Office of Internal Audit

Audit of the Patricia & Phillip Frost Art Museum

Report No. 18/19-11

May 24, 2019

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: May 24, 2019

To: Jordana Pomeroy, Director Museum Operations

From: Trevor L. Williams, Chief Audit Executive

Subject: Audit of the Patricia & Phillip Frost Art Museum - Report No. 18/19-11

We have completed an audit of the Patricia & Phillip Frost Art Museum ("Museum") for the period July 1, 2017, through September 30, 2018, and an assessment of the Museum's current practices through February 2019. The primary objectives of the audit were to determine whether the Museum's procedures and controls ensured that: (a) the recordkeeping, safeguarding, and maintaining of the Museum's collection/inventory are adequate; (b) payroll and other expenditures are appropriate and adhere to University policies and procedures, and applicable laws, rules, and regulations; and (c) applicable information technology risks are mitigated.

The Museum's collection includes over 6,000 objects with a strong representation in the American and European printmaking from the 1960s and 1970s, Pre-Columbian objects, African art, photography, and a growing number of works by contemporary and Latin American artists. The Museum had $909,203 in revenues and $2,227,632 in expenditures for the fiscal year ended June 30, 2018. The net deficit was funded with approximately $1.5 million from the Educational & General Fund.

Our audit concluded that there has been improvement in controls over the Museum's Collection records since our previous audit. However, opportunities for improvement exist over operational and expenditure controls related to the Collection's safeguarding, payroll and personnel administration, expenditures, and the deaccessioning process. We also identified areas of information technology that need attention, particularly in identifying and mitigating risk, disabling local generically named administrator accounts, and removing inactive firewall rules that are no longer needed. The audit resulted in 23 recommendations, which management has agreed to implement.

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
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost, Executive Vice President, and Chief Operating Officer
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Vice President and Chief of Staff, Office of the President

TABLE OF CONTENTS

OBJECTIVES, SCOPE, AND METHODOLOGY

Pursuant to the approved annual plan for the 2018-2019 fiscal year, we have completed an audit of the Patricia & Phillip Frost Art Museum ("FAM" or "Museum") for the period July 1, 2017, through September 30, 2018, and an assessment of the current practices through February 2019. The objectives of our audit were to ensure that:

(a) Procedures and practices for the recordkeeping, safeguarding, and maintaining of the Museum's collection/inventory are adequate;
(b) Payroll and other expenditures are appropriate and adhere to University policies and procedures, and applicable laws, rules, and regulations; and
(c) Applicable information technology risks are mitigated.

The audit was conducted in conformance with the *International Standards for Professional Practice of Internal Auditing* and the *ISACA IS Audit and Assurance Standards*. The audit included tests of the accounting records and such other auditing procedures, as we considered necessary under the circumstances. The audit also included an assessment of internal controls over the Museum's operations. To accomplish specific Information Technology control objectives, we applied a governance, risk and compliance methodology, which utilizes the COBIT 5.0 Framework and the National Institute of Standards and Technology (NIST) Special Publications 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations Guidelines*. Audit fieldwork was conducted from October 2018 through February 2019.

During the audit, we:

- Tested the adequacy of the Museum's record-keeping system;
- Observed the Museum's procedures for protecting its art collection;
- Tested selected transactions against University policies and procedures and Florida Statutes;
- Analyzed the Museum's sources of revenues; and
- Evaluated the adequacy of the Museum's Information Systems Security, Identity Access Management, Network Security, and Business Continuity controls.

Sample sizes and transactions selected for testing were determined on a judgmental basis applying a non-statistical sampling methodology.

As part of our audit, we reviewed our internal audit, Report No. 13/14-12, Audit of the Patricia and Phillip Frost Art Museum, issued April 8, 2014, to determine the status of any applicable prior recommendations related to the scope and objectives of this audit. Any repeat audit findings from the prior audit are indicated throughout this report.

BACKGROUND

Housed on the Modesto A. Maidique Campus of Florida International University ("FIU"), The Frost Art Museum (formerly The Art Museum at FIU) opened in 1977. Following the groundbreaking for its new facilities in 2003, The Art Museum at FIU was officially renamed the Patricia & Phillip Frost Art Museum. The 46,000-square-foot facility opened in November 2008 and the Museum became an independent unit under the direct authority of the Provost.

Initially a relatively small gallery of less than 3,000 square feet, the Museum's programmatic growth during the 1980s and 1990s qualified the Museum for designation as a major cultural institution by both the State of Florida and Miami-Dade County. In 1999, the Museum received accreditation from the American Association of Museums (now the American Alliance of Museums) and reaccreditation in 2011, valid until 2026. In 2001, the Museum became an affiliate of the Smithsonian Institution.

The Museum's mission is to provide transformative experiences through art; collect, exhibit, and interpret art across cultures; and advance FIU's stature as a top tier research university.

Collection

The Museum's Collection is governed by the Collections Management Policy and is composed of various Collections:

- Permanent Collection
    - The General Collection and Sculpture Park – Over 6,000 objects that include American printmaking from the 1960s and 1970s, photography, Pre-Columbian objects dating from 200 B.C. to 500 A.D, and a growing number of artworks from contemporary Caribbean and Latin American artists. A subset of the General Collection is the Sculpture Park (numerous sculptures installed throughout the landscape of the Modesto A. Maidique Campus).
    - The Metropolitan Museum and Art Center Collection – Over 2,500 objects that were donated to the Museum by the Metropolitan Museum of Art Center of Coral Gables.

- Study Collection
    - The Betty Laird Perry Student Art Collection – Composed of artworks obtained through purchase awards granted to selected Bachelor of Fine Arts (BFA) and Master of Fine Arts (MFA) students graduating from the program since 1980.
    - The Study Collection – This collection has related objects in the Permanent Collection, or those of lesser quality that contribute to the understanding and appreciation of the Permanent Collection. These objects can be used for hands-on teaching, demonstrations, study, or exhibition. Objects that have been designated as Study Collection may be disposed of through FIU's Property Control procedures.
- Other
    - Non-Collection Objects – The Non-Collection designation allowed the Museum to deaccession objects that did not merit the same standards of care as the Permanent Collection but that had value as office decoration. The Non-Collection designation is no longer in use. Objects designated as Non-Collection are considered property of FIU and may be disposed of through FIU's Property Control procedures.
    - The University Collection – With regard to acquired works, the Museum, at its discretion, determines whether the work is appropriate for accession into the Museum's Permanent Collection or Study Collection. In the event that a work of art is not appropriate for accession into the Museum's Permanent collection or is not useful as a Study Collection object, the work may be classified as part of the "University Collection." The Museum will maintain written and electronic records pertaining to these objects, but the responsibility for inventory, care, storage, and insurance of works of art within the University Collection rests with the University unit that maintains custody of the work of art.

    - Art in State Buildings – The Museum maintains the archives of the Art in State Buildings collection for collection objects installed in buildings throughout the campus. These works are commissioned and/or acquired through the State of Florida's Art in State Buildings program. The care of these objects and expenses related to their care are the responsibility of University Facilities and the appropriate building managers.

