FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit Report of University Implementation of Prior Years' Recommendations

Report No. 17/18-10

April 24, 2018

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

MEMORANDUM

DATE: April 24, 2018

TO: Mark B. Rosenberg, University President

FROM: Allen Vann, Chief Audit Executive

SUBJECT: **Audit Report of University Implementation of Prior Years' Recommendations Report No. 17/18-10**

We have completed an audit of University Implementation of Prior Years' Recommendations. The objectives of our audit was to test, on a sample basis, the self-reported management data regarding implementation of past audit recommendations, and to determine whether recommendations were effectively implemented as asserted by management.

The audit covered selected recommendations issued by the Office of Internal Audit and reported by management as implemented between October 1, 2012 and April 30, 2017.

Overall, our audit disclosed that management has improved on their implementation of past audit recommendations. The number of fully implemented recommendations increased to 73% from an average of 69% over the prior three audits. To management's credit, the number of recommendations classified as not implemented dropped to 5% compared to 11% reported in 2013.

The audit resulted in re-issuing 11 mostly partially implemented prior recommendations. Management agreed to implement all of our recommendations.

We would like to take this opportunity to express our appreciation to you and your staff for the cooperation and courtesies extended to us during the audit.

Attachment

C: FIU Board of Trustees
Kenneth G. Furton, Provost and Chief Operating Officer
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President
Elizabeth Bejar, Vice President for Academic Affairs
Robert Grillo, Vice President of Information Technology and CIO
Barbara Manzano, Assistant Vice Provost Planning & Finance

BACKGROUND

Based upon direction from the Board of Trustees (BOT), the Office of Internal Audit's practice for monitoring implementation of past recommendations includes obtaining semiannual status reports from responsible/cognizant officials. The implementation status and date of implementation for those recommendations self-reported to us by management is compiled by our Office and routinely presented to the BOT's Audit and Compliance Committee. About every three years, our Office will test, on a sample basis, management's self-reported data to assure that they in-deed have implemented the recommendations. Our last follow-up audit, Report No. 13/14-06, was issued in 2013.

Our Office follows the Institute of Internal Auditors' International (IIA) Standards for the Professional Practice of Internal Auditing. Those standards require our Office to establish a follow-up process to monitor and ensure that recommendations have been effectively implemented, and to make sure the Board of Trustees and senior management understand and assume the risks associated with inaction. In our opinion, the process described in the first paragraph of this section comports with the IIA standards.

OBJECTIVES, SCOPE, AND METHODOLOGY

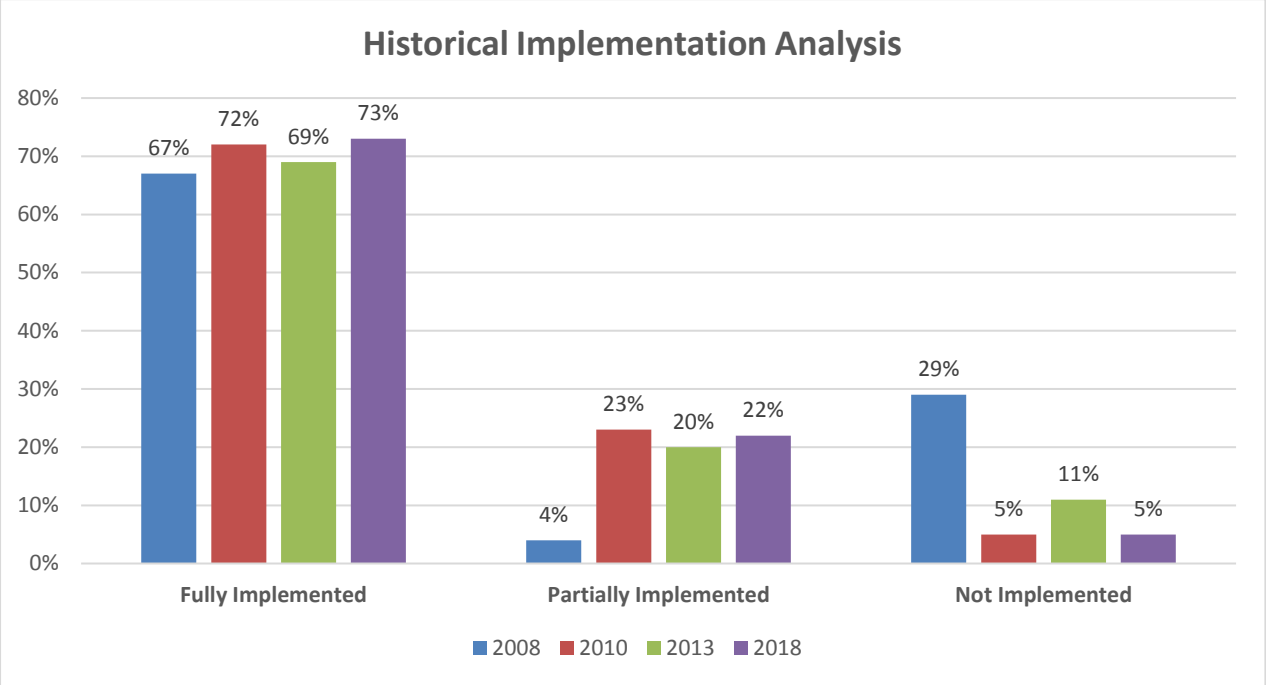
As previously stated, the objectives of our audit was to test, on a sample basis, the self-reported management data regarding implementation of past audit recommendations, and to determine whether recommendations were effectively implemented as asserted by management.

