FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of The Wolfsonian-FIU Museum

Report No. 17/18-09

April 23, 2018

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

MEMORANDUM

DATE: April 23, 2018

TO: Tim Rodgers, Director Museum Operations

FROM: Allen Vann, Chief Audit Executive

SUBJECT: Audit of The Wolfsonian-FIU Museum, Report No. 17/18-09

We have completed an audit of The Wolfsonian-FIU Museum (Museum) for the year ended June 30, 2017. The primary objectives of our audit were to ensure that: (a) the collection is properly maintained and accounted for; (b) financial controls are functioning as intended; and (c) Information Technology risks are mitigated.

The Museum currently oversees the Mitchell Wolfson, Jr. collection of over 180,000 objects of art and rare books dating from the late nineteenth to the mid-twentieth century. The Museum had $3.8 million in revenues and $6.7 million in expenditures. It received approximately $2 million from Educational & General (E&G) funding and $1 million from an Academic Affairs loan to fund the deficit.

Our audit disclosed that as was the case during our last audit, the Objects Collection is partially stored in the Museum's Annex, which has not been adequately maintained placing the Collection at risk. Otherwise, process controls and compliance with policy and procedures were generally followed. Nevertheless, opportunities for improvement exist over operational and expenditures controls related to Collections inventory and access, Museum Gift Shop operations, payroll and personnel administration, and controls over expenditures. We also identified Information Technology areas that need attention particularly in identifying high-risk devices, patch management, performing risk assessments, enabling and reviewing audit logs, reducing user access privileges, firewall rule reviews, and business continuity plan. The audit resulted in 30 recommendations, which management 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 and Chief Operating Officer
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President
Robert Grillo, Vice President of Information Technology and CIO

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan for 2016-2017, we have completed an audit of the Wolfsonian-FIU Museum ("Museum") for the period from July 1, 2016 through June 30, 2017. The objectives of our audit were to ensure that:

(a) Collection/inventory procedures and records are adequate;
(b) The collection is properly maintained and safeguarded;
(c) Payroll and other expenditures are appropriate;
(d) Auxiliary operations revenue collection procedures are handled properly; and
(e) Information Technology risks are mitigated.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing,* and included tests of the accounting records and such other auditing procedures, as we considered necessary under the circumstances. To accomplish specific Information Technology (IT) control objectives, we applied a governance, risk and compliance framework, which utilizes the *Control Objectives for Information and Related Technology (COBIT) 5.0 Framework and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, Revision 4 (Rev. 4) - Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. Audit fieldwork was conducted from September 2017 through January 2018.

As part of our audit, we reviewed internal and external audit reports issued during the last three years to determine whether there were any prior recommendations related to the scope and objectives of this audit and whether management had effectively addressed prior audit concerns. Although no such reports were found, our Office did issue an audit report in April 2013, Report No. 12/13-11, Audit of the Wolfsonian-FIU Museum, which recommendations within our current scope were reviewed as part of this audit. We have highlighted within the Operational and Financial Controls section of this report any recommendations that are repeat audit findings. In the Information Technology Controls section, all prior audit recommendations were reviewed and reported on.

BACKGROUND

The Wolfsonian, Inc., a Florida not-for-profit corporation, and f/k/a The Wolfsonian Foundation, Inc., was established in 1986 to create and operate a museum and research center in Miami Beach, Florida, and to support a comprehensive program focused on the collections, exhibition, interpretation, preservation, research and publication of the decorative, design and architectural arts. Effective July 1, 1997, the Florida International University Foundation, Inc. ("FIU Foundation") and the University entered into a gift agreement with Mitchell Wolfson, Jr. and The Wolfsonian, Inc., whereby Mr. Wolfson Jr. agreed to donate all title and interest in and to all objects constituting "The Mitchell Wolfson, Jr. Collection of Decorative and Propaganda Arts," and The Wolfsonian, Inc., donated its assets, including 1001 Washington Avenue, subject to certain terms and conditions.

As a result of the gift agreement, The Wolfsonian, Inc. amended its articles of incorporation and bylaws to provide that all of its directors be appointed and removed at any time with or without cause by the FIU Foundation, with the intention to effect a transfer of complete control of the assets, interests and obligations of The Wolfsonian, Inc. to the FIU Foundation. After the gift agreement, the operation of the museum, formally operated by The Wolfsonian, Inc., became an academic unit of the University reporting directly to the Provost, and is referred to as the "Wolfsonian-FIU", hereinafter "Museum". Subsequent to implementing the gift agreement, employees of The Wolfsonian, Inc. became University employees.

The Museum currently oversees the Mitchell Wolfson, Jr. collection of over 180,000 objects of art and rare books dating from the late nineteenth to the mid-twentieth century. Through a series of academic study and fellowship programs, national and international traveling exhibitions, and scholarly initiatives, the Museum promotes public education and awareness of the social, historical, technological, political, economic, and artistic material culture of Europe and America in the 1890-1950 period.

The Museum was accredited by the American Alliance of Museums (AAM) (formerly the American Association of Museums) in 2006 for a period of ten years, which has since been extended through 2020.

In March 2004, the University completed the purchase of a previously leased warehouse known as the Annex for $892,000, less $132,250 in rent credits previously paid for by the Museum. A significant portion of the art collection is stored at the Annex. It was noted in the prior Audit (Report No. 12/13-11), that this structure did not appear to be adequately maintained (i.e., wall cracking, deteriorating exterior, and water intrusion). As a result, the Museum is currently working on finding a new storage space and relocating items stored in the Annex to a space with more favorable conditions. The Museum is also in the process of finding a lessee for the Annex building and adjacent parking lot.

In July 2013, Mr. Wolfson donated his Downtown Miami office condominium and the collection housed within (approximately 25,000 items) to FIU. In October 2016, the Museum sold this downtown space for $1.8 million; a portion of the sale proceeds were used to move the 25,000 collection items to the Annex and a third-party storage space. The Museum plans to use the remaining funds ($1 million) to develop a master plan for the Museum's remodel and to relocate the Collection storage off Miami Beach. The results of the sale were excluded from the consolidated financials presented herein for audit purposes.

To assist in its capital funding needs, $982,019 was loaned to the Museum from Academic Affairs during the current audit period. The loan agreement carries a 1% interest rate that will not be capitalized until pay-down begins in 2021 with interest totaling $54,817. Principal and interest yearly payments are $103,684 and are due from 2021 through 2030.

Large volumes of the Museum's expenditures are reimbursed from its funds managed at the FIU Foundation, including all non-grant travel and departmental card expenses. As such, these expenses are originally recorded by the Museum and subsequently reimbursed through the FIU Foundation. The reimbursement is recorded as DSO Non-Operating Revenues in the Museum's books and as a Transfers-Out in the FIU Foundation's books. At any given time, there could be a one-month's lag in expenditure reimbursement from the FIU Foundation. At June 30, 2017, the Museum had recorded $1.66 million in revenue reimbursements, which is presented in the consolidated financial statements herein, along with the FIU Foundation's corresponding transfers-out expenditures.