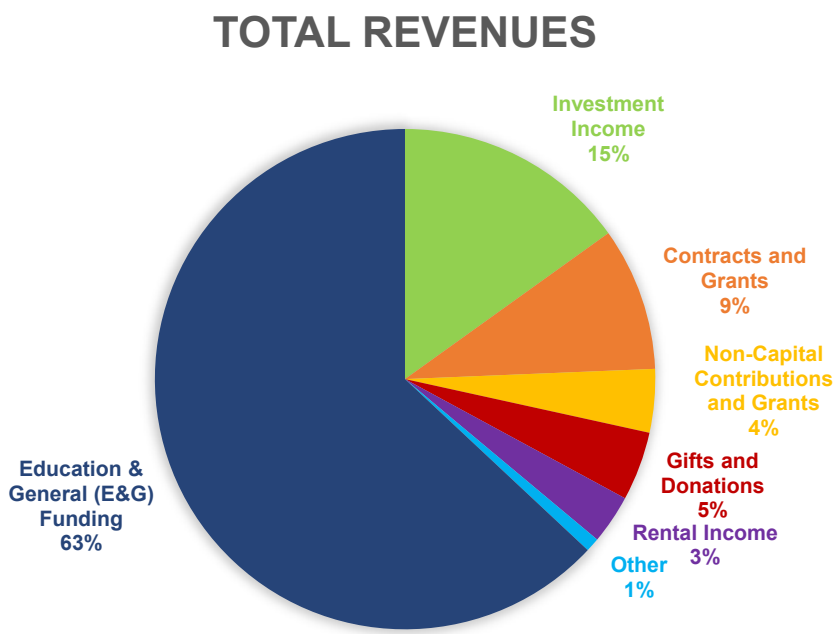
The Museum's Collection is insured for $19 million through the University's Facilities Assessment, Analysis, and Risk Management Department.

Financial Information

We identified 13 activity numbers and 22 Project IDs managed by FIU and the FIU Foundation related to the Museum's operations, totaling $909,203 in revenues and $2,227,632 in expenditures, subsequent to consolidation for the fiscal year ended June 30, 2018, their most recently completed fiscal year.

FIU Foundation accounts are used mostly for professional services related to art exhibitions. The FIU Foundation either pays vendors directly or processes transfers to the Museum (as reimbursements). In the latter scenario, expenses are originally recorded by the Museum and subsequently reimbursed through the FIU Foundation. These reimbursements are recorded as Non-Capital Contributions & Grants on the Museum's books when received and Transfers-out on the FIU Foundation's books when reimbursed. In the consolidated financial statement presented on page 5, $78,927 of such transactions were eliminated during the process of consolidation. However, $97,060 reimbursed by the FIU Foundation in 2017 (pertaining to 2016-17 transactions), were recorded by the Museum in 2017-18 as Non-Capital Contributions & Grants revenues, although the Museum had originally recorded the expense on its books in 2016-17.

The graph below depicts actual funding percentages, including $1,549,847 in Educational and General (E&G) funding.



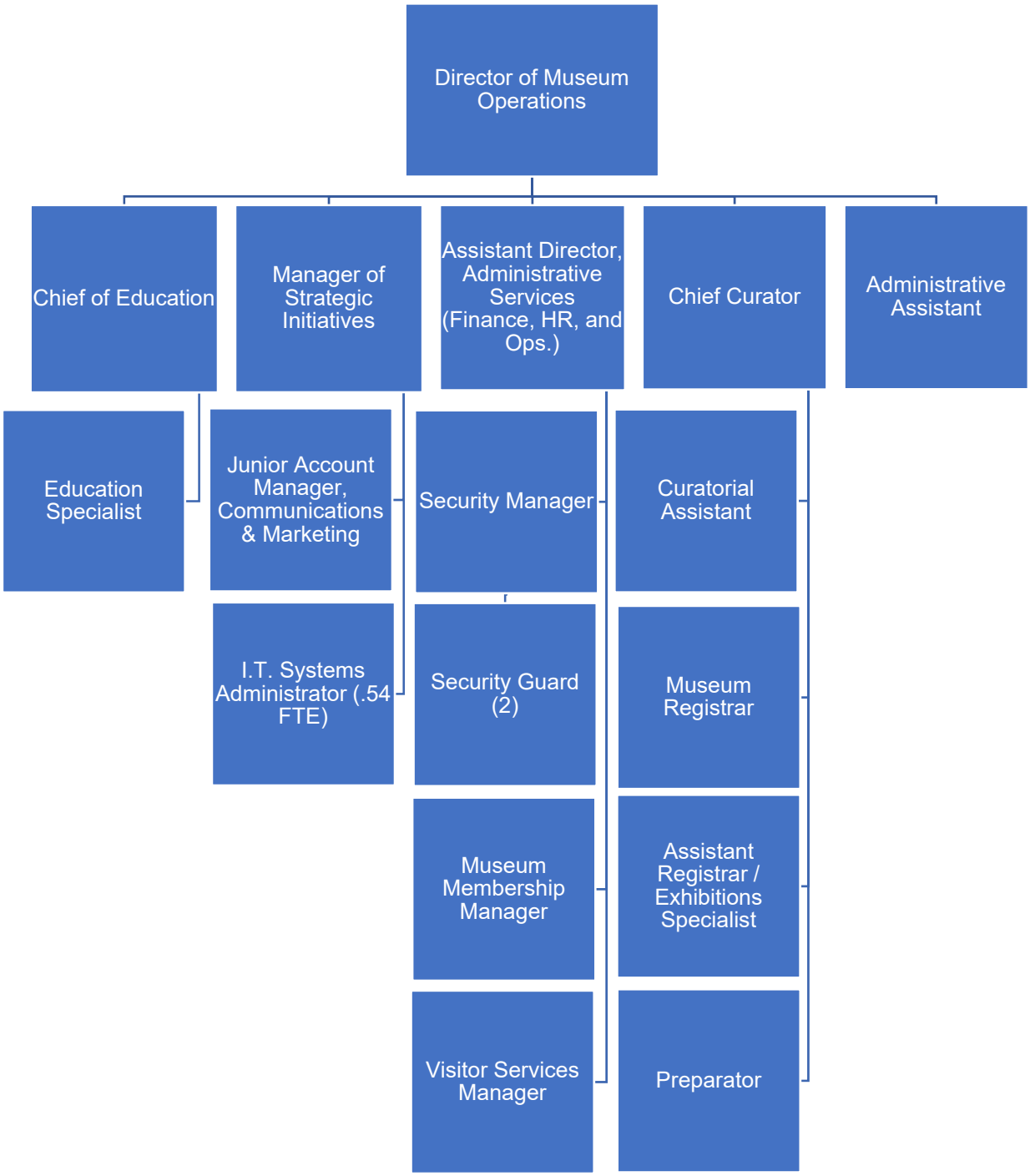
The Patricia and Phillip Frost Art Museum
Consolidated Results of Operations (Museum and FIU Foundation)
Fiscal Year Ended June 30, 2018

REVENUES:			
Endowment Investment Income (Restricted)		$ 371,042	41%
Contracts and Grants		227,589	25%
Gifts and Donations		109,746	12%
Non-Capital Contributions and Grants		100,735	11%
Rental Income		78,012	9%
Sale of Goods and Services		12,414	1%
Continuing Education Fees		6,830	1%
Private Revenue		2,835	-
Total Revenues		$ 909,203	100%
EXPENDITURES:			
Salaries & Benefits:			
Administrative Salaries	$ 786,379		
Fringe Benefits	346,049		
Staff Salaries	175,120		
Other Personnel Services	54,162		
Salaries – Overtime	4,793		
Cellphone and Miscellaneous Payroll Allowance	3,030		
Total Salaries & Benefits		$ 1,369,533	61%
Operating Expenditures:			
Professional Services	$ 483,707		22%
Other Operating Expenses	229,817		10%
Materials and Supplies	93,518		4%
Repairs and Maintenance	17,866		1%
Utilities	17,691		1%
Operating Capital Outlay	13,000		1%
Scholarships	2,500		-
Total Operating Expenditures		858,099	39%
Total Expenditures		$ 2,227,632	100%
Net Deficit funded from Educational & General Fund[1]		**$ (1,318,429)**	

[1] The Museum received approximately $1.5 million from Educational & General (E&G) funding.