Between October 1, 2012 and April 30, 2017 there were 620 implemented recommendations self-reported by management. Of these, 207 were determined to have been followed-up in recent audits or scheduled to be followed-up in upcoming audits. From the remaining 413, we judgmentally selected 41 recommendations considered high-risk, representing 10% of the population for testing.

Our examination included, but was not limited to, observation of actual practices and processing techniques, interviews with University personnel, and testing of selected transactions and devices during the period audited, as considered necessary under the circumstances. Sample sizes and transactions selected for testing were determined on a judgmental basis.

OBSERVATIONS

Based on our testing, we have concluded that management's implementation rate has improved from the results of the previous last three follow-up audits issued in 2008, 2010 and 2013, as depicted in the following chart:



Most of the tested recommendations were overwhelmingly acted upon (73%), with 22% still being worked on and only 2 recommendations pending. According to management, these remaining recommendations will be completed shortly.

On the following pages are the results of each of the recommendations tested and the responsible area executives. Note that due to organizational and personnel changes, not all of the executives listed were in the position for which the recommendation was originally directed. Likewise, some the names of the audited units have changed since the original audit.

Report Recommendations	Fully Implemented	Partially Implemented	Not Implemented	Responsible Area Executives
Audit of the Information Systems Continuity Plan (2010/11-01)				
2.1 – Business Impact Analysis/ Disaster Recovery Plan	✓			Furton/Grillo
4.3 – IT Security Awareness Training/IT Continuity	✓			Furton/Grillo
Audit of the Herbert Wertheim College of Medicine Information Systems Security Controls (2012/13-04)				
1.1 – ID Protected Data & Critical Systems	✓			Rock/Kunkle
1.2 – Risk Assessment	✓			Rock/Kunkle
1.12 – Security Awareness Program		✓		Rock/Kunkle
1.16 – Disaster Recovery Testing		✓		Rock/Kunkle
2.5 – Badge Access Reports	✓			Rock/Kunkle
3.2 – Database Administrator Access	✓			Rock/Kunkle
3.4 – Server Administrator Members	✓			Rock/Kunkle
3.7 – Audit Log Review Process			✓	Rosenberg/Boston
Audit of the University's Compliance with the National Collegiate Athletic Association's Student-Athlete Eligibility Requirements (2012/13-08)				
3.1 – Student-Athlete Eligibility	✓			Rosenberg/Boston
Audit of the School of Journalism & Mass Communications (2012/13-09)				
3.2 – Equipment Inventory	✓			Schriner/Ponte
7.1 – Workstation Security		✓		Schriner/Ponte
7.4 – Administrator Accounts	✓			Schriner/Ponte
Audit of Controls over Salary Costs Charged to Grants (2013/14-05)				
1.1 – Non-exempt Employee Hours are Properly Approved	✓			Furton/Gil
4.1 – Administrative/Clerical Hours Charged to Grants	✓			Furton/Gil

