

FIU

**Office of
Internal Audit**

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT STATUS REPORT




Board of Trustees

September 14, 2023



Office of Internal Audit

Date: September 14, 2023
To: Board of Trustees Audit and Compliance Committee Members
From: Trevor L. Williams, Chief Audit Executive 
Subject: OFFICE OF INTERNAL AUDIT STATUS REPORT

I am pleased to provide you with our quarterly update on the status of our Office’s activities since our last update to the Board of Trustees Audit and Compliance Committee on June 15, 2023.

Projects Completed

Audit of Facilities Assessments and Deferred Maintenance

We have completed an audit of Facilities Assessments and Deferred Maintenance for the period of July 1, 2021, through June 30, 2022, and have assessed the current practices through May 2023. During the audit, we reviewed FIU’s Facilities Management Department (“Facilities”) processes to ensure that the University has existing controls that are adequate and provide reasonable assurance that Facilities assessments and deferred maintenance are adequately scheduled, performed, monitored, and communicated.

The facilities condition assessment and deferred maintenance activity is among the various activities engaged in by Facilities to achieve their commitment of providing quality, sustainable facilities, and diligent oversight of all aspects of FIU’s physical environment. Facilities expended approximately \$95.8 million for major and minor projects during the audit period, of which \$12.8 million (13 percent) was related to 44 total deferred maintenance projects.

Overall, our audit concluded that Facilities has established internal controls and processes for the areas in scope and has excelled in their management of some of these areas, including the permitting of deferred maintenance projects, managing service contracts, and approving project expenses. However, we identified areas for process improvement, including processes related to Life Cycle Asset Management, preventive maintenance, and deferred maintenance project monitoring. Some examples of how controls could be strengthened include:

- Developing comprehensive written departmental procedures for the existing Life Cycle Asset Management function to address key processes.
- Ensuring that preventive maintenance is automatically scheduled for all critical life safety assets and that the completion of preventive maintenance is timely documented within the Maximo system.
- Implementing a robust Construction Project Management System that encompasses all key processes.
- Formalizing the process for reconciling Facilities’ internal reports to the General Ledger.

Work in Progress

The following ongoing audits are in various stages of completion:

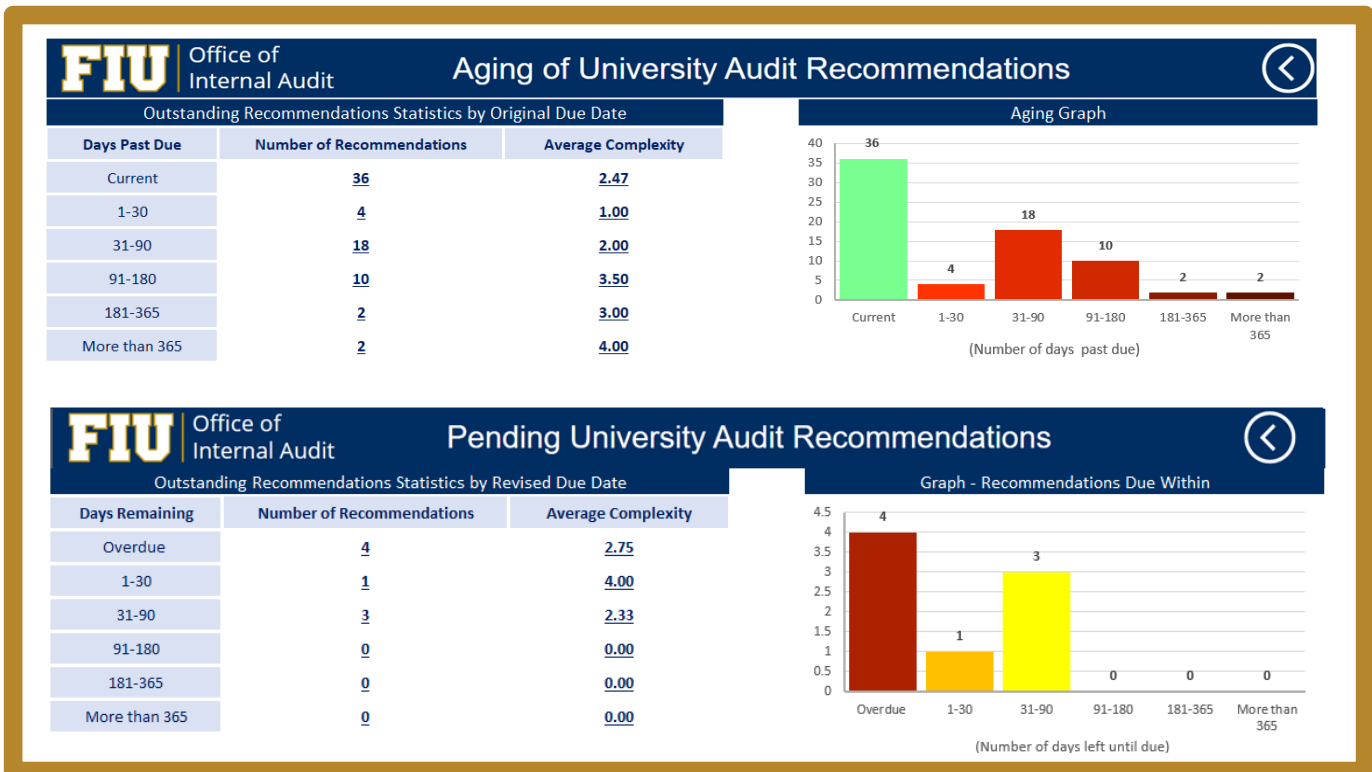
<u>Ongoing Audits</u>	
Audits	Status
Payments to Separated Employees	Fieldwork in Progress
Data Breach of Protected Information	Fieldwork in Progress
Digital Brand Management	Fieldwork in Progress
Natural Disaster Preparedness and Response	Fieldwork in Progress
Food Network South Beach Wine & Food Festival	Fieldwork in Progress
Panther Tech	Fieldwork in Progress
Continuous Auditing	Fieldwork in Progress

