FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of
The Patricia & Phillip Frost Art Museum

Report No. 13/14-12

April 8, 2014

FIU | FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: April 8, 2014

To: Carol Damian, Director & Chief Curator, Frost Art Museum

From: Allen Vann, Audit Director

Subject: **Audit of the Patricia and Phillip Frost Art Museum, Report No. 13/14-12**

Pursuant to our approved annual plan, we have completed an audit of the Patricia and Phillip Frost Art Museum. The primary objectives of our audit were to: assure that the art collection is properly accounted for, well maintained and safeguarded; good financial controls are in place; information technology controls are adequate and effective. During FY 2103 revenues and expenditures totaled $2.58 million and $2.24 million, respectively. Based on the Museum's record keeping, we cannot provide meaningful quantitative data relating to its art collection.

Except as noted, our audit disclosed that the Museum's financial controls and procedures were good. While our physical inventory tests of artwork accounted for all of the objects in our sample of recorded items, weaknesses in record keeping procedures for the collection and information technology controls pose an unnecessary risk that losses could go undetected. Management agreed to implement our 25 recommendations.

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

Attachment

C: Sukrit Agrawal, Chair, BOT Finance and Audit Committee and Committee Members
Mark B. Rosenberg, University President
Douglas Wartzok, Provost and Executive Vice President
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Robert Grillo, Vice President and Chief Information Officer
Javier I. Marques, Chief of Staff, Office of the President

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan, we have completed an audit of The Patricia & Phillip Frost Art Museum (Frost Art Museum or Museum). The primary objective of our audit was to determine if the Museum's established controls and procedures are adequate to ensure that:

- The art collection is properly accounted for, well maintained and safeguarded;
- Good financial controls are in place;
- Information technology controls are adequate and effective; and
- University policies and procedures, applicable laws, rules and regulations are complied with.

Our audit included the Museum's revenues and expenditures for the period July 1, 2012 through June 30, 2013. 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.

For 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 Publications 800-53A Revision 1 Guide for Assessing the Security Controls in Federal Information Systems and Organizations*.

During the audit, we reviewed University's and Museum's policies and procedures, applicable Florida statues, and University rules, observed current practices and processing techniques, Interviewed responsible personnel; and tested selected transactions. Sample sizes and transactions selected for testing were determined on a judgmental basis. Audit fieldwork was conducted from September 2013 to January 2014.

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. There were no prior audit recommendations related to the scope and objectives of this audit requiring follow-up.

BACKGROUND

Housed on the Modesto Maidique Campus of Florida International University (FIU or University), 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.

Initially a relatively small gallery of less than 3,000 square feet, the Museum 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 reaccredited in 2011. In 2001, the Museum became an affiliate of the Smithsonian Institution.

The mission of the Frost Art Museum is to:

- Enrich and educate local, national and international audiences through the language of art by collecting, preserving, researching, interpreting and exhibiting art from diverse cultures throughout human history.
- Provide a resource for scholarly research and interdisciplinary collaboration, augmenting the university's educational mission as both a local and global center of knowledge and culture.

Collections

The Frost Art Museum's collection is a melding of several distinctive collections, which includes the General Collection, the Metropolitan Museum and Art Center Collection, and the Betty Laird Perry Emerging Artist Collection:

- The General Collection includes American printmaking from the 1960s and '70s, photography, Pre-Columbian objects dating from 200-500 AD, and a number of works by contemporary Caribbean and Latin American artists.

