travel Reimbursements

- SBS does not have adequate controls in place to properly authorize and monitor travel for academic appointees. None of the travel reimbursements reviewed had been pre-authorized and the majority lacked leave of absence approvals as required by policy.

- University funds were utilized for personal travel expenses not related to official University business. IAS noted instances when academic appointees were reimbursed for personal travel related expenses before and/or after University business (i.e., conferences, symposiums, meetings, etc.)

- IAS noted instances when travelers were inaccurately reimbursed (actual amount paid or reimbursed differently than supporting documentation).

- Some travel reimbursements were not properly supported or justified. For example, documentation or justification was not provided for the following: not flying into the closest airport and renting cars to drive more than six hours to the conference site; not staying at the conference sites; a bona fide explanation for why their spouses accompanied the traveler; a letter of agreement with an outside agency for travel expenses; and personal days during their travel.

- The payee/traveler did not sign the reimbursement form certifying that the expenses claimed were incurred for University business.

Other Reimbursements

- Some reimbursements were not properly approved and/or lacked proper separation of duties. The department chairs' or dean's reimbursements were not approved by the dean or vice chancellor, respectively, as required per policy but instead by the payee's subordinate. Also, as a best business practice, the payee should not prepare and submit his own reimbursements.

- Some reimbursements requiring an exceptional approval were not obtained or documented on the claim. The observations include reimbursements to individuals for purchases that exceeded $500, reimbursing expenses from the prior fiscal year, missing receipts/invoices, exceeding the maximum lodging rates, and upgrades to flying economy class.

IAS also noted that several reimbursements to individuals (some are PALCard holders) were for purchases of computers, supplies, and equipment. In purchasing supplies or equipment, PALCard is the appropriate method of purchase. Lack of internal controls such as prior authorization for purchases increases the potential for errors/inaccuracies, waste, and fraud to go undetected.

Management Action Plan

By March 1, 2014, policy requirements will be communicated to all faculty and staff to ensure compliance in obtaining proper approvals for payments, obtaining exceptional approvals, requiring payee/traveler signatures, and

documenting business purpose and/or justification for expenses. In addition, the Dean's Office will follow-up with the specific departments and unit to ensure compliance with University policies. If deemed necessary, additional training will be provided to individuals. Also, all PayQuests reimbursements submitted to Accounting will be reviewed by the Dean's Office to ensure UC policy compliance. This new process will be implemented by March 1, 2014.

3. Payroll - Overtime

Background

Personnel policy on overtime for staff members requires the department head to approve overtime for non-exempt employees to meet essential operating needs. The department is responsible for ensuring an employee requested advance approval for overtime work and properly report the overtime worked in a timely manner prior to compensation.

Observation

IAS reviewed the payroll data for pay periods during fiscal year 2013 for staff in the academic departments. In the review, IAS identified nine staff members who reported working overtime and received either compensatory time off or overtime compensation.

Further review disclosed that the departments did not comply with the policy or have appropriate internal controls to ensure best business practices. The review found that some staff members did not request approval from their supervisors prior to working overtime as required by policy. It should also be noted that some staff members reported working overtime in error, and their supervisors mistakenly approved the time sheets when, in fact, no overtime was approved or actually worked.

In addition, IAS noted that the overtime approved in advance was given verbally. There were no written records substantiating that any overtime approvals were obtained in advance and necessary. Such documentation can verify proper reporting of actual overtime hours. Consequently, justification that overtime was necessary to meet essential operating needs was also not documented.

Compliance with the policies and procedures ensures that payroll is not only properly approved and processed in accordance with regulatory requirements, but also valid for compensation.

Management Action Plan

Effective immediately, the proper policies and procedures, including timely requests for overtime as well as appropriate approval and documentation, will be communicated to all faculty and staff. In addition, the Department Timesheet Administrator will review and verify that reported overtime is properly supported prior to compensation. The Dean's Office will be conducting training for the department timesheet administrators to go over the non-represented staff policies and the various union policies for overtime.