Prior Audit Recommendations Follow-Up Status Report

Since June 1, 2020, University management has been able to utilize the OIA Panther Audit Platform to update and report the status of prior audit recommendations. Upon receiving the submission from management through the Platform, OIA staff performed a substantive examination of the accompanying documentation or revised process to validate the status of the recommendation as reported by management. The outcome from our auditing efforts results in either acceptance or re-characterization of the reported status.

Since our last report to the Committee on management’s progress towards completing past audit recommendations, there were 73 recommendations due for implementation through June 30, 2023. Based on the work performed, we have concluded that 58 of said recommendations (79 percent) were completed, 10 (14 percent) were partially implemented, and 5 (7 percent) were not implemented by their expected due date. Management has provided expected completion dates for all recommendations that were not completed. (See table and revised plans of action to complete the outstanding recommendations along with due dates on the following pages.) We thank management for their cooperation and encourage continued improvement.

The following graphs display an aging of outstanding audit recommendations as of June 30, 2023, as reflected in the Platform, indicating the number of days delayed for those recommendations past due and the number of days remaining before due for implementation for recommendations with a revised due date.



AUDIT RECOMMENDATIONS FOLLOW-UP
JANUARY 1, 2023 – JUNE 30, 2023

Areas Audited	Total Due for Implementation	Implemented	Partially Implemented	Not Implemented
Admissions Policy Compliance	1	1		
Export Control and Selected Foreign Influence Compliance	2	2		
FERPA Compliance	1	1		
Healthcare Affiliated Agreements for Student Placement/Rotation	1	1		
Media Sanitization Guidelines and Controls	1	1		
Performance-Based Funding and Emerging Preeminent Metrics	1	1		
Review of Bank Account Reconciliations	1	1		
Robert Stempel College of Public Health & Social Work	4	4		
Conflict of Interest and Related Party Transactions	7	5	2	
Cybersecurity Prevention and Detection Controls – Ransomware	35	29	3	3
IT Controls Over Procurement Services	3	1	2	
Procurement and Competitive Bidding Procedures	2	1	1	
Student Safety- Hazing Prevention	14	10	2	2
Totals	73	58	10	5
Percentages	100%	79%	14%	7%

MANAGEMENT RESPONSES TO OUTSTANDING AUDIT RECOMMENDATIONS WITH REVISED TARGET DATES

Conflict of Interest and Related Party Transactions (March 7, 2022)

1. Audit Issue: **Related Party Transactions** (Recommendation #5.1)

Recommendation:

Procurement Services should implement a mechanism to detect related party transactions.