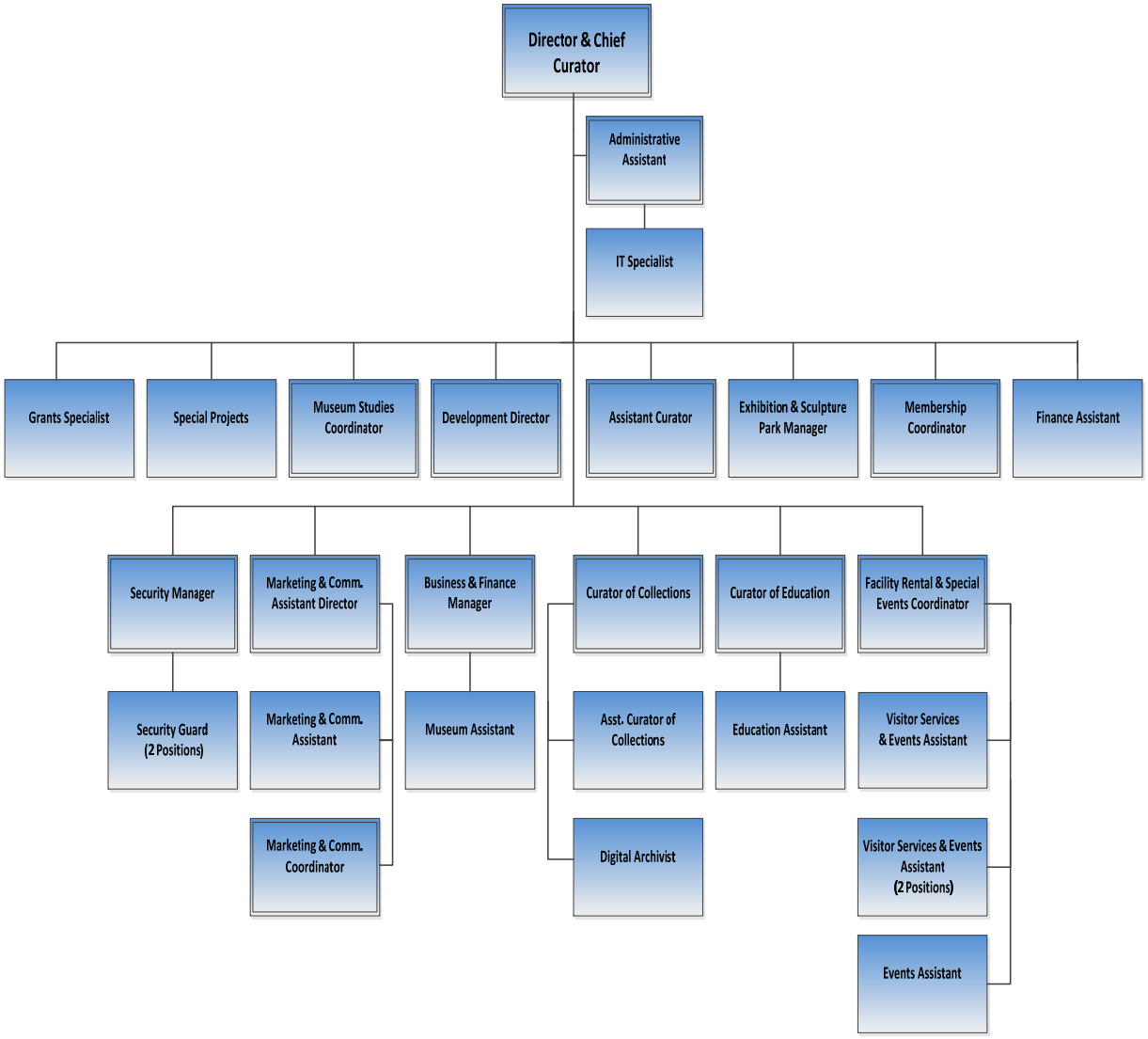
- The Metropolitan Museum and Art Center Collection includes more than 2,300 sculptures, photographs, and paintings. When the Metropolitan Museum and Art Center of Coral Gables closed, its collection was donated to the Frost Art Museum in 1989.

- The Betty Laird Perry Emerging Artist Collection is comprised of artworks obtained through purchase awards granted to selected Bachelor of Fine Arts (BFA) and Master of Fine Arts (MFA) students graduating from the FIU's studio arts program since 1980.