We identified 48 activity/project numbers managed by the Museum, including those at the FIU Foundation, totaling $3,834,365 in revenues and $6,744,399 in expenditures, subsequent to consolidation, for the fiscal year ended June 30, 2017.

Wolfsonian-FIU Museum
Consolidated Results of Operations (Museum & FIU Foundation)
Fiscal Year Ended June 30, 2017

REVENUES:			
DSO Non-Operating Revenues	$	1,662,005	43%
Contracts & Grants		842,356	22%
Gifts and Donations		673,607	18%
Transfers-In		335,505	9%
Sale of Goods – Gift Shop & Café		177,003	5%
Ticket Sales		115,750	3%
Rental Income		16,345	-
Sale of Services		8,760	-
Other Operating Revenues		3,034	-
Total Revenues	$	3,834,365	100%
EXPENDITURES:			
Salaries & Benefits:			
Administrative Salaries	$	2,329,640	62%
Fringe Benefits		914,606	25%
Staff Salaries		317,876	9%
Other Personnel Services		147,645	4%
Salaries - Overtime		17,064	-
Cellphone & Misc. Payroll Allowance		8,529	-
Total Salaries & Benefits	$	3,735,360	100%
Operating Expenditures:			
Transfers-Out	$	1,618,236	54%
Professional Services/Officials		350,757	12%
Miscellaneous		234,068	8%
F&E under $5,000		135,037	4%
Materials and Supplies		112,273	4%
Other Equipment and Supplies		95,401	3%
Purchases for Resale – Gift Shop & Café		92,849	3%
Telephone Equipment		61,227	2%
Rental of Buildings		49,294	2%
Insurance		48,531	2%
Advertising/Promotion		48,396	2%
Postage		44,908	1%
Travel		36,780	1%
Shared Services Fee		27,735	1%
Repairs and Maintenance		24,635	1%
Administrative Overheard		15,966	-
Legal Fees & Services		9,110	-
Purchased Utilities		3,836	-
Total Operating Expenditures	$	3,009,039	100%
Total Expenditures	$	6,744,399	
Net Deficit funded from FIU General Fund and Academic Affairs Loan[1]	**$**	**(2,910,034)**	

[1] The Museum received $2.1 million from Educational & General (E&G) funding and $982,019 from the Academic Affairs loan.

Personnel

As of September 2017, the Museum had 54 employees, organized as follows:

* Temporarily assigned to Associate Director, Curatorial & Education.
** Temporarily assigned to the Deputy Director, Business Affairs.

Systems

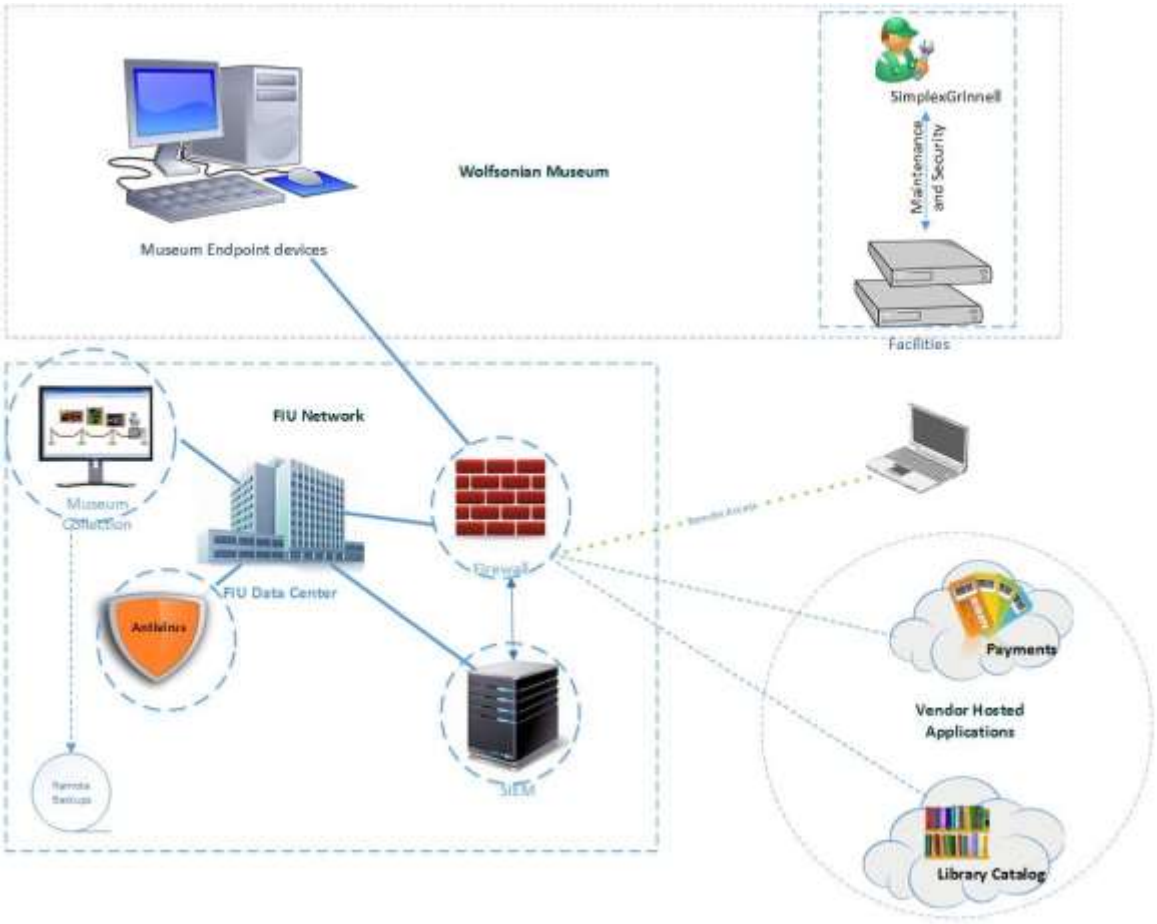
The Museum's workstations are connected to the Museum Network, which is connected to the FIU Network. The Museum currently utilizes the following information systems:

- Re:discovery Proficio to catalog the Objects Collection. This system is hosted in the FIU data center.

- EOS (web-based) to catalog the Library Collection. This system is hosted remotely by Quality Technology Services (QTS).

- ALTRU (web-based) for retail management, events and ticketing. This system is hosted remotely by the vendor.

- CCURE by Simplex Grinnell for the Museum's facility security system. This system is on a stand-alone server and is not connected to any network. All server maintenance is provided by the vendor, Simplex Grinnell.



FINDINGS AND RECOMMENDATIONS

As previously reported, the Objects Collection is partially stored in the Museum's Annex, which has not been adequately maintained placing the Collection at risk. Otherwise, process controls and compliance with policy and procedures were generally followed. Nevertheless, opportunities for improvement exist over operational and expenditures controls related to Collections inventory and access, Museum Gift Shop operations, payroll and personnel administration, and controls over expenditures. We also identified Information Technology areas that need attention particularly in identifying high-risk devices, patch management, performing risk assessments, enabling and reviewing audit logs, reducing user access privileges, firewall rule reviews, and business continuity plan.