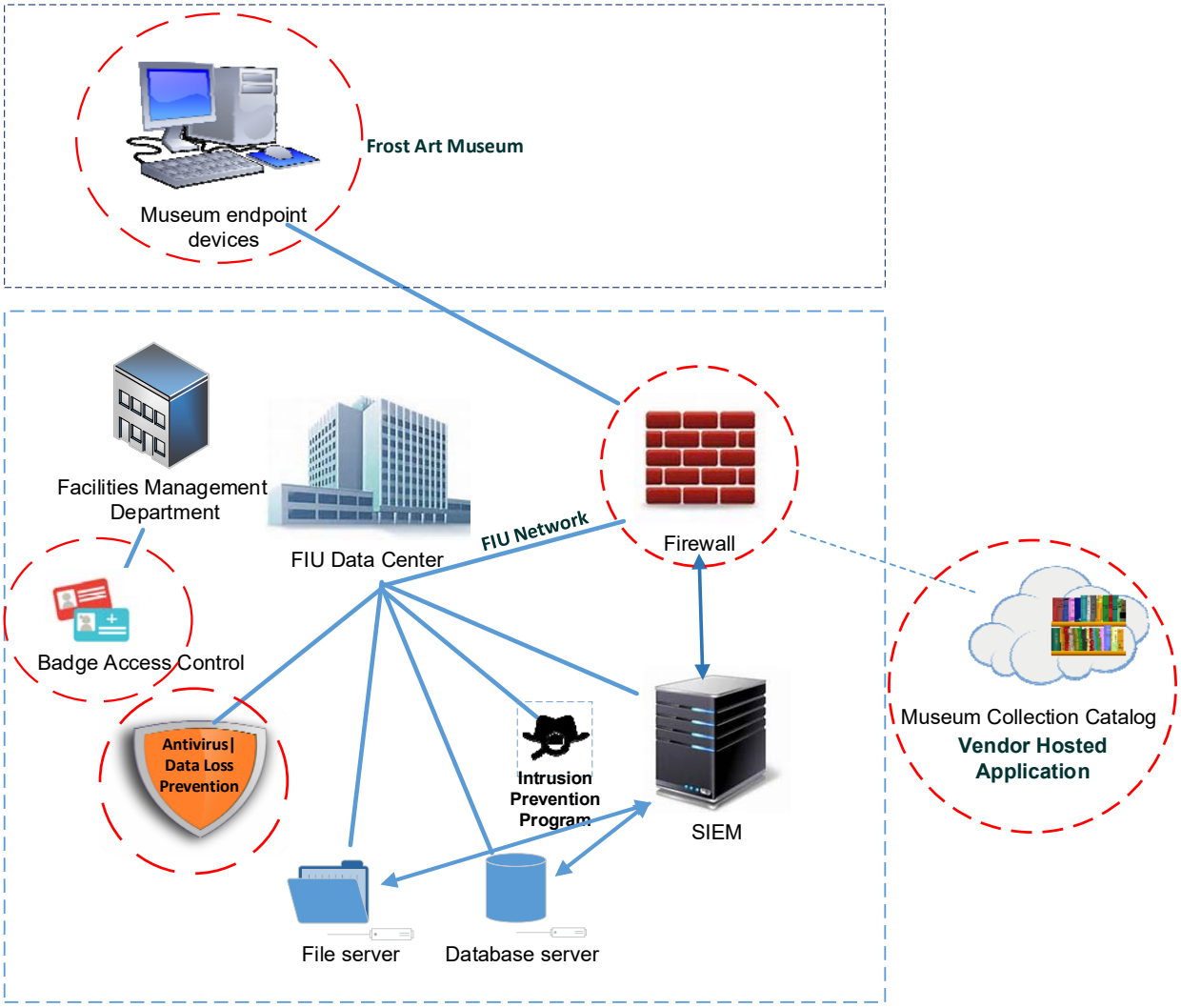
Personnel

As of April 15, 2019, the Museum had 18 permanent positions, organized as follows:



Information Systems

Information Technology tested included information systems, access, network, and business continuity controls related to the Museum and their recent implementation of the Collection and Catalog application. Areas highlighted in red represent controls that need improvement and are discussed in further detail in Section II Information Technology Controls.



OBSERVATIONS AND RECOMMENDATIONS

Our overall assessment of internal control is presented in the table below. In summary, we noted an improvement in controls over the Museum's Collection records since our previous audit. However, opportunities for improvement exist over operational and expenditure controls related to the Collection's safeguarding, payroll and personnel administration, expenditures, and the deaccessioning process. We also identified areas of information technology that need attention particularly in identifying and mitigating risk, disabling local generically named administrator accounts, and in removing inactive firewall rules that are no longer needed. Our observations and recommendations pertaining to these identified areas are detailed on the following pages of this report. We have also included management's response to our observations and recommendations, along with their implementation dates.

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**X**	
Policy & Procedures Compliance	**X**		
Effect		**X**	
Information Risk		**X**	
External Risk		**X**	
INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance	Non-compliance issues are minor	Non-compliance Issues may be systemic	Non-compliance issues are pervasive, significant, or have severe consequences
Effect	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk	Information systems are reliable	Data systems are mostly accurate but can be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk	None or low	Potential for damage	Severe risk of damage

SECTION I
Operational and Financial Controls

1. Safeguarding of the Collection

The Museum's *Collection Management Policy* states that, "It is FAM's responsibility to provide security and protection for its collections, traveling and temporary exhibitions, property, staff, and visitors." We evaluated the existing security mechanisms and processes in place at the Museum using the *Suggested Practices for Museum Collections Space* as adopted by the American Alliance of Museums. We concluded that other than the Fire Suppression System and the Panic Alarm, which we tested and found no exceptions, security controls over the collection and the collection records need strengthening, particularly in the following areas:

Surveillance Cameras

During our review of the Museum premises, we noted that the Museum had 57 surveillance cameras and all of the cameras were properly functioning. The *Suggested Practices for Museum Collections Space* indicates that for high-risk items[2], camera coverage requires:

- "Forensic Detail" coverage of everything exiting the space via fixed cameras;
- "Forensic Detail" coverage of all alarm points within the space via pan-tilt-zoom (PTZ) cameras; and
- "General Surveillance Detail" of at least 75% of the space via fixed or PTZ cameras.