The Frost Art Museum has recently begun to present exhibitions in Latin America and is working on future collaborations and partnerships with leading art institutions in these regions. These efforts to foster cultural, educational, and artistic exchanges compliment the University's commitment to its ever-growing international audiences.

Personnel

The Frost Art Museum is an independent unit under the direct authority of the Provost and Executive Vice President and its operations are overseen by the Director/Chief Curator. As of September 2013, the Museum had 29 employees (12 administrative personnel, 7 staff, 1 part-time administrative, 5 temporary non-student employees, and 4 student assistants). The Museum's organization chart is shown below.



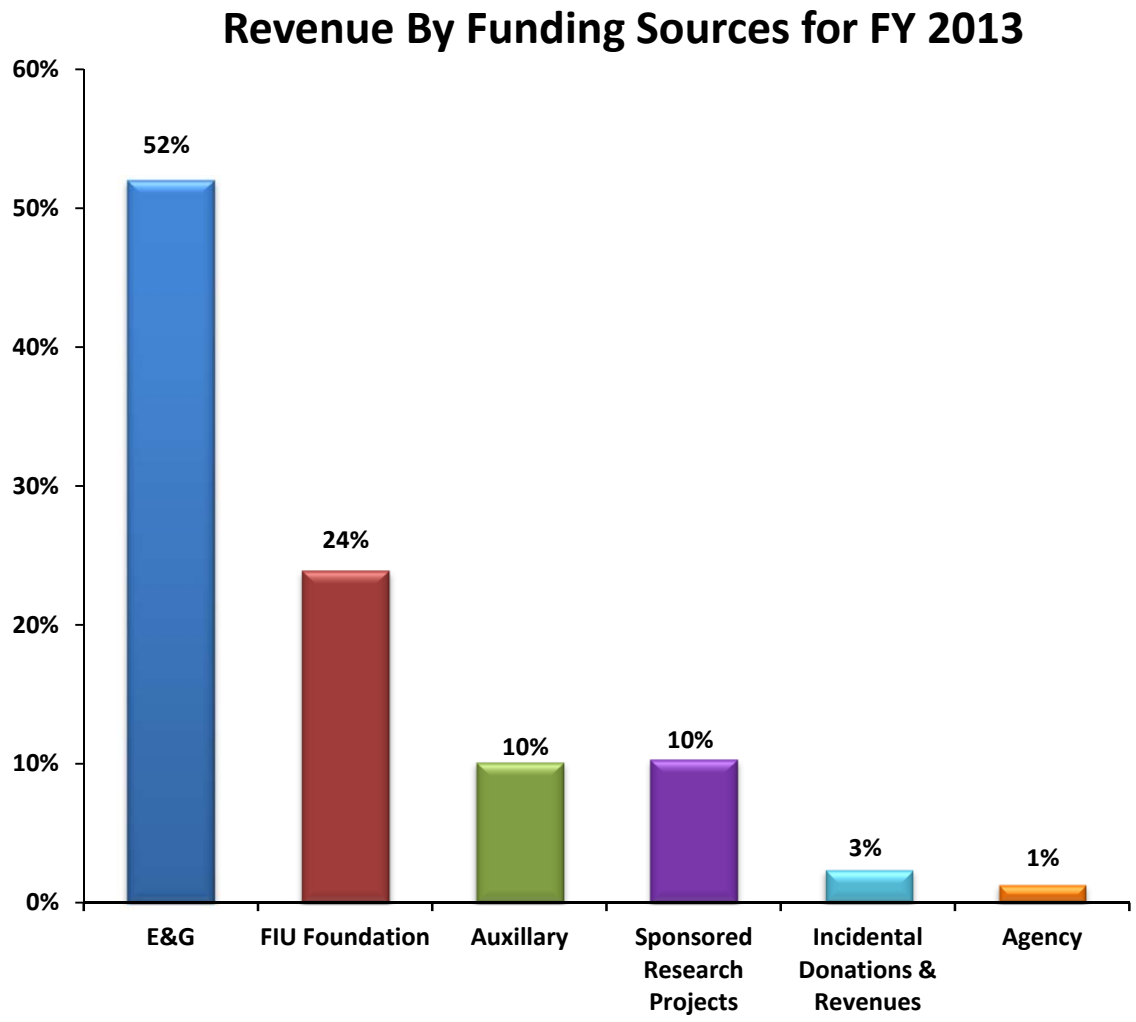
The Director/Chief Curator is stepping down from her current position to devote more time to teaching as a full-time professor at FIU's Department of Art and Art History but will remain as Chief Curator. She will continue to serve as the Director until a new one is appointed. During the audit a part-time IT specialist, who assisted in supporting in the IT systems, also resigned. Subsequently, a full-time IT position has been approved.