Action Plan to Complete:

Procurement Services has requested that the following conflict of interest questions that was provided by Vilma Mesa from OGC be added during Supplier on Boarding in PeopleSoft: Vendor confirms that Vendor is familiar and complies with all applicable conflict of interest legal requirements including Florida's Code of Ethics for Public Officers, Chapter 112, Part III, Florida Statutes (the "Code of Ethics"). All vendors must disclose the name of any FIU officer or employee who is employed by Vendor (Section 112.313(7), Florida Statutes) or owns, directly or indirectly a material interest in the Vendor's company or any of its branches (Section 112.313 (3), Florida Statutes). Therefore:

- A. Vendor hereby certifies that neither Vendor nor its employees, officers or owners have, or any of the aforementioned has a relative that has a relationship with FIU, that will result in a violation of the Code of Ethics, including, but not limited to Sections 112.313(3) and (7), Florida Statutes and Section 112.3185(6), Florida Statutes, by reason of the Vendor entering into the agreement with FIU.
- B. Vendor declares it has not and will not provide gifts or hospitality of any dollar value or any other gratuities to any FIU employee to obtain or maintain an agreement with FIU.
- C. Vendor agrees that it shall disclose any conflict of interest by submitting information to vendors@fiu.edu prior to entering into an agreement with FIU and/or immediately upon learning of such conflict of interest.

The PantherSoft Team has completed the requested changes in PeopleSoft, FSSS will test and let Procurement Service know when the changes are live in Supplier on Boarding. Due to upgrades in PeopleSoft, this had to wait to go live until later in May. Every quarter Procurement Services will conduct a random sample of 10 suppliers and manually verify against addresses of active employees. We have attached the report for transactions in the 2nd quarter (Oct-Dec) of FY22-23. We will submit future

report on Teams and have given the Auditors access. We have not been able to create a query that will look for related party transactions because that will require comparing the address field of suppliers with the address fields of employee. Text fields cannot be compared via simple query because “123 Street”, “123 STREET” and “123 St.” are all different. Supplier and employee addresses will need to be standardized for it to work, which is not the case for older suppliers in the system. Please see the attached 2nd Quarter report. HR can also develop a long-term solution. One recommendation is for HR to include in the annual outside activity/conflict of interest form some language asking employees if their outside activity is with FIU, own directly or indirectly a material interest in a company registered as a supplier with FIU or has a relative who owns a company or is an officer of a company registered with FIU. If an employee informs HR of such conflict, then HR will reach out to Procurement Services, and we will check if any transaction exists for the said company.

Original Target Date: December 31, 2022

New Target Date: March 31, 2023¹

2. **Audit Issue: Disclosure of Supplier Conflicts of Interest (Recommendation #6.2)**

Recommendation:

Procurement Services should provide guidance to all applicable areas (i.e., Academic Affairs, Human Resources, General Counsel) on where the disclosed conflicts are documented and what their responsibility is regarding reviewing conflicts.

Action Plan to Complete:

Vilma Mesa from OGC is scheduling a meeting with current approvers of conflict-of-interest compliance questions in TCM to provide necessary training, along with their supervisors. It is the responsibility of the Department Head who assigns approvers in TCM to identify the subject matter expert in the workflow approval for TCM's conflict of interest questions. Serge Menyonga will provide Vilma with a list of approvers in TCM. The information shared with the current approvers will be incorporated into the TCM training material that is currently being updated.

Original Target Date: August 31, 2022

New Target Date: August 31, 2023

¹ This recommendation was subsequently implemented as of August 1, 2023.

**Cybersecurity Prevention and Detection Controls - Ransomware
(November 15, 2022)**

1. Audit Issue: **Identity Management and Access Control** (Recommendation #2.4)

Recommendation:

Implement a process to ensure that access to FIU systems is timely disabled for individuals who terminated employment with the University.

Action Plan to Complete:

Updated management response: CASTIC will add an AD security group review to its offboarding procedures to ensure that access to CASTIC managed resources is removed. Furthermore, supervisors will receive an email reminder emphasizing the importance of timely submission of the necessary separation documentation.