However, we noted that none of the Museum's collection storage areas (rooms 206, 215, 408, and 410) or its collection records area (room 216) have cameras inside, which would provide general surveillance detail. Moreover, there are no cameras that capture the exterior spaces of the fourth floor storage rooms (rooms 408 and 410).

Access to the Collection Storage Space

The *Suggested Practices for Museum Collections Space* states that access to collections space shall be limited to the minimum number of staff whose official duties require frequent and regular access. Moreover, staff who do not require such access should not receive access and/or keys to the collections space.

[2] Items considered to be of sufficient value such that the impact of their unauthorized access, removal, theft, or damage would be highly detrimental to the image or reputation of the institution and could impact the mission of the museum.

During our review of the Museum premises, we noted:

- All security staff (two security guards and one security manager) may independently access the Collection storage areas; however, their job duties do not require frequent and regular access to these storage areas. The *Suggested Practices for Museum Security* states that when electronics are deemed adequate to protect Primary Collection Storage areas, it may not be necessary for security officers to actually enter the collection storage room except to check alarms. When practical, entry into collection storage by security officers should be a two-person assignment. During our background check testing on page 15, we noted that the one (1) sampled guard tested had access to the Collection, although a Level II screening was not performed as required per University Policy No. 1710.257 – *Background Check Requirements*;

- The *Suggested Practices for Museum Space Security* states that Museums should "avoid mixing any other functions such as general office space, work areas, or non-collection storage with collections spaces to limit access to collections." During our testing, we noted:

    - Storage room 410 is a shared storage room that contains collection and non-collection items. As such, other staff members (i.e., IT personnel) have access to this space. Additionally, this space is not equipped with an access card system or any other security mechanisms to track who enters and exits the room.

    - Collection records are stored in room 216, which is housed within room 215. However, the door to room 216 is left open, allowing individuals with access to the Collection in room 215, to also have access to all original collection records.

- Moreover, during our Collection Inventory testing, we noted three (3) Museum employees have system privileges in the Re:discovery Proficio ("Proficio") application to add and delete objects, in addition to having physical access to collection storage areas. Upon notification, this total has been reduced to one (1) Museum employee. There are no mitigating controls in place to reduce the risk caused by the lack of segregation of duties.

Security Guards

Per the Museum's *Collections Management Policy*, "Guards, front desk attendants, and gallery monitors shall be responsible for enforcing the security policies and procedures as it pertains to gallery visitors." During our tour of the Museum on December 19, 2018, we observed both of the on-duty security guards were distracted on their smartphones and not actively performing their patrolling duties. The Museum's security guards are provided with hand-held receivers (walkie-talkies) to communicate and therefore, cellphones are not required to

perform their job duties. We noted that there were visitors present in the Museum at the time. Upon us entering one of the galleries, the first guard stopped using his smartphone. However, the second guard remained on his smartphone for the remainder of our time in the gallery. We visited the Museum again on January 29, 2019, and noted that the same guard who had been distracted on his smartphone during our first visit, was again distracted on his smartphone. Museum management informed us there had been previous disciplinary issues with the guard. We were subsequently informed by Employee and Labor Relations that this employee resigned on March 7, 2019. If security guards are distracted, it could negatively affect their ability to enforce the Museum's security policies and procedures.

Climate Control

Per the Museum's *Climate Control Guidelines*, "The temperature in the galleries and storage should be maintained at 68-72 degrees Fahrenheit and the Relative Humidity maintained at 45-55 percent." However, we reviewed these two parameters for 14 areas within the Museum during varying one- and two-month periods and noted that the temperature for seven (7) of the 14 areas routinely exceeded 72 degrees Fahrenheit. Furthermore, we noted that for 13 of the 14 areas, the relative humidity levels routinely exceeded 55%.

If the Collection is not adequately safeguarded, valuable pieces can be removed without detection or items may be damaged.

Recommendations

The Museum should:	
1.1	Install additional surveillance cameras in high-risk areas of the Museum not currently monitored to ensure adequate coverage of the Collection.
1.2	Limit access to the Collection and collection records to staff members whose duties require frequent access.
1.3	Implement a compensating control for the employee who has access to both Proficio and the Collection to reduce the associated risk.
1.4	Implement a policy for security guards which addresses cellphone usage.
1.5	Work with Facilities Management to ensure that temperature and relative humidity levels for the galleries and collection storage areas adhere to the Museum's Climate Control Guidelines.

Management Response/Action Plan:

1.1 The Assistant Director of Administrative Services and the Security Manager met with FIU Work Management as well as their electrical contractor to discuss installation of cameras in and outside of the vaults located on the 2nd and 4th floors of the Museum. The Museum's Chief Curator provided valuable input to the discussion. Cameras will be installed in multiple locations within those floors and will be in line with the adopted AAM suggested practices.

Implementation date: July 2019

1.2 The Museum will continue to ensure that only necessary curatorial and security staff have access to storage areas. An analysis was conducted of existing employee access. Management has determined that security staff must have access to these areas in order to ensure full safety measures are followed during a time of emergency.

Implementation date: Immediately

1.3 The access to both collections storage and the ability to delete records in Proficio is only allowed for the Chief Registrar. The Chief Curator met with the Museum's IT Systems Administrator to remove the Chief Registrar's ability to delete records, but were unable do so. The Chief Curator has reached out to Proficio to see if they can make this adjustment on their side. The Chief Registrar has the ability to add files; however, as a mitigating control, the Chief Curator will be reviewing items that have been added/edited, on a bi-weekly basis. The Chief Curator will then sign off on said review.

Implementation date: Immediately

1.4 Unless there is an emergency or pertinent matters, security guards are verbally instructed not to view content or use cellphones while visitors are in the galleries. The Security Manual will be updated to reflect this policy. Security staff will receive a document that must be signed stating that they acknowledge said policy.

Implementation date: Immediately

1.5 HOBO (hygrothermograph dataloggers) readings are taken daily and any issues/concerns are addressed with FIU Facilities Management. When galleries or storage areas are noted to be too hot, too cold, too humid, etc., current HOBO readings are reported to the Security Manager, who then advises Facilities Management. If the climate has not been corrected by the following day, the issue is escalated to the Director of Physical Plant. All members of the curatorial staff are responsive in reporting climate issues and the staff is dependent upon Facilities Management to provide corrective action. Going forward, the curatorial team will look at the forthcoming week’s weather forecast to troubleshoot when temperatures will spike, in order to anticipate climate control fluctuations.

Implementation date: Immediately

2. Payroll and Personnel Administration

Payroll Time Approval

Payroll and fringe benefits represent 61% of the Museum's consolidated expenditures. We reviewed 100% of the 3,079 payroll entries, representing all of the employees' hours worked and leave taken during the fiscal year 2017-2018 and noted an opportunity for continued improvement.