Financial information

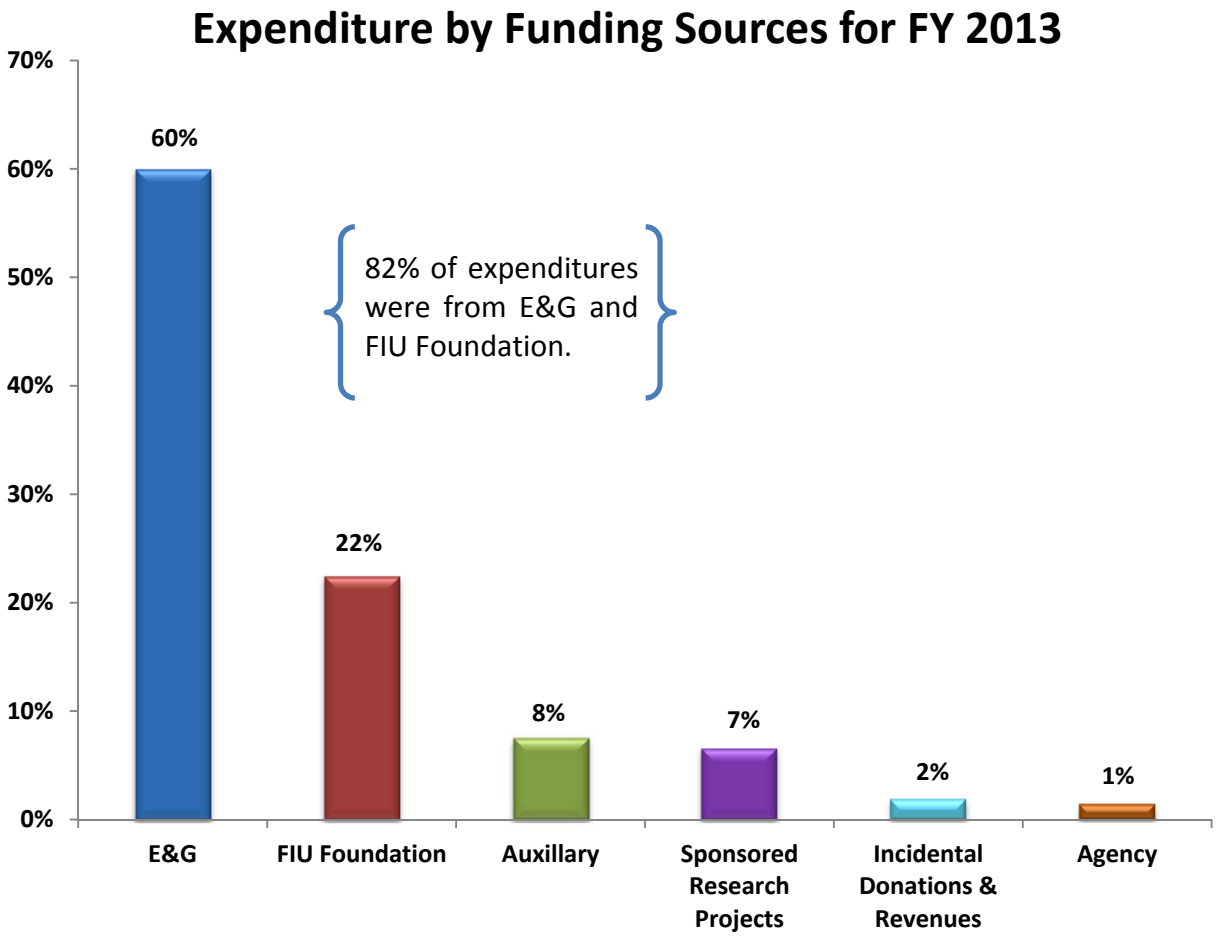
The majority of the Museum's funding comes from the University. However, grants from the State of Florida and Miami-Dade County, complimented by endowments, membership and private and corporate giving, provide funding for annual programs and enables the Museum to offer free admission to all exhibitions and public events.