Our overall evaluation of internal controls is summarized in the following table.

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	Instances of non-compliance are evident	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 need to be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk	None or low	Moderate	High

SECTION I
Operational and Financial Controls

Detailed below are the areas identified by our audit testing where opportunities for improvement exist.

1. Collection Inventory

The Museum has approximately 180,000 objects, which range from the period of 1890 to 1950. These pieces make up the Objects Collection, as well as the Library Collection.

The Re:discovery Proficio database is used to catalog and track the Objects Collection. The Objects Collection is stored in the main museum building's fourth floor storage room, but the vast majority is stored at the Annex. As previously noted in the prior audit, the Annex had the same deteriorating conditions. The Annex building did not appear to be adequately maintained (i.e., wall cracking, deteriorating exterior, and water intrusion). The Museum is in the process of finding a lessee for the Annex building and adjacent parking lot. They are also currently working on finding a new storage space and relocating items stored in the Annex to a space with more favorable conditions.

The EOS database is used for cataloging and tracking the Library Collection. The Library's collection is stored in the main museum building's third floor library space.

Objects and Library Inventory

We tested 100 art collection objects in the Re:discovery Proficio database to validate their existence. The objects were located both at the main museum building and at the Annex. For the most part all objects were found without exception. However, during our testing we noted the following:

- The location of one object was not updated within the Re:discovery Proficio database, after the object had been moved. The movement was recorded in the transfer paperwork on August 24, 2016; however, as of our testing date (November 9, 2017), this transfer had not been recorded within the database. *[There was a similar finding in the prior audit.]*

- One object was not tagged with its respective accession number[2]. Museum staff informed us that the object lost its identification tag and has since been retagged.

[2] A unique number given to each new acquisition entered in the Museum's database system.

- One object was recorded twice, with distinct accession numbers, within the Re:discovery Proficio database. Per discussion with Museum staff, the object was originally purchased framed in 1988. Between 1988 and 1990, the original accession number became disassociated from the object possibly when it was unframed. Thus, when it was "found in collection" in 1990 it was given an "XX" "found in collection" accession number. The two object records have since been reconciled to represent the one original object. *[There was a similar finding in the prior audit.]*

Additionally, we tested 25 library items in the EOS database to validate their existence. During our review, we noted that there were 4 missing objects, which were all subsequently located by Library personnel.

The American Alliance of Museums Standards require 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.

A formalized inventory process is not being performed for either the Objects or Library Collections. *[This was also a finding in the prior audit.]* Museum management stated that inventory is indirectly performed as items are pulled for an exhibit.

If items are not properly recorded, timely tracked, or inventoried, valuable collection pieces may go missing without detection.

Recommendations

The Museum should:	
1.1	Timely record the movement of all collection objects and library items within the corresponding information system.
1.2	Ascertain that all objects are recorded and affixed with a unique accession number.
1.3	Routinely perform a physical inventory of the Objects and Library Collections.

Management Response/Action Plan:

1.1 Management will incorporate policies and procedures for the documentation and entry of all movement of collection objects. This policy will include provisions for timely unit-level audit reports and reviews to confirm compliance with policies and procedures by the deputy director or designee.

Implementation Date: June 2018

1.2 Management will review the current label and tag identification procedures to identify opportunities for improvement of policy, procedures, and operations.

This issue will be mitigated by implementation of improved collection inventory policies and procedures and the implementation of improvements to museum security operations.

Implementation Date: December 2018

1.3 The physical inventory of 180,000 objects and books is a major undertaking requiring significant human and fiscal resources. Management will review and revise inventory control policies and procedures to incorporate and implement monthly “cycle counts” into operation.

Implementation Date: June 2018

The preparation for the potential relocation of the museum collection as part of the realization of The Wolfsonian’s long-term plans will allow for large-scale “cycle counts” of all collection items. The implementation of the “cycle counts” will be complete by June 2018; the estimated completion for large-scale “cycle-counts” is December 2022.

Implementation Date: December 2022

2. Access to Collection and Collection Records

The *Suggested Practices for Museum Collections Space*, as adopted by the American Alliance of Museums, 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. The Suggested Practices indicate that for high-risk items ("items are 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"), 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.

The security over the art collection and the collection records need strengthening. During our review of the Museum premises, we noted:

- There were six employees with storage space access (Annex and fourth floor storage room). Storage spaces are used to house objects not on display. The aforementioned six employees also have user access rights to edit and/or add and delete inventory records. *[This was also a finding in the prior audit.]*
- Collection storage areas (Annex and fourth floor storage room) did not have surveillance camera coverage throughout. Museum staff informed us that this is primarily due to budget constraints.
- Original collection records were accessible to all employees with second floor access, instead of being restricted to Registrar personnel.

If the Collection is not adequately secured, valuable pieces can be removed without detection or identification of who was responsible for the removal.

Recommendations

The Museum should:	
2.1	Implement adequate surveillance camera coverage of the Collection.
2.2	Implement mitigating or dual controls to reduce the risk caused by the lack of proper segregation of duties.

2.3	Limit access to the Collection and collection records to staff members whose duties require frequent access.

Management Response/Action Plan:

2.1 Management initiated the installation of Annex surveillance equipment by FIU Technology Services in October 2017. Full implementation of the surveillance equipment is conditional to the completion of integration of the access control and surveillance systems into the FIU IT Network (See Recommendation 7.1 and associated Management Response). Management will also be reviewing the deployment and improvements of the surveillance and access control systems.

Implementation Date: December 2018

Effective March 19, 2018, a contract guard is on stationary post at the Annex to monitor entry and exit of staff and visitors, check all packages and bags, and be present for the opening and closing of the building. This mitigating action will remain in place until the Annex phase of implementation and integration of the access control and surveillance system is complete.

2.2 Management will review application software capabilities, business policies, and processes to identify opportunities to implement dual control or design mitigating controls within collection operations or museum security operations to reduce risk due to issues with segregation of duties.

Implementation Date: December 2018

2.3 Management will revise the overall access matrix for all museum staff as part of the overall expansion and improvement of the deployment and operations of the access control and surveillance systems. Business processes and operations will be revised to ensure access to original collection records is limited and secure.

Implementation Date: December 2018

3. Museum Shop

The Museum's Gift Shop (Shop) is located on the first floor of the Museum. The Shop contains exhibit-related items that are priced up to $2,750. Shop management informed us that a significant portion of high-valued inventory was obtained under the direction of the previous Museum Director; however, since then, the Museum has enhanced its offerings with lower-priced items. As of June 30, 2017, inventory on hand was approximately $925,000 (at retail value). The Shop uses the ALTRU software for tracking inventory and processing sales and purchases.