Per the University's Payroll & Compensation procedures, Managers/Proxies should have first-hand knowledge of the employee's hours reported, or should obtain written confirmation from the employee's supervisor of the hours being reported. All employees time/leave entries must be signed off by the managers by 2:00 p.m. on the Monday of pay week. Otherwise, the Payroll Department automatically approves the entries. Managers should avoid delegating time approval to a direct report. If there is a need to delegate such authority, either of the following steps can be taken:

- The proxy prints the employee's time card and has the supervisor sign indicating approval of hours reported. This type of approval should be maintained in the time approvers file for audit records;

- The supervisor emails the proxy indicating approval of hours reported. This type of approval should be maintained in the proxy's file for audit records.

We noted some instances in which time was not properly approved. This was also an observation in our prior audit. Specifically, we noted that time was:

- Approved directly by the Payroll Department without approval from Museum personnel (235 entries – 8%). There were 83 (3%) such entries during the previous audit;

- Self-approved by two (2) employees, without written support for supervisory approval (23 entries – less than 1%). No such finding in the previous audit;

- Approved en masse by the Museum's HR Liaison without written support (22 entries – less than 1%). No such finding in the previous audit; and

- Approved by others[3] without written support from the employee's supervisor (16 entries – less than 1%). No such finding in the previous audit.

Not properly approving payroll may result in employees being compensated for work not performed and/or failure to properly record leave.

[3] Someone from within the Museum, but not a supervisor, HR Liaison, or delegate.

Outside Activity/Conflict of Interest Disclosures

According to Employee and Labor Relations (ELR) procedures, the Outside Activity/Conflict of Interest reporting requirement must be completed by all FIU faculty and staff members on an annual basis, regardless of whether or not the employee has an activity to report.

We noted that none of the 15 employees active at the 2017-2018 fiscal year end or the 16 employees currently active had completed an Outside Activity/Conflict of Interest disclosure. The Report of Outside Activity Form ensures that conflicts of interests are appropriately addressed by the University. By reporting outside activity, employees help to ensure that FIU's academic, research, and administrative affairs are conducted with the utmost integrity and in compliance with all legal requirements.

Failing to identify conflicts of interest may result in the University's primary objectives being influenced by secondary interests.

Background Checks

University Policy No. 1710.257, *Background Check Requirements*, requires Level II[4] background screenings for museum employees and positions with unrestricted access to a Great Grand Master Key. Employees are required to obtain this clearance prior to employment at the Museum.

We selected 11 employees and noted that for six (6), Level II screenings were not conducted.

As noted in University Policy No. 1710.257, if appropriate background screenings are not performed, the University may expose itself to "hiring individuals with a proven tendency to defraud or steal from their employers, who engage in workplace violence, or who otherwise appear to be untrustworthy and unreliable".

Terminations

For the period audited, there were nine (9) employees who were terminated or transferred out of the Museum. We noted that the employment statuses for two (2) of these individuals was not timely updated within PantherSoft. These employees had temporary positions and reported to different supervisors. The employees were "terminated" in PantherSoft 70 and 134 days, respectively, after separation from the Museum.

[4] A Level I background screening consisting of a search for any criminal information at the federal, state and county levels on an individual within the last seven (7) years. The Level II criminal background investigation requires fingerprinting that searches the Florida Department of Law Enforcement and the Federal Bureau of Investigation database in addition to the Level I search.

Failing to timely terminate employees within PantherSoft, exposes the University to additional risks, such as allowing separated employees continued access to the building and University systems. (See page 29, subsection 7 - Least Privileged Access.)

Recommendations

The Museum should:	
2.1	Ensure that the University's payroll approval process is adhered to.
2.2	Ensure that all Museum personnel complete the Outside Activity/Conflict of Interest Form annually.
2.3	Work with Human Resources to ensure that all relevant employees obtain the required Level II screenings.
2.4	Timely notify Human Resources of employee terminations.

Management Response/Action Plan:

2.1 Email reminders are sent by the Assistant Director of Administrative Services at the end of every pay period for time submission as well as on the Monday of pay week for time approval by 2pm. This practice will continue indefinitely. Going forward, delegated proxies will use email for time approval.

Implementation date: Immediately

2.2 Although this is the responsibility of each individual employee and managers are not notified if forms have been completed, going forward, administration will implement an acknowledgement/attestation document from each employee to ensure completion and compliance with this requirement. This document shall be completed at the end of each fiscal year. The Assistant Director of Administrative Services will also reach out to Employee & Labor Relations to obtain current completion status of all employees.

Implementation date: Immediately

2.3 The Assistant Director of Administrative Services will request confirmation notification from Human Resources that incoming employees have completed Level II screenings. Employees that do not currently have Level II screenings will have to complete this request. The Museum will contact Human Resources to complete this task.

Implementation date: June 2019

2.4 The Assistant Director of Administrative Services will submit all employee termination documentation to Human Resources in a timely manner (within one week of employee's separation).

Implementation date: Immediately

3. Expenditure Controls

The Museum had 13 associated activity numbers and 22 project IDs at the FIU Foundation, totaling $2,227,632 in expenditures for the fiscal year ended June 30, 2018. Of these expenditures, $858,099 (39%) were related to non-payroll transactions. We obtained a listing of the detailed expenditures incurred during the audit period and judgmentally selected a sample of 74 non-payroll transactions, totaling $316,561, to determine whether expenditures were appropriate, properly authorized, adequately supported, properly recorded in the University's accounting records, and were in compliance with University policies and applicable laws and regulations.

Credit Card Expenses

We reviewed all 430 credit card transactions totaling $175,995 for proper approvals. We determined there was not proper internal control approval structure between the initiating and the approving of transactions. Specifically, we noted that the Visitor Services Manager approved 69 (80%) her superior's (Assistant Director Administrative Services) credit card transactions, totaling $16,794. Proper accounting controls would require the Assistant Director's transactions to be approved by her supervisor and not by a subordinate.

Other Expenses

We reviewed 31 other (not including travel, credit card, or payroll related) expenditures, totaling $257,880. During our review of these expenditures, we noted the following:

- Six (6) transactions, totaling $51,485, in which goods/services were received by the same individual who requested the purchase. These are two incompatible functions that should be separated to maintain proper internal control. Lack of segregation of duties when purchasing and receiving items increases the risk of the University incurring inappropriate charges.

Additionally, there were other inconsequential matters that came to our attention pertaining to travel-related expenditures that were discussed with Museum management for their follow-up.

Recommendation

The Museum should ensure that:	
3.1	The approval of credit card transactions and receipt of purchases for goods/services is performed using proper internal controls.

Management Response/Action Plan:

3.1 Credit card approvers were updated in August of 2018. Going forward, credit card approvers will be updated in a timely manner to ensure proper internal controls are being followed. The Museum has implemented an additional mitigating control for tangible items: a physical sign-off sheet that will be kept with the requisition. For services received, we will be requesting written confirmation from respective individuals, instead of just verbal confirmation.