Report Recommendations	Fully Implemented	Partially Implemented	Not Implemented	Responsible Area Executives
Audit of University Implementation of Prior Years' Recommendations 2013 - University's Fuel Inventory Controls (2013/14-06)				
1.1 – Recordkeeping Controls	✓			Jessell/Martinez
5.2 – Physical Security	✓			Jessell/Martinez
Audit of the Patricia and Phillip Frost Art Museum (2013/14-12)				
1.1 – Collection Database Accuracy		✓		Furton/Pomeroy
6.1 – Museum Application	✓			Furton/Pomeroy
7.3 – Database Administrator	✓			Furton/Pomeroy
8.3 – Emergency Disaster Plan		✓		Furton/Pomeroy
Audit of the School of Computing and Information Sciences (2013/14-15)				
1.1 – User Account Procedure	✓			Volakis/Iyengar
1.2 – Administrator Accounts		✓		Volakis/Iyengar
2.3 – User Passwords	✓			Volakis/Iyengar
3.2 – External Vulnerability Testing	✓			Volakis/Iyengar
5.3 – Continuity Plan	✓			Volakis/Iyengar
Audit of the Southeast Environmental Research Center (2014/15-04)				
4.2 – Grant Costs	✓			Heithaus/Crowl
5.1 – Credit Card Approvers	✓			Heithaus/Crowl
8.2 – Nepotism	✓			Heithaus/Crowl
Audit of the College of Architecture (2014/15-08)				
3.5 – Conflict of Interest Forms		✓		Schriner/Silverio
4.5 – Optional Student Fees		✓		Schriner/Silverio

Report Recommendations	Fully Implemented	Partially Implemented	Not Implemented	Responsible Area Executives
Audit of Camps and Programs Offered to Minors (2014/15-09)				
1.1 – Expand Pre-employment Requirements		✓		Hardrick/Hudson
Audit of the Parking and Transportation Department (2014/15-10)				
1.3 – Employee Classification/ Parking Rates			✓	Marques/Hartley
1.7 – Firewall Security/Credit Card Machines	✓			Marques/Hartley
Audit of Study Abroad and International Student Exchange Programs (2015/16-05)				
3.2 – Centralize Collection Process	✓			Newman/Boudon
Audit of University Building Access Controls (2015/16-06)				
4.6 – User Accounts	✓			Jessell/Cal
Audit of the College of Education (2015/16-09)				
1.2 – Separation from Employment Clearance Form/Equipment	✓			Heithaus/Dinehart
4.2 – Materials and Supplies Fee Revenues	✓			Heithaus/Dinehart
Review of Bank Account Reconciliations (2016/17-05)				
1.3 – Independent Trial Balance	✓			Jessell/Brophy
Audit of the Chaplin School of Hospitality & Tourism Management (2016/17-06)				
2.1 – Student Fees/Dean's Discretionary Account	✓			Furton/Cheng
TOTAL COUNT	**30**	**9**	**2**	

The following are the original recommendations determined to be either partially implemented or not implemented, along with our current observations, and management's revised response/action plan and implementation dates.

PARTIALLY IMPLEMENTED:

1. **Audit of the Herbert Wertheim College of Medicine Information Systems Security Controls (Report No. 2012/13-04)**

   Recommendation No. 1.12 – Security Awareness Program: Develop and implement a security awareness-training program. The program should be periodically evaluated to ensure it is up to date and effective.

Auditor's Observation: To support that adequate HIPAA and FERPA trainings were being conducted, management provided the HIPAA and FERPA 2016 Trainings Annual Report. HWCOM administered HIPAA and FERPA training to 487 and 477 employees, respectively. However, 89 remained pending to complete HIPAA and 95 were pending to complete FERPA in 2016. When compared to the 2017 Trainings Annual Report, 32 names pending for HIPAA training reappeared and 33 names pending for FERPA training reappeared.

Management Response/Action Plan: During the month of April 2018, the College of Medicine will contact all the employees that have not completed the Annual HIPAA and FERPA trainings during 2016 and were still pending during 2017 to request the completion of the pending trainings. During the month of May 2018, follow up emails will be sent to the employees and results will be evaluated to determine if additional actions are necessary.

During the 2018 Annual HIPAA and FERPA trainings (to be launched during June 2018), the College of Medicine will add additional controls by comparing the list of employees pending completion of the trainings to the employees that did not complete the trainings during the 2017 Annual HIPAA and FERPA trainings. This measure will be added to the procedure in place and will be part of the controls done on an annual basis moving forward.