The Museum's revenues and expenditures for the fiscal year 2012-13, as recorded in the University's and FIU Foundation's accounting records, totaled $2.58 million and $2.24 million, respectively.

The following chart provides a breakdown of the Museum's revenue funding sources for the fiscal year 2012-13.



University accounts are used for the Museum's operations, mainly employees' salaries and benefits. Foundation accounts are used mostly for art exhibitions. The Museum's total expenditures by funding sources for the fiscal year 2012-13 are depicted in the following chart.

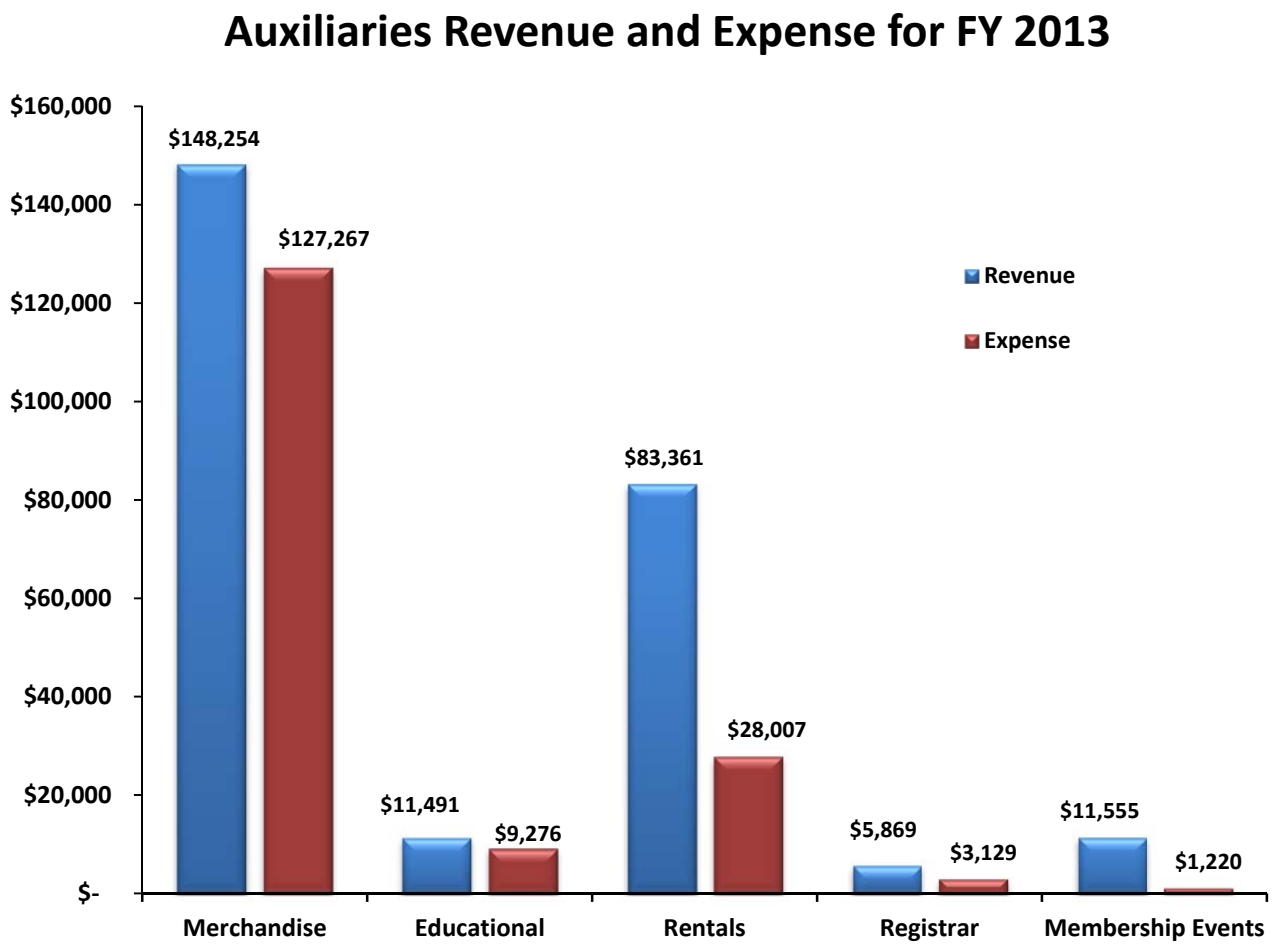


Auxiliary Operations

The Frost Art Museum had five separate auxiliary operations as follows:

1. Merchandise (Catalogs & Exhibitions)
2. Educational
3. Rentals
4. Registrar
5. Membership events

During the fiscal year 2012-13 the Museum generated revenues totaling $260,530, while expending $168,899 from its auxiliary activities. The following chart provides total revenue and expense for each auxiliary operation.



The bulk of its merchandising revenue ($136,200) was generated by having a fine art fundraising auction in November 2012. The income from this first time event helps supporting the Museum's operations.

FINDINGS AND RECOMMENDATIONS

With the exception of collection records, our audit disclosed that the Museum's financial controls and procedures were good. While our testing procedures found no evidence that the collection has been compromised, record keeping for the art collection particularly collections management and information technology security controls related to information systems, identity access, and business continuity pose an unnecessary risk that losses go undetected and therefore, must be strengthened.

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

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		X	
Policy & Procedures Compliance	X		
Effect		X	