Implementation date: Immediately

4. Property Control

Florida *Board of Governors Regulation 9.002* states, “All tangible personal property with a value or cost of $5,000 or more and having a projected useful life of one year or more shall be recorded in the financial system as property for inventory purposes.” FIU Asset Management provided us with a listing of the Museum’s capital assets. As of December 3, 2018, the Museum had 170 capital assets, with associated costs totaling $3,391,925. We noted that all items were observed by Asset Management within the last year. However, we noted that $2.4 million (58%) of collection objects with appraised values of $5,000 or more were not recorded by Asset Management. *This was also an observation in our prior audit.*

In addition, the Museum maintains attractive items which are defined as University property costing less than the threshold amount of $5,000, but which are particularly vulnerable to theft and misuse. The University’s *Property Control Manual* states that, attractive items, “should be marked as University property and catalogued by the user department.” As of October 18, 2018, the Museum had 78 listed attractive items. These items are used throughout the Museum and serve different areas and purposes.

We selected a sample of 15 items from the attractive property log to validate their existence. We noted seven (7) instances in which the actual location of items did not match their locations on the log. Additionally, we selected ten (10) items from the Museum and traced them to the attractive property log. We noted one (1) instance in which a laptop under $5,000 was not included in the attractive property listing. However, upon notifying the Museum of this discrepancy, the item was subsequently added to the log.

Inadequate tracking of property may result in theft or misuse of items without detection.

Recommendations

The Museum should:	
4.1	Further analyze their object collection valuation and work with Asset Management to ensure that all collection objects appraised for $5,000 or more, are properly recorded.
4.2	Ensure that all attractive property costing less than $5,000, be maintained and timely updated on the attractive property log.

Management Response/Action Plan:

4.1 The Chief Registrar will research the list, make a "notes" column describing actions needed for the object and make copies of appraisals for submission to Asset Management. The Chief Registrar has sent an email with questions to the Director of Gift Services in Advancement and Property Control for the proper actions to rectify the list. Going forward, Property Control/Asset Management will be contacted for any object that is either purchased or received as a gift-in-kind and is appraised at over $5,000.

Implementation date: August 2019

4.2 All attractive property costing less than $5,000 will be maintained and updated in a timely manner (within one week of procurement) within the attractive property log.

Implementation date: Immediately

5. Collection Inventory

The Museum's collection includes over 6,000 objects with a strong representation in American and European printmaking from the 1960s and 1970s, Pre-Columbian objects, African art, photography, and a growing number of works by contemporary and Latin American artists. The Museum utilizes the Proficio application to catalog and track collection items. The Museum's Permanent Collection is stored on the second and fourth floors of the main building.

Physical Inventory

The Museum currently conducts section-by-section rolling inventories on an annual basis, covering 10%-15% of its Permanent Collection. This process involves locating the objects, noting their condition, and updating their location in the management database. However, in observing the performance of the physical inventory, we noted that there is a lack of segregation of duties. The tasks of physically counting the collection objects and inputting the inventory (along with any changes) into the Proficio application are performed by one individual.

Deaccessions

The Museum has established standard policies and procedures on disposing and deaccessioning objects. According to said Policy, "Deaccessioning of collections shall only take place if it is determined that the item(s) are no longer appropriate for Permanent Collection and/or for the purposes of strengthening and improving the collection." This Policy, however, does not state who has authority to approve deaccessions or provide thresholds for approving deaccessions.

The American Alliance of Museums Standards state that one of the roles of a museum's governing authority is to ensure that policies are articulated and that prudent oversight is practiced.

During 2017 and 2018, the Museum deaccessioned 106 items. We selected a sample of 10 objects with deaccessioned prefixes and validated that deaccession forms were completed for all 10 items. However, neither of the checkboxes ("Approve" or "Disapprove") on the signed forms were marked to indicate if the deaccessions were approved or not. Additionally, notating the deaccessioned status of an item in the system is not always done in a timely manner. We noted two (2) objects were approved for deaccession on November 9, 2017, and May 24, 2018, respectively, but as of March 6, 2019, had not been marked as deaccessioned within Proficio.

Collection Documentation

The American Alliance of Museums Standards requires that museums have a system of documentation, records management, and inventory in effect to describe each object and its acquisition, current condition and location, and movement into, out of, and within the museum.

We tested a total of 60 collection items to validate their existence and to determine if items were properly accounted for. Other than an inconsequential error, all collection items were found without exception and were properly accounted for.

Recommendations

The Museum should:	
5.1	Document within its Policy the approvals required to deaccession objects.
5.2	Ensure that Deaccession Forms are properly completed, approved, and that objects are timely updated within the Proficio application.

Management Response/Action Plan:

5.1 The Deaccessions Policy will be updated to define the approvals needed for deaccessions. The Chief Curator will work with the Museum Director to propose, and document objects within the Museum's collection for deaccessions that will ultimately be approved by the Museum Director. Any object that is valued over $25,000 should also be approved by the University Provost.

Implementation date: August 2019

5.2 The Chief Registrar will complete outstanding deaccession items within Proficio database. Going forward, deaccessions will be updated within Proficio database in a timely manner, ideally within a week of decision about object.

Implementation date: June 2019

SECTION II
Information Technology Controls

6. Information Systems Security

Information Systems Security includes implementing and maintaining preventive, detective, and corrective measures, such as installing up-to-date security patches and virus definitions on endpoint devices, for example laptops and desktops that connect to the Museum network to protect them from malware and unauthorized disclosure of sensitive data.

Physical Surrounding

Based on the IT control principles found at COBIT DSS05.05, the Museum should restrict access to sensitive IT devices. We tested 11 computers and found that three (3) were physically located in a locked office and eight (8) were in cubicles separated from the public by a locked entryway. The Museum adequately positioned the computers tested away from the public's access and/or view.

The physical surroundings adequately protected the endpoint devices tested from unauthorized access of unattended workstations and limited the ability of unauthorized persons to view sensitive information.

Media Sanitization Process

According to the *Media Sanitation Guidelines*, the Information Security Department must ensure that sensitive information has been removed from equipment selected for disposal, donation, or recycling. For the Frost Art Museum's surplus devices, the Assistant Director of Administrative Services contacts the Division of IT either through a call or by completing the online *Property Control Request for Surplus / Pick-up of Equipment* form ("Form"). The Museum adequately maintains a list of the devices sent to surplus. The provided Form for eight (8) devices matched their list of surplus devices.

Asset Management

According to Policy 1910.005, *Responsibilities for FIU Network and/or System Administrators*, the System Administrators shall maintain an asset report that includes the model, operating system, host name, primary user, and the system's primary function. The IT Administrator provided an inventory list of 21 devices that included the host name, computer, and assigned user's name. Missing from the device list were the operating system and primary function. Without the information, the Division of IT is unable to determine what security controls to implement.

In addition, Policy 1910.005 requires departments' IT administrator to send a quarterly report to the Division of Information Technology of any systems implementation or changes to the IT environment. We noted that the Museum did not include five (5) computers on its inventory list and that all of the devices were not risk rated. Discussed in Report No. 15/16-02, Audit of University's IT Network Security Controls, risk rated inventory lists allow the Division of IT to better assess

the adequacy of network security controls for these devices. A report from the Museum, which categorizes the risk of each device allows the Division of IT to focus their efforts on high-risk devices and thereby increase the effectiveness of the University's cybersecurity controls.

Malware Prevention

Malware is defined as software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. According to FIU Procedure 1930.020c, the Division of IT will control the distribution of anti-virus definition files, operating system updates, and hard drive encryption. In our testing, we noted that the Division of IT controlled and implemented antivirus on all of the 11 devices tested.