Implementation date: June 2018

2. Audit of the Herbert Wertheim College of Medicine Information Systems Security Controls (Report No. 2012/13-04)

Recommendation No. 1.16 – Disaster Recovery Testing: Ensure continued service and the protection of sensitive data by performing disaster recovery testing and refine the Continuity of Operations Plan (COOP) accordingly, giving due consideration to critical business operations identified in the business impact analysis; and document COOP roles and responsibilities.

Auditor's Observation: After reviewing the HWCOM's Disaster Recovery Plan, necessary components included roles and responsibilities, critical operations, classification of services, vendor services, and backup requirements. However, for critical operations, only 3 of the 10 operations defined as "critical" were formally tested.

Management Response/Action Plan: Effective immediately, COM IT will ensure to document or seek to obtain documentation of disaster recovery activities and exercises on critical systems. Types of documentation and disaster recovery exercises will be based on ownership of the system. COM IT will document various forms of disaster recovery testing for systems it manages. Systems managed by third parties will be subject to availability and access to their disaster recovery testing documentations. Adherence to this change will be evidenced by the next cycle of disaster recovery testing for the identified critical systems.

Implementation date: December 2018

3. **Audit of the School of Journalism & Mass Communications (Report No. 2012/13-09)**

Recommendation No. 7.1 – Workstation Security: Work with the Information Technology Security Office to ensure that workstations are adequately protected from malicious code.

Auditor's Observation: We scanned five workstations and found that three did not have data loss prevention software installed and four computer hard drives were not encrypted.

Management Response/Action Plan: Some McAfee products have interfered with our information systems and continue to do so. On March 8, 2018, the Division of IT sent out a McAfee compatibility matrix to help Information Technology Administrator with McAfee product updates. We have been in communication with the appropriate parties in the Division of IT and Network Security and System Engineers about these problems. They aware of the missing McAfee products and will continue to work with the Departments in the School of Mass Communication and Journalism to ensure that our devices are adequately secure.

Implementation date: September 2018

4. **Audit of the Patricia & Phillip Frost Art Museum (Report No. 2013/14-12)**

Recommendation No. 1.1 – Collection Database Accuracy: Ensure that the collection database is accurate, complete, and current, which includes: (a) Improving its collection report to accurately capture a total object count; (b) Entering each object condition into the collection database; and (c) Ensuring any missing accession numbers and objects are investigated and formally deaccessioned, if necessary.

Auditor's Observation: We requested the inventory list from the Museum's Chief Registrar. A sample of 21 items were tested to determine if the Museum was practicing adequate record keeping. Of the 21 items tested, 5 appeared duplicated on the list. The inventory list also did not contain information on object condition. Management explained that because of significant changes to their registration and collections staff, they did not enter the object condition into the database, but rather maintained hand-written condition notes for new accession numbers and put hard copies in folders.

Management Response/Action Plan: The Chief Registrar created a spreadsheet pulled from the database with a basic condition note listed in one column. From this spreadsheet, we will develop an internship project whereby the blank fields can be appropriately updated. A student can identify the object/object record, enter the basic condition note in the spreadsheet, and then update the database accordingly. The Chief Registrar is anticipating that it will take two full semesters plus the summer to complete this project. With an internship beginning in Fall 2018, the Chief Registrar anticipates completion by the end of Summer 2019.

Implementation date: Summer 2019

5. **Audit of the Patricia & Phillip Frost Art Museum (Report No. 2013/14-12)**

   Recommendation No. 8.3 – Emergency Disaster Plan: Work with Emergency Management to conduct a tabletop exercise to test components of its Emergency/Disaster Preparedness and Recovery Plan.

   Auditor's Observation: We obtained support that the Museum had participated in a tabletop exercise training, but it was not specific to the Museum.

   Management Response/Action Plan: The Museum will work with Emergency Management to conduct a tabletop exercise testing the Museum's Emergency/Disaster Preparedness and Recovery Plan.

   Implementation date: Fall 2018

6. **Audit of the School of Computing and Information Sciences (Report No. 13/14-15)**

   Recommendation No. 1.2 - Administrator Accounts: Review and disable generically named administrator accounts and comply with the University's password parameter settings.

   Auditor's Observation: A sample of three endpoint security scans were performed. The results showed that the "Hammerfall" computer from the prior audit still had an active generic administrator account called "cyg_server". Management stated that generic accounts were supposed to be used at initial installs. However, our findings showed that the last login under this account name was December 13, 2017.