Information Technology 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 Technology Risk	**System controls are effective in mitigating identified data risks**	**System controls are moderately effective in mitigating identified data risks**	**Systems controls are ineffective in mitigating identified data risks**
External Risk	**None or low**	**Medium**	**High**

(page intentionally left blank)

Section I. FINANCIAL AND OPERATIONAL CONTROLS

The areas of our observations during the audit are detailed below.

1. Collections Management

The Frost Art Museum uses collection management software called "MuseumPlus" to manage and organize its collections. The Museum also has a comprehensive collections management policy, which serves as a guide in managing its collections. Our observation in this area is discussed as follows:

a) Art Collection Records

Per the Records and Documentation procedure on Inventory (Academic Affairs (AA) Policy 14.30, *Acquisitions to the Frost Art Museum Collection*), the Museum's Registrar shall be responsible for maintaining a current inventory of all the Museum collections, with minimum information to include accession/registration number, University property number, basic description of object, current location and condition. Our review of 7,447 permanent collections generated by MuseumPlus disclosed:

- 6,634 objects (89%) had their description field blank. Some objects' description was recorded in another field when the data from the old database application (FileMaker) were transferred to MuseumPlus.

- 4,076 objects (55%) did not have a value assigned. Prior to year 2005 many donated objects were reportedly received with inadequate documentation.

- 307 objects were listed more than once. It appears that due to a database design, multiple instances of individual objects were noted in the report.

- 21 objects were missing and 6 objects had no current location. The Museum is aware of missing objects, which will be investigated and formally deaccessioned, as necessary.

- 2 objects did not have an accession number. We were informed that these objects will be researched against the donor records for the accession number.