Inventory Count

We selected 35 Museum Shop items for testing: 25 from the inventory report and 10 from the floor. During our review, we noted five exceptions (retail value totaling $1,005), ranging in count differences from one to five. *[This was also a finding in the prior audit.]* We noted the following factors, which may have contributed to these differences:

- Not all inventory within the Shop is stickered or tagged with existing SKUs (stock keeping units);

- Some inventory is held in the Senior Retail Manager's office. It appears that the door to the office remains open throughout the day, leaving items accessible to all Museum staff;

- The Shop stores inventory in the main museum building and at the Annex; however, the log maintained by the Shop to account for items between both locations does not appear to be periodically updated to reflect current inventory.

If Shop inventory is not properly accounted for, items may be unknowingly removed, resulting in a loss of revenue.

Physical Inventory

On an annual basis, the Museum Shop performs a physical inventory of all items. We reviewed the most recent physical inventory completed in May 2017 and noted the following:

- The Physical Count Worksheet was not signed by the employee(s) who performed the physical inventory;
- Upon discussion with the Museum staff, it was determined the physical inventory was performed by Shop staff (Visitor Associate) and discrepancies were later reviewed and adjusted for by the Shop Manager. We noted that the Visitor

Associate and the Shop Manager have access to the inventory and the ALTRU system.

To achieve segregation of duties, the normal job activities of the person performing the physical count should not include custodial activities.

Without a comprehensive physical inventory process, the Shop is vulnerable to inaccurate inventory counts, which may ultimately affect the Shop's merchandising decisions. Moreover, inventory shrinkage problems caused by loss, damage, and theft may go undetected.

Inventory Turnover

The Museum Shop has not established a formalized process for reviewing inventory aging. We acknowledge that the Museum Shop has reduced the quantity of aged inventory since the prior audit; however, this reduction in aging inventory was achieved by a key Shop employee that had knowledge of when these items were purchased. The ALTRU system does not list the specific dates of when inventory was purchased. Museum management informed us that ALTRU does not have this capability.

Without a formalized inventory aging process, the Shop may experience inventory obsolescence and financial losses.

Financial Performance

The Museum Shop generated revenues of approximately $159,000, which resulted in a net loss of approximately $41,000 for the year ended June 30, 2017. An analysis of net income (loss) for the last five years reflects that the Museum Shop has generated losses in all five years (2013 – 2017) totaling approximately $143,000. *[This was also a finding in the prior audit.]*

Furthermore, as noted in the previous audit, the GAAP matching principle (accrual basis accounting) is not followed; instead, cash basis accounting is applied due to the nature of the inventory. Therefore, cost of goods sold is recorded when inventory is purchased.

Finally, as an auxiliary operation, the Museum Shop should be managed as a self-supporting activity and should at minimum, produce break-even results. The Board of Governors' Rule 9.013, Auxiliary Operations, states, "These activities shall support the

educational endeavor of the institution and enhance its functioning; therefore, they shall not detract or distract from this basic endeavor in any way, financially or otherwise."

During our fieldwork, we noted that the Museum Shop had implemented different strategies (i.e., shift in merchandise price point strategy, installation of window display fixtures, aggressive promotional discounting of aging items) to improve the Shop's financial performance; however, the Shop's current efforts and plans to break-even have not been formally documented.

The Shop's negative operating performance may affect the Museum's ability to achieve its strategic plan.

Recommendations

The Museum should:	
3.1	Sticker/tag all Museum Shop inventory with SKUs to prevent selling items with incorrect SKUs. Otherwise, when items cannot be tagged, the Shop should implement a process to identify such objects (i.e., pictures of objects for the corresponding SKU in ALTRU).
3.2	Secure the Museum Shop inventory and limit its accessibility to designated Shop employees.
3.3	Implement an effective tracking mechanism to monitor Museum Shop inventory held at the Annex.
3.4	Have employees performing the physical inventory sign-off on the physical count worksheet, for added accountability.
3.5	Implement mitigating or dual controls (i.e., two-member team counts, blind counts) to reduce the risk caused by the lack of proper segregation of duties.
3.6	Establish a process for periodically monitoring and responding to aging inventory.
3.7	Formalize the Museum Shop's existing financial plan to break-even, including utilizing all available platforms.

Management Response/Action Plan:

3.1 Management will implement a solution to ensure that all museum shop merchandise is tagged, or if not tagged, that an alternate method of SKU identification exists.

Implementation Date: December 2018

3.2 Management will incorporate changes to access controls for the museum shop areas as part of the overall expansion and improvement of the deployment and operations of the access control and surveillance systems.

Implementation Date: December 2018

3.3 Management will review retail application capabilities, store operations, policies, and procedures to establish a comprehensive inventory control program to ensure accountability and accuracy of the museum store inventory. This program will include cycle counts, dual control accountably for inventory counts, and mitigating controls to ensure integrity of overall inventory data.

Implementation Date: December 2018

3.4 See Response to 3.3

3.5 See Response to 3.3

3.6 Management will formalize the business plan for the museum store, coffee bar, and admissions to generate and maintain an annual net profit. This plan will continue the current merchandising program, include an aggressive promotional pricing program, and address the tracking of aging inventory. In the future, management will work to develop new sales channels, platforms, and strategies.

Implementation Date: June 2018

3.7 See Response to 3.6

4. Payroll and Personnel Administration

Payroll and fringe benefits represent 73% of the Museum's consolidated expenditures, excluding Transfers-Out. We reviewed 5,124 entries, representing 100% of the employees' hours worked and leave taken for the $3.7 million in related expenditures for the fiscal year 2016-2017 and noted an opportunity for continued improvement.

Payroll Time Approval

The Museum's payroll approval process for fiscal year 2016-2017 was found to have materially improved since the prior audit; however, we still noted some instances in which time was not properly approved. *[This was also a finding in our prior audit.]* Specifically, we noted that time was:

- Approved directly by the Payroll Department without approval from Museum personnel (5% of all time entries);

- Approved en masse by the Museum's HR Liaison without written support (5% of all time entries);

- Self-approved by two employees, including one proxy, while written support for supervisory approval was not retained (1% of all time entries).

Per FIU's Human Resources Department, all employee 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. Additionally, Managers shall avoid delegating time approval to a direct report.

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

Employee Separation

Separation forms serve to ensure that terminated employees return all University property issued during their tenure and to settle all outstanding debts with the University prior to their last day or physical/logical access may not be revoked. We noted that separation forms were not completed for 3 (of 12) Museum employees which were terminated during the audit period. *[This was also a finding in the prior audit.]* (As noted in Finding No. 8, Identity Access Management – Access Control Policies and Procedures, we noted all 12 employees' access was adequately disabled.)

Per FIU's Human Resources Department, "The supervisor and employee must complete the *Separation from Employment/Transfer Clearance Form* on or before the effective date of separation. The form is completed online and printed, signed by the supervisor, and submitted to Employee and Labor Relations … for processing".

If separation forms are not completed, then University property held by departing employees may not be returned and physical/logical access may not be revoked.