4. Human Resources

Background

UCI departments are responsible for ensuring compliance with personnel records management requirements. The requirements include that all required personnel documents are complete and placed into the four separate and distinct files: general employee, payroll, medical, and confidential or organized per Employee Records Online System Procedures (EROS).

UCI Administrative Policy Sec. 300-10 states that background checks be completed on critical positions.

UCI policy on performance appraisal states that the performance of each employee shall be appraised at least once during probation and thereafter annually in writing by the employee's immediate supervisor.

Observation

a) Background Checks

For nine of the 16 personnel records selected for review, a copy of the background check clearance email was not on file and maintained as required by policy. The email confirmation should be filed in the personnel confidential file to acknowledge background check clearance. Human

Resources reviewed their records and confirmed that a background check was not performed for four of the nine staff members. The review also disclosed that academic administration was not familiar with University policy which states that all employees, both limited and career, in positions deemed critical (handling or access to checks, controlled substances, or research animals) are required to clear a background check. Promptly obtaining cleared background checks on staff in critical positions will ensure that business risks are minimized within the department.

b) Performance Evaluations

Nine personnel records were selected for review and current performance evaluations for three staff members were not completed as required by policy. Failure to conduct performance evaluations may result in unimproved productivity and performance.

In addition, it should also be noted that photocopies of employees' California driver's license, permanent resident cards, employment authorization card, and passport were inappropriately filed in two of the personnel records reviewed.

Management Action Plan

Background Checks

The University personnel policy on background checks was communicated to the academic departments and the Office of the Dean Directors and will be communicated to the other units and programs within SBS as well. Background checks will be scheduled immediately for those identified staff members in positions deemed critical where Human Resources confirmed the employees had not completed a background check. Also, upon receiving the results of the background checks, copies will be placed in the personnel files as required by policy. The above actions will be completed by December 31, 2013.

Performance Evaluations

Annual reminders will be sent out to all departments and units to ensure that performance evaluations are completed and filed by an established deadline.

The Dean's Office will ensure that the performance ranking codes have been entered into the PPS system to track incomplete evaluations and conduct a follow-up to ensure all outstanding evaluations are completed by December 31, 2013. Also, personnel analysts will follow-up with supervisors of newly hired employees to make certain that at least one evaluation is completed during the probationary period.

In addition, personnel analysts will ensure photocopies of driver's license, passport, permanent resident card, etc. are properly purged and are not being placed in personnel files

5. Risk Assessment and Security Plan

Background

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 information technology 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

SBS Computing performs informal ad-hoc information security risk assessments; however, formal information security risk assessments specifically for the Biological Sciences Information Technology (IT) environment have not been completed on a regular basis. In addition, 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 risk to SBS informational resources. 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

SBS Computing will meet with the Office of Information Technology (OIT) security team on October 28, 2013 to start formalizing the documentation of the Biological Sciences IT environment security risk assessment and security plan by using the Security Risk Assessment Questionnaire (SRAQ). We will also document the policy for when and how the network file server is scanned for personal identifiers (social security numbers, credit cards, etc.) using Identity Finder and develop a strategy to scan desktop computers and servers for vulnerability issues using OIT's vulnerability service. Target date for completion is March 2014.

6. Access Control

Background

According to IS-3, password management should include periodic identification of weak passwords, password encryption, and other security measures as deemed appropriate. Also, administrative and technical controls should be in place to authorize access to only those persons who have a legitimate business purpose to access specific resources ("Authorized Individuals"), modify access as appropriate, revoke access upon termination or when job duties no longer require a legitimate business reason for access.

Observation

A review of the Biological Sciences domain controller group policy indicated that account policies and password policies need to be strengthened. For instance, minimum password length is set below the current recommended UC Irvine campus (UCInetID) password requirement and password complexity/strength is not enabled.

SBS Computing has documented specific technical procedures for creating and deleting user accounts on their domain[2]. Also, regular process for reviewing Windows Active Directory accounts has been implemented. However, opportunities for improvement were noted in managing user access and accounts.