- None of the objects had a condition described. Their condition was noted in the collection files, which requires a data entry person to enter the information to MuseumPlus. Currently, the Museum has no employees who perform this function.

The Museum Operations Coordinator attributed the inadequate maintenance of the Museum's collection database to staffing shortage.

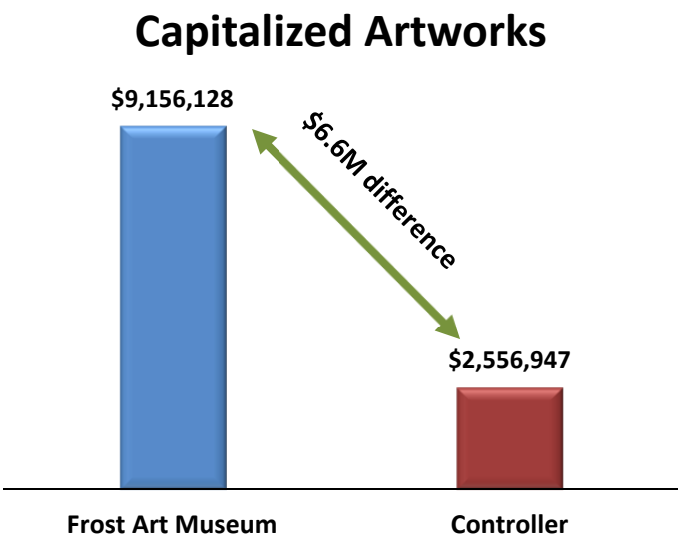
b) Artwork Observations

We took a physical inventory of all artworks/objects valued at $100,000 or more recorded in the collection database. For all 26 selected objects, a total value of $6.2 million, 23 were located and 3 were identified as being returned to the lending institutions. However, the 3 loaned objects were returned in 1997, 2009 and 2011, respectively, but the collection database was not timely updated to reflect their return. For one of the objects return receipt documentation was not evident.

Eight artworks were also judgmentally selected from the Museum and traced back to the collection database without exception.

c) Capitalization of Works of Art

The University's financial statements include Works of Art and Historical Treasures as part of its capital assets. They were recorded at historical cost at the date of acquisition or at estimated fair value at the date received in the case of gifts. For donated objects proper documentation such as appraisals and deed of conveyance is required in order to be capitalized by the Controller's Office.



At June 30, 2013, the University's Works of Art totaled $3,962,039, which included $2,556,947 from the Frost Art Museum. However, our review of the Museum's collection records (excluding loaned items and those valued at less than $5,000) showed their objects value totaled $9,156,128, resulting in almost $6.6 million difference. This difference might be greater if the 4,076 objects with unassigned values in the collection records (see section a) above) were valued and considered.

We were informed that the difference was mainly caused by accepting donations without sufficient documentation before 2005 and neglecting to report donated art works to Asset Management in the Controller's Office. According to the Museum Operations Coordinator, typically museums may keep collection records for organizing and managing, but not for the purpose of capitalizing. Also, many objects were assigned a monetary value for insurance purpose only, in accordance with the Collection Management Policy, which states, "The Museum may assign a monetary value to a work of art by reference to comparative price or other available information for its internal purposes only (such as insuring works of art)."

Recommendations

The Frost Art Museum should:	
1.1	Ensure that the collection database is accurate, complete, and current, which includes: a) Improving its collection report to accurately capture a total object count; b) Entering each object condition into the collection database; and c) Ensuring any missing accession numbers and objects are investigated and formally deaccessioned, if necessary.
1.2	Maintain documentary evidence of all objects returned to other institutions.
1.3	Determine if any objects, where applicable, need to be provided to the Controller's Office for the capitalization.

Management Response/Action Plan:

1.1(a) We are working with MuseumPlus company to rectify the exporting issue of duplicate records.

Implementation date: May 2014

(b) The Museum is hiring a Data Entry Specialist to clean and input object data. This requires pulling hard copies and entering the information into the database. This is a long-term project.