Conflict of Interest

We noted that 35 (of 42) employees reviewed did not complete the Outside Activity/Conflict of Interest disclosures for 2016-2017. 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.

Per Employee and Labor Relations (ELR), the reporting requirement must be completed by all FIU faculty and staff members on an annual basis, regardless of whether or not employees have an activity to report.

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

Recommendations

The Museum should:	
4.1	Ensure that managers/supervisors timely approve the biweekly payroll for their direct reports. If a proxy is self-approving his/her time, the proxy should obtain written approval from his/her supervisor, prior to time submission.
4.2	Complete the Separation from Employment/Transfer Clearance Form for all departing employees.
4.3	Ensure that all Museum personnel complete the Report of Outside Activity Form annually.

Management Response/Action Plan:

4.1 Management will continue to remind and train all supervisors in the requirement to complete the approval of reported time and leave. Management will also reach out to FIU payroll and other HR liaisons to discuss best practices and explore other solutions to improve performance.

Implementation Date: Ongoing with substantial improvement by June 2018

4.2 Management will develop on- and off-boarding processes, including checklists, to ensure timely completion of all FIU and unit-level required actions.

Implementation Date: December 2018

4.3 Management has established an annual unit-level reminder to complete this reporting. Management will also work with FIU Human Resources to suggest improvements to this annual reporting process.

Implementation Date: Immediately

5. Expenditure Controls

The Museum has 48 activity/project numbers, including those at the FIU Foundation, totaling over $6.7 million in expenditures. Of these, $1.6 million represented Transfers-Out, mostly for FIU Foundation reimbursements. The balance of $5.1 million represented operating expenses, including $3.7 million related to payroll and fringe benefits.

We tested approximately 69% of all non-payroll related operating expenditures (88 transactions, totaling approximately $954,487). The results were as follows:

Travel Expenses

We reviewed 14 travel-related expenditures (four Expense Reports), totaling $5,919, and noted:

- Nine instances (two Expense Reports), totaling $2,298, in which expenditures were not adequately documented; the Travel Authorization (TA) was only submitted for $10 when all the expenses were to be paid out-of-pocket. All anticipated travel expenses should be included in the TA in order to encumber such amounts.

- Four instances (two Expense Reports), totaling $3,621, in which Expense Reports were not submitted on time. These two Expense Reports were submitted 40 and 110 days after the completion of the trip. [*There was a similar finding in the prior audit.*] Per FIU's Travel Manual, 'after returning from a trip or incurring an expense, reimbursement is made by completing an Expense Report with accompanying receipts. The Expense Report must be submitted within ten (10) days after the completion of the trip or incurrence of the expense'.

  For one of the aforementioned Expense Reports, we also noted two instances, totaling $2,655, in which expenses were paid to non-employees and the proper documentation was not completed. Per FIU's Travel Manual, 'travel reimbursement for non-employees is made via a *Reimbursement of Travel Expenses for Non-Employees Payment Form*, in addition to an Expense Report created on behalf of the non-employee'.

Other Expenses

We reviewed 39 other expenditures, totaling $874,790, and noted:

- Three instances in which overtime, totaling $2,130, was paid without prior approval to contracted Security Officers; however, per the state contract, *'Security Officers may not incur overtime unless authorized to do so by an Eligible User in writing prior to the provision of overtime services*'.

- One instance in which an expense for $10,000 was not properly allocated amongst the related activity numbers. This expense was for the final yearly installment of a three-year software license with Blackbaud for the ALTRU system, which is utilized by the Museum's Gift Shop, Café, facility rental, and Box Office areas. However, the entire expense was allocated to the Box Office. The Board of Governors' Rule 9.013, *Auxiliary Operations*, states, "*Each auxiliary service is an individual entity and shall be accounted for as such. A service may be operated by the institution or by a private contractor under the institution's supervision. Under either arrangement, all pertinent institutional revenues and costs shall be assigned to each auxiliary and the consequent financial results of operations determined.*"

- One instance in which an expense for $12,485 was not properly classified. *[This was also a finding in the prior audit.]* The expense was for the transportation of collection items housed in the Downtown Miami office condominium to a storage facility. This expense was classified as 'Rent of Buildings' instead of 'Professional Services'.

Credit Card Expenses

We reviewed 35 credit card expenditures, totaling $73,778, and noted that all transactions were processed in compliance with the University's Credit Card Policies and Procedures.

If the Museum's expenditures are not adequately documented, timely submitted, properly classified or allocated, then inappropriate expenses may be posted to the University's accounting records, resulting in non-compliance with University policies and procedures, as well as the potential for misuse of funds.

Recommendation

The Museum should:	
5.1	Ensure that all expenditures are fully documented, appropriately and timely submitted and approved, allowable, and properly classified and allocated.

Management Response/Action Plan:

5.1 Management will develop improved unit-level tools and training to ensure all managers are familiar with the proper policies and procedures related to travel expenses and other expenses.

Implementation Date: Ongoing but refresher training and improved policy materials planned for December 2018

6. Property

Asset Management provided us with a listing of the Museum's capital assets. As of November 29, 2017, the Museum had 58 capital assets, totaling $1,244,426. We noted that all items were observed by Asset Management within the last year.

In addition, the Museum also maintained attractive items which are defined as University property costing less than $5,000, but which are particularly vulnerable to theft and misuse. As of October 23, 2017, the Museum had 47 attractive items (composed of iPads and iPods). These devices are used throughout the Museum and serve different areas and purposes. During our review of attractive property, we noted:

- A record log of all attractive property is maintained by the IT Assistant Director; however, 4 of the 47 items on the log had incorrect 'home bases'. Additionally, we selected a sample of 10 items from the record log to validate existence. We noted that the names on the devices' settings for 2 of these items did not match with the name on the attractive property listing. We were able to identify these devices by their serial numbers. The device name listed within the settings is used to identify the given device and its intended use.

- The movement or tracking of attractive property is performed by distinct individuals, dependent on the nature of the devices. As of our review date, we noted 2 iPads were removed from the IT tracking log and this activity was not documented. Additionally, we noted that exhibition iPads were not being tracked by anyone or on any log.

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

Recommendations

The Museum should:	
6.1	Ensure that all attractive property is properly recorded.
6.2	Formalize procedures and designate specific employees for tracking all attractive property.

Management Response/Action Plan:

6.1 Management will incorporate policies and procedures for attractive property into the unit's comprehensive security policies, procedures, and operations.

Implementation Date: June 2018

6.2 See response to 6.1

SECTION II
Information Technology Controls

7. Information Systems Security

Information Systems Security includes preventive, detective and corrective measures, which are implemented and maintained (especially up-to-date security patches and virus definitions) on endpoint devices such as laptops and desktops that connect to the Museum network to protect them from malware and unauthorized disclosure of sensitive data.