Original Target Date: September 1, 2023 New Target Date: September 30, 2023

2. Audit Issue: **Identity Management and Access Control** (Recommendation #2.16)

Recommendation:

Evaluate whether workstations on the Panther domain and unmanaged workstations should also be equipped with McAfee DLP.

Action Plan to Complete:

The DoIT does agree that all workstations should be managed, and we will evaluate the deployment of DLP to those on the Panther Domain, which are primarily lab computers. As far as unmanaged workstations, the DoIT does not currently have a way to install software to unmanaged workstations. We agree that unmanaged workstations would leave an identified gap. The DoIT does encourage all IT Admins to join their computers to the AD or Panther Domains to benefit from the enterprise tools we have to offer, however, at this time we do not have a way to identify all the unmanaged workstations nor a way to enforce network-based policies to require them to join. We will initiate the engagement and start the campaign to promote the use of managed devices.

Original Target Date: June 30, 2023 New Target Date: June 30, 2023²

² This recommendation was subsequently implemented as of August 7, 2023.

3. Audit Issue: Information Protection Processes and Procedures (Recommendation #2.20)

Recommendation:

Ensure all workstations are running updated operating systems.

Action Plan to Complete:

CASTIC identified 445 out of 2293 workstations are on unsupported OS (19%) - 6/8/2023:

A. 8% Mac Unsupported (as of 6/8/2023)

B. 11% Windows Unsupported (after patch deployment)

Met with NSSE on 5/9/23 to learn how McAfee affects Windows operating system upgrades. Process was developed to fix the McAfee issue. Patch was developed to download and install the latest Windows operating system. This patch is automatically deployed and will address any workstations moving into the future as well. From 05/19/2023 to 06/08/2023, the number of unsupported workstations dropped from 315 to 244. Unfortunately, our management tool (PDQ Inventory) is unable to track these changes over time. Any workstations that remain on an unsupported Windows operating system are currently offline or are being addressed manually because of various issues (lack of hard drive space, poor overall system performance, etc.). These workstations are automatically aggregated into a management group called 'Unsupported Windows Versions' within PDQ Inventory. Any additional workstations that meet the criteria for an unsupported operating system are automatically added to this group. An automated operating system update script task is immediately deployed after a workstation is detected on the FIU Network. This task also applies to mobile devices that connect to the VPN. Be advised that PDQ Deploy considers workstations that cannot be accessed as failed deployments. Meaning that they are offline or offsite. As of 6/5/2023, 191 out of 516 macOS workstations are unsupported (37% of total Mac fleet). CASTIC will perform sweeps to update these Macs to the latest OS. This is a manual process that will require addressing each workstation individually.

Original Target Date: September 1, 2023

New Target Date: October 31, 2023

4. Audit Issue: Security Continuous Monitoring (Recommendation #3.2)

Recommendation:

Incorporate privilege escalation attacks into monitoring capabilities.

Action Plan to Complete:

We have identified a tool which will provide the visibility, monitoring, reporting, and an approval process for privilege escalations. This tool needs to be procured, so we

are trying to secure funding now and will be developing a project plan to configure and deploy it along with the documentation needed for users and admins.

Original Target Date: April 1, 2023

New Target Date: October 31, 2023³

5. Audit Issue: **Security Continuous Monitoring** (Recommendation #3.4)

Recommendation:

Consider monitoring for unauthorized software.

Action Plan to Complete:

There are several ways DoIT will be able to meet this recommendation in the future.

- A. DoIT is starting a project to implement Intune, and mobile device management solution which we will be able to manage what applications are installed on workstations.
- B. DoIT is trying to secure funding to purchase a privilege access management tool which will give us the ability to remove admin access preventing the install of many unsupported applications.
- C. DoIT is developing a catalogue of authorized and supported software which will be published on the AskIT site.

Original Target Date: April 30, 2023

New Target Date: November 30, 2023

6. Audit Issue: **Security Continuous Monitoring** (Recommendation #3.8)

Recommendation:

Ensure the timely remediation of vulnerability reports.