   Management Response/Action Plan: We will complete a sweep of all Microsoft Windows systems in the School to ensure that there is only one local administrator privileged account on each end-station, necessary for os/app operations. New deployments of Microsoft Windows images will be reviewed so that the image is consistent with this practice.

   Implementation date: August 2018

7. **Audit of the College of Architecture (Report No. 2014/15-08)**

   Recommendation No. 3.5 – Conflict of Interest Forms: Ensure that Outside Activity/Conflict of Interest Forms are properly completed and approved.

   Auditor's Observation: CARTA management provided documentation and support that showed an e-mail notification sent to employees as a reminder to complete Conflict of Interest (COI) forms before the October 31, 2016 deadline. An additional e-mail identified eight employees from the CARTA Dean's Office with a "not submitted" status that were sent another reminder 10 days before the deadline.

A query was performed through the Human Resources System for the 2016/17 fiscal year. A total of 20 employees from eight departments within CARTA failed to submit their COI forms. Three of the original eight employees reminded to complete their COI forms were included in the list of 20 at the time of the audit.

Management Response/Action Plan: Owned by HR, but will work closely with that office to make ensure CARTA employees comply.

Implementation date: Immediately

8. Audit of the College of Architecture (Report No. 2014/15-08)

Recommendation No. 4.5 – Optional Student Fees: Ensure that all expenses from optional student fees collected are only limited to equipment or supplies/materials used directly by the students for courses.

Auditor's Observation: Nine transactions made by the Schools of Architecture, Music, and Art & Art History were reviewed. Of the nine, two were determined not to be in accordance with the purpose of the Optional Student Fees. Storage units paid for by the School of Music were not used directly by the students or for the direct instruction of the course. Hoists purchased by the School of Art & Art History and installed in the Sculpture Facility were paid for with the optional student fees when the costs should have been funded through the equipment fee.

Management Response/Action Plan: The Dean's Office will monitor fee expenditures on a quarterly basis. A training session with all CARTA Departments will be conducted during Spring 2018 term to reinforce policies and guidelines applicable to student fees.

Implementation Date: Immediately

9. Audit of Camps and Programs Offered to Minors (Report No. 2014/15-09)

Recommendation No. 1.1 – Expand Pre-Employment Requirements: Expand the Pre-Employment Requirements Policy to govern all employees and volunteers in contact with minors.

Auditor's Observation: During the testing period, we reviewed the Policy and found that it had not been amended since March 31, 2009, prior to our original audit.

Management Response/Action Plan: An updated version effective as of February 15, 2017 was e-mailed to the Internal Audit Office via web link. The updated version included a section emphasizing the need for Level II background screening periodically every 5 years if an employee is in contact with minors/vulnerable persons. The updated policy version will be made live for the public audience effective by September 20, 2017.

Implementation date: Immediately

NOT IMPLEMENTED:

10. Audit of the Herbert Wertheim College of Medicine Information Systems Security Controls (Report No. 2012/13-04)

Recommendation No. 3.7 – Audit Log Review Process: Develop and implement a formal audit log review process.

Auditor's Observation: The Health Affairs Compliance Officer is no longer with the University and the position remains unfilled. As a result, audit logs are not being reviewed.

Management Response/Action Plan: The search committee is in the process of interviewing candidates. We are told that someone should be in place by June and audit logs should be updated and available by September.

Implementation date: September 2018

11. Audit of the Parking and Transportation Department (Report No. 2014/15-10)

Recommendation No. 1.3 – Employee Classification/Parking Rates: Establish controls to ensure that employees' classifications are properly reviewed and parking rates are accurately assessed.

Auditor's Observation: Since the original finding was principally with AFSCME union employees, we selected 18 AFSCME employees earning $31,200 or less to review the parking rate assessed. We found that 8 of the 18 employees were not assessed the proper parking rate.

Management Response/Action Plan: The dashboard was implemented as outlined in response to the request. However, two separate issues, which may have caused the permits to be sold at an incorrect rate, have been noted. These errors would not have been identifiable through the dashboard. They are more specifically:

a) A systems permit setup error by our IT person for online sales. This error has been corrected in the software system; and
b) Human error by the clerk selling the wrong permit type.

In addition to our continued viewing of the dashboard, permit sales now are being cross-referenced through PantherSoft to ensure the permit is being sold at the correct rate. Human errors are being corrected through retraining of data verification.

Implementation date: Immediately