Asset Management

As per NIST SP800-53A (Rev. 4) RA-2, *Security Categorization*, information systems lists should be categorized based on their likelihood and impact to the Museum operations in the event the devices become compromised. The IT Assistant Director provided the inventory list of 90 endpoint devices. Upon examination, we noted that the devices were not categorized and the Access Control and Surveillance Server was not included. According to the Deputy Director of Business Affairs, the server was not included because it was not connected to the Museum's Network. However going forward there are plans to attach it to the network and add it to the inventory list. Discussed in Report No. 15/16-02, Audit of University's IT Network Security Controls, asset lists allow the Division of IT to better assess the adequacy of network security controls for these devices.

In addition, FIU Policy 1910.005, *Responsibilities for FIU Network and/or System Administrator*, 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 found that a quarterly report was not provided to the Division of IT. A report from the Museum, which categorizes the risk of each device, will increase the effectiveness of the University's cybersecurity controls. The Museum was aware of the policy but unsure on how to report to the Division of IT. Discussed in Report No. 17/18-02, Audit of the University's IT Network Security Controls Follow-up, interviews with IT Administrators showed there was no formal guidance on how they can ensure the governance of policies in their department. Through an organization-wide effort, the Museum's inventory list should include risk categories and be reported to the Division of IT on a quarterly basis to increase the effectiveness of the Museum's asset management controls.

Malware Prevention

Malicious code, if undetected in endpoint devices, can be used by malware to disrupt computer operations, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user. According to FIU Procedure 1930.020c, *System and Application Management,* all FIU owned endpoint devices that connect to FIU's network must have anti-virus software running within 24 hours of their release. During our examination, we selected 10 endpoint devices based on the use of sensitive data. All 10 devices tested had the anti-virus satisfactorily installed prior to activation.

In addition, according to the aforementioned Procedure, the Division of IT will control the distribution of anti-virus definition files, operating system updates, and hard drive encryption. In order to accomplish this, the Division of IT must centrally manage the Museum's endpoint devices. According to the Network Engineering and Telecommunications Department, they managed 9 of the 10 devices tested. The one device not centrally managed was assigned to the IT Assistant Director. Upon discovery, the device was immediately added to the list of devices centrally managed by the Division of IT.

We also tested for unpatched vulnerabilities, which allow malicious code entry points into the network. Once on the network, malicious code can cause temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses relating to restoring systems and files, and potential harm to an organization's reputation. Using a vendor based security analysis tool, we found that 3 of 10 high risk endpoint devices tested were missing 2, 21, and 23 critical updates, respectively.

Endpoint devices that operate on the network with missing critical security updates increase the entry points of malicious code on to the network from these devices thereby reducing the overall effectiveness of the Museum/FIU's malicious code protection controls.

Conduct Risk Assessment

According to COBIT 5 APO12.02, *Analyze Risk,* the Museum should build and regularly update IT risk scenarios, including compound scenarios of cascading and/or coincidental threat types, and develop expectations for specific control activities, capabilities to detect, and other response measures. In November 2017, the PCI Compliance Team mandated that all departments that have FIU payment card devices must fill-out a Merchant Device Inventory Sheet and Tampering Checklist, as recommended in PCI-DSS Version 3.2's Requirement 9.9 *to protect devices that capture payment card data via direct physical interaction*. On a monthly basis, the Museum's IT Assistant Director checks all PCI devices for physical tampering and submits his results to the PCI Compliance Team. Based on an examination of the documentation provided, we determined that the Museum has not found any evidence of device tampering.

However, the Museum did not conduct any formal risk assessments of its IT environment. By not performing a formal risk assessment, the Museum reduces their ability to identify and mitigate the risk to the confidentiality, integrity and availability of the data in the Museum's information systems environment.

Recommendations

The Museum should:	
7.1	Work with the Division of IT on the security categorization of asset management list that will be reported on a quarterly basis and include the Access Control and Surveillance Server on the inventory list.
7.2	Ensure that the three endpoint devices' security updates are performed timely.
7.3	Continue to work with the FIU PCI Compliance Team to implement PCI compliant payment card readers and with the Division of IT to conduct a formal risk assessment of the Museum's information systems.

Management Response/Action Plan:

7.1 Management has initiated this process with Division of IT to incorporate the categorization of assets; implement a quarterly reporting process; and complete the integration of the access control and surveillance technology infrastructure into the FIU IT Network.

Implementation Date: December 2018

7.2 Management has completed the security updates on the three endpoints.

Implementation Date: Immediately

7.3 Management has implemented all required PCI Compliance protocols required to date. Management will continue to work with the PCI Compliance team and the Division of IT to realize full compliance of all application, hardware and risk assessments.

Implementation Date: June 2019

8. Identity Access Management

The Identity Access Management Controls reviewed included policies, procedures, least privileged access, segregation of duties, and unique identification. According to 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

According to the Museum's MBWC [Miami Beach Women's Club] Access and Key Control Policy - P&P 614, the Museum's Director or Deputy Director of Business Affairs must approve all badge access requests in writing. In an interview with the Museum's Deputy Director of Business Affairs, he explained their onboarding process as follows:

- The FIU Human Resources Department creates user account in PantherSoft;
- The hiring manager sends a request to the Museum's IT and application owner(s) to grant them badge access and access to applicable information system; and
- Once approved, the onboarding process is completed.

The Museum hired one employee during the audit period. An examination of the documentation provided to us showed that the Deputy Director approved the access request to the payment application. Additionally, the Museum formally approved the employee's badge access in writing and the access granted was consistent with the request provided.

In interviews with applications' administrators, we noted that when an employee separation occurs, access is removed on the day of the termination. During the audit period we identified that 12 employees were terminated from the Museum. In an examination of user access list provided by the Museum, we determined that all 12 terminated employees were adequately disabled from the applications.

Audit 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. One benefit of having audit logs is the ability to detect anomalies in system use. During our examination, we interviewed the system administrators to determine whether the applications had the capability of logging user activity and whether the data owners periodically reviewed the logs.

In our examination, we determined that the Access Control and Surveillance audit logs are reviewed as a detective control when an alarm has occurred. For the Payments application, the IT Assistant Director stated that the logs could be used regularly to generate reports to see role and permission changes of users as well as any changes to

revenue even after they have posted to the general ledger, such as changes to the revenue amount or its designations. However, the Museum does not presently use the functionality. Additionally, the Collection log files were deactivated at the time of our testing. Upon discovery, the Collection's log files were enabled. Lastly, the Library application does not have the ability to record user activity.

By not reviewing log files, the Museum increases the risk of inappropriate access; errors in the databases that can lead to items going missing without being detected; items not found when needed; and improper reporting results.

Unique 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. By assigning a unique identification (ID) to each user account, it ensures that individuals are accountable for their actions. We examined the user listings received for the four in-scope applications and found that there were five generic user accounts with administrator access: four were vendor support accounts, and one was used by a Museum employee.

Using a vendor based security analysis tool, we examined endpoint devices and found local generic administrator accounts for 2 of the 10 endpoint devices selected. After further examination, we found that one administrator account did not require a password to log in. We informed the Museum's IT Assistant Director and he removed the administrator access on both accounts.