Action Plan to Complete:

Vulnerabilities in the initial audit have been addressed. Remediation of vulnerabilities is ongoing. Patches for common software like Google Chrome, Mozilla Firefox, Office, Acrobat, Windows updates, etc., are deployed on a daily basis. Relevant deployment logs are sent to castic@fiu.edu detailing the success rate of deployments. Offline machines that were not successfully targeted are listed as failed deployments. To address this, schedules are configured in PDQ Deploy to target these hosts after they come online. CASTIC is currently addressing Log4J vulnerabilities related to SPSS 20 and Papercut. The latest version of SPSS (28) is currently being deployed to older systems to replace SPSS 20. Only 2 SPSS 20 hosts are remaining. We are collaborating with DoIT to upgrade the Papercut server and remove the Papercut client from CASTIC owned systems. A sample Papercut uninstall report is attached. Attached are the following:

³ This recommendation was subsequently partially implemented as of August 11, 2023.

- A. Email communications with DoIT regarding Papercut.
- B. Sample Papercut uninstall deployment report.
- C. Vulnerability reports from February, March, and April. Be advised that the drastic difference in identified vulnerabilities in the April report is due to those systems being unavailable during the patch deployment Window. The February and March report show that vulnerabilities are being addressed in a timely manner. The majority of vulnerabilities in those reports like Log4J, Silverlight, etc., are currently being investigated or remediated now.

Original Target Date: September 1, 2023 New Target Date: September 30, 2023

**Information Technology Controls Over Procurement Services
(February 11, 2022)**

1. Audit Issue: **Identify Access Management** (Recommendation #1.1)

Recommendation:

Establish and implement procedures for documenting the process for Jaggaer terminated and transferred users as well as inactive/dormant accounts.

Action Plan to Complete:

This is contingent to the shopper role and account sync going live. We finalized the contract with Jaggaer. We had a meeting with Jaggaer's project manager on 11/22/2022. They were able to do the setup as requested by nProdigy and provided the information. Serge followed up with nProdigy this morning, and there are a few tweaks they requested from Jaggaer. We will continue to work with Jaggaer and nProdigy on this project. We have a new expected completion date of 1/31/23.

Update 6/2/23 - This project was split into 2 phases. Phase 1 was completed on March 13, which entailed the user sync project that enables a user who obtains or terminates the shopper role in PeopleSoft to also obtain or terminate the role in Jaggaer. Phase 2 is to sync the requester role and all the Contract+ (TCM), Sourcing, and Invoices (AP Director) to sync as well so that access is terminated in both systems simultaneously. Because of the Make Me Current PS project that was prioritized and required a freeze of all other projects until May 15 of this year, the Phase 2 of the PS/Jaggaer sync project for Requestor roles was delayed and will be re-visited after FYE activities.

Original Target Date: November 30, 2022 New Target Date: October 31, 2023

2. Audit Issue: **Identify Access Management** (Recommendation #1.2)

Recommendation:

Ensure that terminated employee accounts are routinely deactivated from the Jaggaer system.

Action Plan to Complete:

This is contingent to the shopper role and account sync going live. We finalized the contract with Jaggaer. We had a meeting with Jaggaer's project manager on 11/22/2022. They were able to do the setup as requested by nProdigy and provided the information. Serge followed up with nProdigy this morning, and there are a few tweaks they requested from Jaggaer. We will continue to work with Jaggaer and nProdigy on this project. We have a new expected completion date of 1/31/23.

Update 6/2/23 - This project was split into 2 phases. Phase 1 was completed on March 13, which entailed the user sync project that enables a user who obtains or terminates the shopper role in PeopleSoft to also obtain or terminate the role in Jaggaer. Phase 2 is to sync the requester role and all the Contract+ (TCM), Sourcing, and Invoices (AP Director) to sync as well so that access is terminated in both systems simultaneously. Because of the Make Me Current PS project that was prioritized and required a freeze of all other projects until May 15 of this year, the Phase 2 of the PS/Jaggaer sync project for Requestor roles was delayed and will be re-visited after FYE activities.

Original Target Date: November 30, 2022

New Target Date: October 31, 2023

**Procurement and Competitive Bidding Procedures
(June 23, 2021)**

1. Audit Issue: **Header Comments** (Recommendation #5.2)

Recommendation:

Consider developing a mechanism to identify procurement methodology.