- The process of managing users' information access rights and ensuring that they are in accordance with business requirements has not been formalized. In addition, there is no process established to notify SBS Computing staff when users transition out from their departments.

- A review of administrative accounts noted one active administrative account (Systems Center) that was no longer used. However, the IT staff deleted this account during this review.

Without stronger password requirements for the Biological Sciences environment, there is an increased risk of improper or unjustifiable access to systems and data. Also, formal processes for access request and removal decrease the risk of improper or unjustifiable access to electronic resources.

Management Action Plan

SBS Computing will enhance the password standards to be compliant with the campus policy and IS-3 guidelines. Specifically, SBS Computing will:

- Document and implement password strength and requirements and determine if a password expiration policy should be established. Target date for completion is March 2014; and

- Develop and implement a formal process for supervisors for the creation and deletion of user accounts on systems and applications. A formal document will help with coordinating with unit supervisors in ensuring that information access rights are in accordance with their business requirements. Target date for completion is March 2014.

[2] A group of computers and devices on a network that are administered as a unit with common rules and procedures.

7. Collection, Management, and Analysis of Log Data

Background

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 SBS audit logs for a sampled server validated that logs are enabled to capture events such as logon/off, failed logon, access attempts, and others. However, opportunities for improvement of the log management practice were also noted. Specifically, IAS noted that:

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

- There is no central audit log management and logs are stored only on the individual systems generating the log data. The server event logs are stopped or overwritten once the 250 megabytes limit has been reached. The system administrator periodically clears the event logs manually to create additional space and the logs are kept for 12 months.

IS-3 requires the implementation of audit logging policies defining the use, review, and retention of audit logs. Robust logging and monitoring functions enable the early detection and/or prevention and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

Management Action Plan

SBS Computing is currently working with OIT to use log analyzer software and will formalize our log management practices. Target date for completion is March 2014. Specifically, SBS Computing will define and document the following:

- What events need to be logged;

- Where the logs will be centrally stored;
- How long the logs will be kept before archiving;
- How long archived logs will be maintained; and
- Who, how, and how often logs will be reviewed.

8. Faculty Computing Assessment

Observation

Most faculty members in SBS host their own data and maintain their own endpoint devices (e.g. servers, desktops, laptops etc.). Consequently, some of the key concerns noted are the risk of data loss, the need for asset inventory and classification, and safeguards implemented for systems and application security. The specific areas are outlined below.

- There is a need to develop research data storage systems for long term and safe storage. Currently, there are concerns that some faculty members are using portable devices and cloud services such as Dropbox, Crashplan, and Google Apps for storage and file sharing.
- There is no inventory and classification of faculty computing assets (hardware, software, and data). A current inventory and classification of electronic assets is needed to identify and determine the nature of faculty electronic information resources as a basis for implementing appropriate security safeguards. In addition, SBS Computing does not have a process to ensure that faculty endpoint devices are appropriately configured and managed according to their IT environment network security policy. For instance, they cannot ensure that desktops and laptops are current with software security patches and that anti-malware tools are installed and current.

The use of cloud services may increase the risk of data loss and are generally not recommended when it comes to university data. Also, an accurate and up-to-date asset inventory and information asset classification is crucial for ensuring that systems are effectively configured and updated as intended. Lastly, software vulnerabilities that are not patched timely increases the risk

that operating systems and/or applications could be compromised by known vulnerabilities.

Management Action Plan

There is no clear solution to this challenge at this time; however, SBS Computing will mitigate the above information security risk to SBS using the following techniques by September 2014.

- SBS Computing will encourage faculty to store data on SBS servers or OIT managed data storage units. In addition, we will periodically remind faculty of the types of sensitive and/or restricted data that should not be stored and, if stored, must be encrypted.

- SBS Computing will look into ways to better educate faculty on the need to keep their operating systems, applications, and anti-malware software current. In addition, we will encourage faculty to use passwords which are complaint with the campus policy and IS-3 guidelines.