Generic accounts, specifically with administrator privileges, reduces the information systems' ability to track individual user actions. Additionally, the user accounts could be used to bypass existing identity management controls. To reduce the risk of unauthorized access, vendor service accounts should only be active when the vendor is servicing the system and the employee should use a uniquely identified account.

Least Privilege

The COBIT 5 DSS06.03.03 control objective of least privileged user access is to allow authorized users access only that is necessary to accomplish assigned tasks in accordance with their business functions. During our examination of the user listings received for the in-scope applications, we found five users within the Museum Collections application that had Global Administrator access. We asked the Museum Chief Registrar whether their access was appropriate and she informed us that three of the users needed Administrator access to the application based on their current functions. The other two however, did not need this level of access and they immediately modified their security permissions accordingly.

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. The Museum's Objects Collection, Library Collection, and Gift Shop inventory controls are maintained through the three applications currently used. During our examination of the user listings provided, we noted the following exceptions:

- In the Museum's Objects Collection application, 4 of 14 user accounts have the ability to modify users access privileges and included the Chief Registrar, IT Assistant Director, and the vendor support accounts.
- The Museum's Chief Librarian who approves access to the Library application is also the application's administrator. He is the only user with access to modify user access rights.
- For the Payments application, we found that the Museum's Deputy Director of Business Affairs has the ability to approve and modify users' access permissions.

Administrator access should only be assigned to individual users who are responsible to maintain the information systems. The effectiveness of the application's segregation of duties controls may be weakened by the use of the above listed accounts with system administrative privileges.

Recommendations

The Museum should:	
8.1	Perform formal reviews of the applications' audit logs.
8.2	Enable vendor accounts for a limited period of time when necessary and create a unique administrator account for the Access Control and Surveillance application.
8.3	Review roles and privileges allocation to user accounts and distinguish which privileges not to combine to prevent a segregation of duties conflict.

Management Response/Action Plan:

8.1 Management will review all unit-level policies, procedures, and operations to incorporate formal review protocols for all application audit logs.

Implementation Date: December 2018

8.2 Management will work with individual application administrators and/or application support teams to review vendor accounts and set new policies of vendor access accounts. The administrator account for the access control and surveillance system has been removed and replaced with named accounts.

Implementation Date: July 2018

8.3 Management will establish a centralized program to manage roles and privileges for all unit-level applications including mitigating controls to manage any segregation of duties conflicts.

Implementation Date: December 2018

9. Network Security Controls

Network Security Controls includes defining and protecting internal and external boundaries, limiting access points to the boundaries using firewalls, comprehensive monitoring of inbound and outbound data traffic, and documenting and reviewing active firewall rules.

Monitoring Access Points

Network data flow diagrams provided by the Network Engineering and Telecommunications Department showed that the Museum's network is adequately segregated by internal and external boundaries. Endpoint devices are protected by the Border Firewall IPS[3] and the Border Router (see Figure 1). Remote access connections must be done via a secure VPN[4] connection. The Museum firewall is monitored by the Security Information and Event Management (SIEM) system. The SIEM monitors connected devices' log files and provides real-time situational awareness to identity malicious activity.

Vulnerability scans provide an additional layer of security to identify potential high-risk areas of compromise by examining the device's configuration settings. Comparing the asset management list with the Museum's systems scanned for vulnerabilities by the Division of IT, we found that 32 of the 95 systems were not listed. Unmonitored endpoint devices could become compromised and go undetected, thereby reducing the effectiveness of the Museum's network monitoring controls.

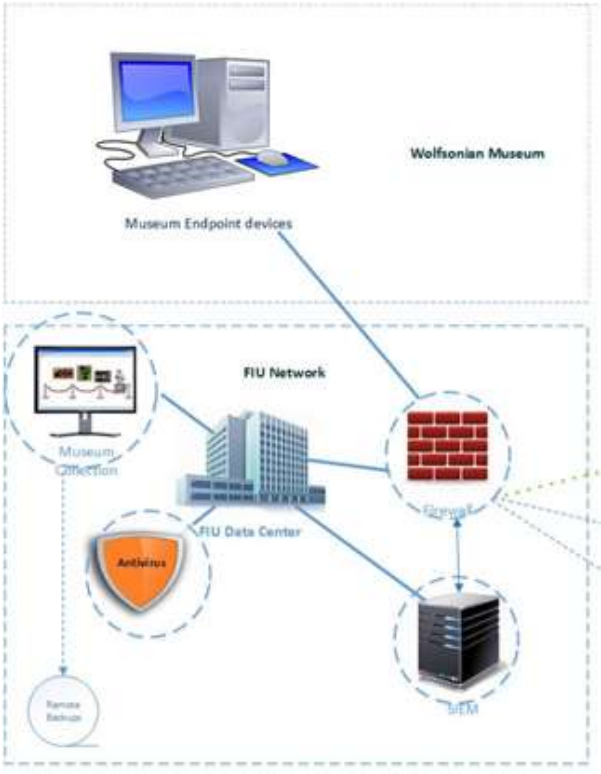


FIGURE 1. FIU NETWORK SYSTEMS

Dataflow traffic

According to *NIST SP800-53A (Rev.4) SC-7(4), Boundary Protection, External Telecommunications Services*, 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. Network access requests should include specific endpoint IP[5] addresses, ports and duration. During the audit period, the Museum sent three requests to the Division of IT to access the Museum's servers. One of the three requests did not include the duration and the business need. Without adequate

[3] Intrusion Protection Systems
[4] Virtual Private Network
[5] Internet Protocol

documentation, management would be unable to determine whether a firewall rule is appropriate.

According to NIST SP800-53A (Rev.4) SC-7(3), *Boundary Protection Access Points*, the Museum should limit the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. In our interview with the Museum's IT Assistant Director, we determined that a review of network traffic flow was not performed. We asked the Division of IT to run a zero hit count for all their systems' firewall rules to identify which ones are actively in use. The results showed that 148 out of 1508 (10%) firewall connections have been used in the last 12 months. Inactive firewall connections that are no longer needed provide unnecessary potential entry points for network attacks.

Security Awareness Training

According to the FIU Security Website, all FIU faculty and staff are required to participate in the security awareness training. The University offers a comprehensive security awareness training to all employees in order to protect the organization and address the multitude of vulnerabilities day-to-day employee activity creates. Inattentive staff or employees not familiar with basic IT security best practices can create opportunities for hackers to compromise the University's network and sensitive data. Examining a Security Awareness training completion report for the Museum provided by the Division of IT, we found that training was completed by 48 of the 49 Museum employees. Immediately upon notification, the 1 employee successfully completed security awareness training.

Recommendations

The Museum should:	
9.1	Ensure all systems are included in the vulnerability scans performed by the Division of IT.
9.2	Include the business need and duration for all active rules and work with the Division of IT to review firewall rules, and disable all inactive connections.