Action Plan to Complete:

Procurement Services reached out to FSSS on September 29, 2021 to request information on purchase order fields that may be used to better identify procurement method. The Contract ID field was specifically pointed out by Procurement as an area of interest as the Facilities Department is currently using the PeopleSoft contracts module and we'd like more information on how it works. Denise Catlin from Facilities met with Procurement on October 19, 2021 to demo the module and to explain how it is being used by FM Construction. We concluded this would not work for our purposes and must therefore continue the consultation/exploratory phase with the FSSS team on which field(s) can be used.

Attached is a high-level specification for the following audit recommendation: Audit of Procurement and Competitive Bidding Procedures Recommendation 5.2 - Consider developing a mechanism to identify procurement methodology.

Herve-Serge Menyonga is working with FSSS to set up a ticket once the PeopleSoft upgrade is completed. At that time, we will work with FSSS to develop business requirements around the fields available to us.

We can currently track procurement methods in the interim, which involves a combination of standard comments at header and line level on the purchase order. We have done our due diligence to try to develop another mechanism to identify procurement methodology.

Original Target Date: March 31, 2022

New Target Date: September 29, 2023

Student Safety - Hazing Prevention (October 19, 2022)

1. Audit Issue: **Hazing Prevention Training** (Recommendation #4.3)

Recommendation:

Create a consistent, ongoing, and comprehensive anti-hazing education plan that expands the population of students required to complete hazing prevention training. The plan could also include the following:

- A. Requiring students to complete hazing prevention training prior to participating in a student organization or group.
- B. Regularly assessing the education plan to address trends in student safety.
- C. Incorporating various formats of hazing prevention training courses such as in-person and peer-to-peer training and discussions.
- D. Monitoring completion of training requirements.

Action Plan to Complete:

Prevent.Zone training is now live on FIU Develop, [Hazing Prevention 101](#).

New students (i.e., first semester) will be batch enrolled on the Friday after add/drop for each semester.

Original Target Date: October 1, 2023

New Target Date: October 1, 2023

2. Audit Issue: **Incident Investigation and Adjudication Processes and Procedures** (Recommendation #8.1)

Recommendation:

Timely open and close incident reports and cases.

Action Plan to Complete:

SCAI and OIA will meet on (or around) January 15, 2024 to review the implementation of recommendation 8.1.

Original Target Date: April 30, 2023

New Target Date: January 15, 2024

3. Audit Issue: **Incident Investigation and Adjudication Processes and Procedures** (Recommendation #8.3)

Recommendation:

Complete follow-up discussions and meetings with FIU departments and student organizations and groups.

Action Plan to Complete:

Effective January 2023 monthly meetings will be conducted to ensure all audit recommendations are reviewed and completed, as well as to assure compliance.

Original Target Date: November 1, 2022

New Target Date: March 3, 2023⁴

4. Audit Issue: **Incident Investigation and Adjudication Processes and Procedures** (Recommendation #8.4)

Recommendation:

Monitor the completion of sanctions and ensure case statuses are accurately reflected in Maxient.

Action Plan to Complete:

SCAI will meet with OIA on (or around) January 15, 2024 to review Recommendation 8.4.

Original Target Date: April 30, 2023

New Target Date: January 15, 2024

Investigation and Consulting Activities

The Office of Internal Audit receives complaints of alleged wrongdoing, including suspected fraud, waste, and abuse. Since our last quarterly report to the Audit and Compliance Committee, we have received two (2) such complaints and have initiated an evaluation of the significance and credibility of said complaints. In addition, we have closed out five (5) other investigations that were ongoing at the time of our last update to the Audit and

⁴ This recommendation was subsequently implemented as of July 27, 2023.

Compliance Committee in June. Pursuant to governing regulations, we have informed the appropriate individuals about those complaints the Chief Audit Executive deemed to be significant and credible.

Our office continues to provide management advisory services and support to other University units through the OIA staff's participation in workgroups and advising on process improvement efforts.

Other Matters

Ms. Leslie-Ann Triana, who has been a professional staff member with the OIA for over a year as a Senior Auditor, was selected to fill the Audit Project Manager position. This leaves the number of vacancies in the office at two—a Senior Information Systems Auditor and Senior Auditor.