Updates and Patches

We tested for unpatched vulnerabilities, which allow malicious code entry points into the network. Using a vendor based security analysis tool, we found that two (2) of the 11 selected endpoint devices tested were missing critical security updates. Upon notification, the IT Administrator uninstalled the vulnerable applications from the devices to eliminate the continued threat.

We also asked the Division of IT to examine the selected devices for the implementation of the hard drive encryption module. Of the 11 devices examined, they reported that nine (9) of the laptops' hard drives were unencrypted. Unencrypted laptops increase the risk of unauthorized access to stored data in the event the device is lost or stolen.

Risk Assessment

COBIT 5 AP010.04 *Analyze Risk*, requires organizations to complete a risk assessment. As such, the Museum should develop IT risk scenarios to support risk decisions that take into account the business relevance of the risk factors. According to the Museum's IT Systems Administrator, the Division of IT has not conducted a formal risk assessment of the information systems used to support the Museum's critical operations. By not performing a formal IT risk assessment, Management is unable to determine effectiveness of their existing data security controls.

Recommendations

The Museum should:	
6.1	Risk rate the computer inventory list.
6.2	Work with the Division of IT's Network Systems Security Engineering to ensure the devices are properly encrypted and connected to the Data Loss Prevention module.
6.3	Work with the Division of IT to conduct a formal risk assessment of the Museum's information systems.

Management Response/Action Plan:

6.1 The Museum will work with the Division of IT to risk rate the computer inventory list.

Implementation date: July 2019

6.2 The Museum will work with the Division of IT to ensure all computers are encrypted and connected to the Data Loss Prevention module.

Implementation date: June 2019

6.3 The Museum will work with the Division of IT to conduct a formal risk assessment.

Implementation date: October 2019

7. Identity Access Management

The Identity Access Management Controls reviewed included policies, procedures, least privileged access, segregation of duties, and unique identification. According to the NIST SP800-53A (Rev. 4) AC 2.1, *Account Management*, user identity, and logical access should be managed to ensure that all accounts are appropriately established, modified, and disabled in a timely manner.

Access Control Policies and Procedures

In October 2018, the Museum switched to the Proficio hosted system. The Profico onboarding, detailed below, was a semiformal process to give their users access.

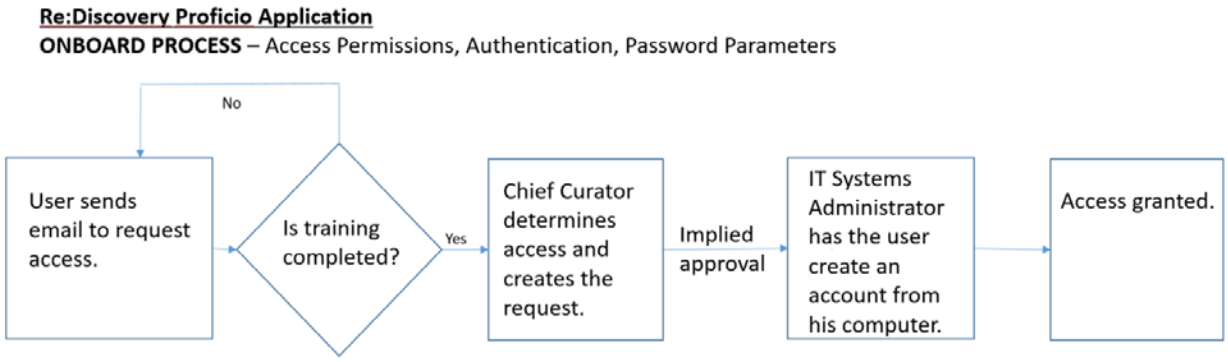


FIGURE 1- PROFICIO ONBOARD PROCESS

In the original process, users had more access than necessary and the informal request made it difficult to ensure access was appropriate. Upon our discussion, the Museum created on-board and off-board access forms that detail the date of the request and the reason. Going forward, the Museum needs to complete the forms to ensure access is appropriate. Since the Museum has recently implemented the Proficio application, it did not have any off-boarded users.

We also examined door access to the Museum and found that one student maintained access to the external and internal entry doors for 95 days after her termination. By not disabling access in a timely manner, especially for student workers, it increases the risk of unauthorized access since they retain their ID cards after termination. Upon our notification, the student's access was disabled. We also examined log reports provided by the Facilities Management Department. There was no evidence that the student assistant accessed the Museum after her termination.

Application Log Controls

Audit logs are chronological records of security-relevant data that document the sequence of activities affecting an operation, procedure, event, file, or document. Log reports are available for the Proficio application, external entry, such as the loading dock, stairwells, and specific internal areas.

Currently, the Proficio application only tracks user's login and logout activity. The application does not have an audit trail option available at this time to record user activity. According to the vendor, they are in the process of developing a feature to address the security gap.

Through our inquiry, we learned that Assistant Director, who is in charge of maintaining door access, did not receive log reports from the Facilities Management Department. Without logs, the Museum reduces its ability to detect anomalies.

Uniquely Identified Users

According to FIU Policy No. 1930.020a, *Data Stewardship*, all highly sensitive data must be accessed by way of a unique name for identifying and tracking user identity.

Our review found that two (2) of the 13 user names for the Proficio application were not a uniquely identifiable user account. One was a test account and the other a vendor account with full access and editing permissions. According to the Director, the accounts were only for troubleshooting and are now deleted. In addition, 10 of the 11 workstations scanned had a generically named local administrator user account. The account gives unrestricted access to the computer and may be used by anyone who knows the username and password. On average, the accounts have not been used in 179 days and should be disabled, where appropriate, to reduce the risk of unauthorized access.

Least Privileged Access

The COBIT 5 DSS06.03.03 control objective of least privileged user access is to allow authorized users only the access that is necessary to accomplish assigned tasks in accordance with their business functions. We examined the user accounts in Proficio and found that the Administrative Assistant, Curatorial Assistant, and the temporary Digitization Coordinator had the ability to remove and loan out museum inventory, which did not align with their job duties. Upon our notification, their access privileges were adequately reduced. Additionally, we also examined badge access within the Museum and found that a total of 294 University employees had access to some or all of the Collection storage areas (room 206, 215, and 408). Aside from Frost employees (13) and University Police (72) who had access to these areas, it appears that the remainder of these employees (209) did not require such access. We noted one (1) College of Business Technology employee that separated from the University on March 7, 2018, but as of October 17, 2018 (the date of the badge access report provided), this employee still had badge access to the Collection storage areas.

Segregation of Duties

According to COBIT 5 DSS06.03, *Manage roles, responsibilities, access privileges and levels of authority*, organizations should allocate roles for sensitive activities so that there is a clear segregation of duties. Typical with new systems implementations, the Museum broadly granted access to get their users onto the application. We examined 13 Proficio user accounts and found that seven (7) users, including the Archivist (an independent contractor), Curatorial Assistant, Museum Registrar, Assistant Registrar, the vendor, the temporary Digitization Coordinator, and a generic user account, had administrator access. With their access, the users have the ability to bypass the applications controls, including the creation of user accounts, mass changes to data, and deletion of records. Upon our notification, access was reduced so that only the Museum Registrar has administrator privileges. She is a backup to the IT Systems Administrator, in the event he is unable to perform his duties.