Management Response/Action Plan:

9.1 Division of IT notified of systems to add to vulnerability scans on March 7, 2018 and management will follow up with Division of IT to complete process.

Implementation Date: December 2018

9.2 Division of IT notified to review and disable all inactive connections on March 1, 2018 and management will follow up with Division of IT to complete process.

Implementation Date: December 2018

10. Business Continuity

The purpose of Business Continuity is to establish and maintain a plan to enable the Museum and the University's Division of IT to respond to incidents and disruptions in order to continue operations of critical business processes at an acceptable level. The information systems environment is located on premise, the FIU Data Center, and in a third-party hosted environment. The 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.

Business Continuity Plan (BCP) and Procedure

Business Continuity ensures that a plan is established and maintained to enable the Museum and Information Technology to respond to incidents and disruptions in order to continue critical business processes, required IT services, and maintain the availability of information at acceptable levels. The Museum has two continuity plan manuals: *The Wolfsonian-FIU Hurricane Mitigation Plan and Emergency Management and Continuity of Operations Plan* (EMCOP) *2016*. Both manuals assist personnel in the event of business disruption due to an anticipated hurricane. The employees receive a copy of *The Wolfsonian-FIU Hurricane Mitigation Plan* at the beginning of the annual hurricane season. Each group member is responsible for specific actions required in preparing, securing, and post-storm recovery operations of the Museum. We also noted that the Plan adequately addresses contingency roles for key personnel and contact information. Additionally, since 2015, the Museum has participated with the Florida Association of Museums - Connecting to Collections Program, the Alliance for Response South Florida - Collections Emergency Response Training Workshop, and the Miami Heritage Responders Emergency Program.

Cited in our prior audit, the Plan now includes restoration priorities and metrics for how long the systems can be offline.

The EMCOP defines critical functions as follows:

- Critical 1: must be continued at normal or increased service load. Cannot pause.
- Critical 2: must be continued if possible, perhaps in reduced mode. Pausing completely will have grave consequences.
- Critical 3: may pause if forced to do so, but must resume in 30 days or less.
- Deferrable: may pause; resume when conditions permit.

Listed in the table below, are the self-identified ratings for the in-scope information systems.

System Name	Critical Rating
Access Control and Surveillance	1
Museum Collection	2
Museum Library	2
Payments	3

FIGURE 2 IN-SCOPE INFORMATION SYSTEMS

The Museum provided detailed documentation of the recovery process for non-IT related items. The procedures included how-to directions on handling precautions, packing methods, and drying methods where applicable. However, the Plan does not include the IT procedures necessary for the Museum to meet the critical ratings listed in Figure 2. Without written procedures, the Museum is unable to ensure that they can meet their Plan's operational requirements in the event of a disaster.

BCP Testing

According to the FIU Policy 180.105, *Emergency Management and Continuity of Operations*, the emergency management program shall outline emergency procedures that will restore essential functions as quickly as possible to bring the University's departments back to operational status. According to the SOC-2 Reports provided, the two hosted systems are tested on an annual basis. Additionally, the Museum's Deputy Director of Business Affairs provided test documentation that showed the Wolfsonian-FIU Hurricane Mitigation Plan was tested during the preparations for the hurricane closing in September 2017. However, missing were the test results, corrective actions taken, and lessons learned, which reduces management's ability to determine the plans viability.

Recommendations

The Museum should:	
10.1	Adopt procedures to ensure that the Business Continuity Plan's IT operations can meet the self-identified critical ratings.
10.2	Include formal test results, lessons learned, and corrective actions taken to ensure the success of the business continuity plan.

Management Response/Action Plan:

10.1 Management will review Business Continuity Plan, unit-level disaster mitigation, and recovery plans to ensure all plans are accurate, complete, and aligned.

Implementation Date: June 2018

10.2 In addition to the annual tabletop exercises completed with other South Florida cultural organizations and the newly establish FIU Regional Academic Locations tabletop exercise in May 2018, management will work with FIU OEM staff to develop unit-level tabletop exercises

Implementation Date: June 2018

11. Implementation of Prior IT Audit Recommendations

The prior Museum audit report, dated April 23, 2013, contained 10 Information Technology recommendations, which management has since reported as fully implemented. Our examination of these recommendations included observation of actual processes, interviews with University personnel, and testing of selected transactions and devices.

The recommendations relating to Operational and Financial Controls where addressed within Section I of this report, while those relating to Information Technology Controls are fully addressed below.

Overall, our examination revealed that 9 recommendations were fully implemented, while 1 was partially implemented, as follows:

Summary of Prior Audit Recommendations				
No.	Recommendation	Implementation Status		
		Fully	Partially	Not
11.1	Work with the FIU Information Technology Security Office to test the server for possible infection.	✓		
11.2	Have the FIU Network Security and Systems Engineering department centrally manage all the Museum servers' antivirus.	✓		
11.3	Review information systems administrator accounts and rename those not uniquely identifiable.	✓		
11.4	Work with University Technology Services department to set the maximum number of invalid attempts, which will either, lock out the user for a specified time period; lock out the user account until released by an administrator; or delay the next login prompt as defined by the University.	✓		
11.5	Modify user access and ensure user privileges do not exceed job duties.	✓		
11.6	Reduce user access of personnel who can modify inventory counts to the minimum number of people required to have such authority.	✓		
11.7	Review administrator accounts to ensure that the accounts are appropriately tied to individual users.	✓		

Summary of Prior Audit Recommendations				
No.	Recommendation	Implementation Status		
		Fully	Partially	Not
11.8	Conduct a business impact analysis for each affected department. The results of the analysis should be incorporated into the contingency plan.	✓		
11.9	Perform formal contingency plan testing with key personnel. Test results should be formally reviewed and corrective actions taken to ensure the plan's ability to support the operations and protect its data in the event of a disaster.		✓	
11.10	The Museum should move forward as expeditiously as possible with its plan to upgrade/replace the security monitoring system.	✓		

Listed below are the recommendations that were determined not to be fully implemented. The results of our current observations are as follows:

Prior Recommendation Partially Implemented:

Recommendation No. 11.9 – Perform formal contingency plan testing with key personnel. Test results should be formally reviewed and corrective actions taken to ensure the plan's ability to support the operations and protect its data in the event of a disaster.

Management's Reported Actions:
Analysis with actual testing will be performed and incorporated into the contingency plan by end of April 2013.

Current Observation:
As noted in the Business Continuity Plan Testing section (see page 35), the Museum conducted the *Emergency Management and Continuity of Operations Plan* (EMCOP) *2016* as previously reported. The Museum's Business Continuity Plan is missing a formal review and corrective actions taken to ensure the Plan's ability to support the operations and protect its data in the event of a disaster.

Recommendation

The Museum should:	
11.1	Implement the cited prior audit recommendations.

Management Response/Action Plan:

11.1 Management will incorporate contingency plan testing into Business Continuity Plan and any departmental mitigation plans, and it will be part of tabletop exercises.

Implementation Date: June 2018 (table top exercises will be an on-going activity)