Recommendations

The Museum should:	
7.1	Complete the on-boarding forms for all Proficio users.
7.2	Perform formal log reviews on a periodic basis.
7.3	Perform an analysis of individuals with badge access to Collection storage areas and ensure that access is limited to employees with a job-specific need.
7.4	Disable local generic administrator access where appropriate.

Management Response/Action Plan:

7.1 The onboarding forms for all existing users will be completed by the Chief Curator.

Implementation date: Immediately

7.2 The Museum will continue to work with the vendor in developing the application's audit trails capability. Once completed, the Chief Curator will work with the Chief Registrar and the Systems Administrator to periodically check the application’s log files.

Implementation date: September 2019

7.3 The Museum will work with the individual departments to disable or reduce badge access.

Implementation date: July 2019

7.4 The Assistant Director of Administrative Services will work with the Systems Administrator to further deactivate administrator accounts.

Implementation date: Immediately

8. Network Security

Network Security includes defining and protecting internal and external boundaries and limiting access points through the use of firewalls and intrusion protection systems. Firewall rules should be approved with supporting documentation.

Internal and External Boundaries

Firewalls and routers are key components of the architecture that controls entry across the Museum's network. Based on the network information provided by the Division of IT, the Museum's data is adequately segregated through the use of firewalls and an Intrusion Protection System.

Monitoring Access Points

The Division of IT provides a layered security approach for monitoring access points, which includes log reviews, vulnerability scans, and data loss prevention reports. The Security Information and Event Management (SIEM) system monitors connected devices' log files and provides real-time situational awareness to identify malicious activity. The Division of IT informed us that the database server connects to the SIEM but not the file server. Upon our notification, the Museum's IT Administrator connected the McAfee EPO (ePolicy Orchestrator) agent and now the file server log files are reviewed by the SIEM.

The Division of IT performs vulnerability scans on a bi-weekly basis to identify potential attack vectors. We examined scans for the last six months to determine if the Museum reviews the reports and mitigating plans implemented for critical vulnerabilities. We identified a recurring critical vulnerability related to an application that is no longer supported by the vendor. Stated in the vulnerability report, the lack of support implies that there are no new security patches released by the vendor and as a result, it is likely to contain security vulnerabilities. The report also states that the solution is to upgrade to a version supported by the vendor. Upon our notification, the Chief Curator contacted the Division of IT and they plan to upgrade the software at the end of June to adequately mitigate the security vulnerability.

An additional layer of monitoring is through the review of Data Loss Protection reports that provide alerts of the potential of unauthorized distribution of sensitive data. We examined reports from May 5, 2018, through September 14, 2018, and noted that there were no alerts reported. The reports provide the Museum an opportunity to check specific files and determine whether sensitive data is properly protected. We found that 10 devices were disconnected to Data Loss Prevention, thereby reducing the effectiveness of the reports.

Data Flow Traffic

Based on the control principle of NIST sp800-53A (Rev. 4) SC-7(4) *Boundary Protection*, the Museum should document each exception to the traffic flow policy

with a supporting mission and/or business need and the duration of that need. According to the Division of IT, the Museum sent two network requests during the audit period. The requests did indicate the business need and duration.

In addition, we examined eight (8) ingress and 13 egress rules pertaining to the Database and File Servers, respectively. Three (3) ingress rules from the File server were questionable due to the rules allowing unencrypted File Transfer Protocol (FTP) and access throughout the campus. A similar FTP observation was noted in our prior audit. The Division of IT promptly disabled the FTP connection and determined that the other two (2) rules were necessary for the Museum's operations.

We asked the Division of IT to run a zero hit count for all Museum firewall rules to determine which ones are actively in use. The results showed that in the last 155 days, the Museum did not use any of the museum's eight (8) ingress rules and only two (2) of the 25 egress rules. Identified in the previous audit, the Museum's IT System Administrator should review firewall rules to ensure they are appropriate. Over time, the rules became outdated and no longer needed. Inactive firewall connections that are no longer needed provide unnecessary potential entry points for network attacks.

Security Awareness Training

The University offers a comprehensive Cybersecurity Awareness Training to all employees in order to protect the organization and address the multitude of vulnerabilities day-to-day employee activities create.

In 2018, the Division of IT launched Cybersecurity Awareness Training program Version II with a completion date of January 29, 2019, for all FIU employees.

As of February 25, 2019, 23 of the 32 Museum staff have successfully completed training, two (2) are in progress, and seven (7) are assigned. Upon our notification, Management informed us that two (2) have completed training and four (4) no longer work for the Museum. The due date to complete the training for two (2) of the three (3) remaining employees is May 31, 2019, with the last employee's due date being August 10, 2019.

Recommendation

The Museum should:	
8.1	Work with the Division of IT to review and document the firewall rules, and disable outdated rules.

Management Response/Action Plan:

8.1 The Museum will document reviews and work with the Division of IT to disable outdated firewall rules.

Implementation date: July 2019

9. Business Continuity

The purpose of Business Continuity is to establish and maintain a plan to respond to incidents and disruptions in order to continue operations of critical business processes at a level acceptable to the Museum. The information systems that are critical to the daily operations highlight the need for periodic review and test of internal and external disaster recovery plans to ensure the confidentiality, integrity, and availability of the applications' information system data.

Planning

Last updated on January 4, 2019, the Museum's Emergency/Disaster Preparedness & Recovery Plan ("Plan") assists personnel in recovering collections from events ranging from a minor emergency to a major disaster. Each group member is responsible for specific actions required in preparing, securing, and post-emergency recovery operations of the Museum. The Plan adequately addresses its purpose, scope, disaster team roles, and responsibilities; coordination among different entities; and recovery procedures. We also noted that the Plan was properly updated to include the Proficio system.

Business Continuity Plan Testing

Tabletop exercises allow testing of the Plan without disrupting operations. The Chief Curator confirmed that the Museum conducted tabletop exercises on February 11, 2019. Though no formal minutes were recorded, she did provide acknowledgement receipts signed by 16 employees and an overview of Lessons Learned from Disaster Plan Training. We did note that Proficio was not included in the exercise.

To ensure the adequacy of the vendor's internal controls, we requested a Service Organization Controls Type 2 (SOC 2) report for the vendor be provided. We learned that the Museum did not obtain or review a copy of a SOC 2 report as part of its data transition process from the Museum Plus application located in the FIU Data Center. Upon further discussion, the Chief Curator was able to obtain a copy of the SOC 2 report for the platform where Proficio resides. The provided SOC 2 report did not note any exceptions during its testing of the Business Continuity Management & Operational Resilience, Business Continuity Planning section.

Since there is an increased impact to the Museum's operations, the Museum should include the Proficio hosted application in their tabletop exercise to ensure continued operations in the event of a disaster.

Recommendation

The Museum should:	
9.1	Include the Proficio application in testing, and document the results, and corrective actions taken during the tabletop exercise.

Management Response/Action Plan:

9.1 The Museum updated its business continuity criteria to include the Proficio application in next year's test.

Implementation date: Immediately

Definition of Internal Auditing

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.