Implementation date: Begins April 2014. Once the part-time person begins we will be able to gauge the project duration.

(c) Missing objects (and two unnumbered) and not located objects will be part of Phase II of the deaccessions project. This project also requires the hiring of the Data Entry Specialist, who will begin April 2014.

Implementation date: Multi-phased projects requiring signatures and meetings will begin April, 2014. See 1.1(b) above.

1.2 This will be ongoing for all objects on loan to the museum.

Implementation date: Immediately

1.3 The Curator of Collections spoke with the Assistant Controller on March 14, 2014. Because many of the Museum's art acquisitions are donations, it cannot require the donors to provide an appraisal. Therefore, the value of the gift is entered into Raiser's Edge as $1 by Advancement. This is the value that is reported to the Controller and so it falls off of their books since the value is under $5,000. The Museum will continue to input the fair market/insurance value provided by the donor into the Collection Management database and will make this information available to the Controller's office at their request.

Implementation date: Immediately

2. Revenue Controls

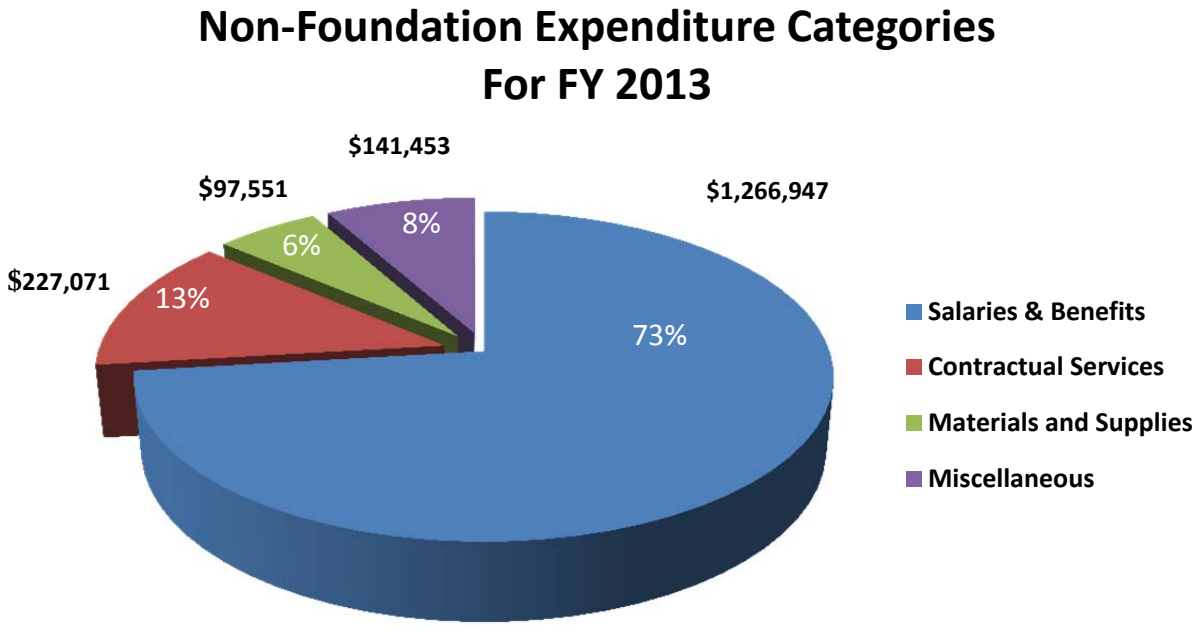
Our audit disclosed that the Museum's controls and procedures relating to revenue collections were adequate. We selected and tested 18 transactions totaling $142,131 from the auxiliary account (activity number 1240030001). All transactions tested were properly supported and recorded in University books and records. No reportable issues were noted in this area.

3. Expenditure Controls

Except for some of the observations noted below, our audit disclosed that the Museum's expenditures were appropriate, allowable, and in accordance with University policies and procedures, applicable laws, rules and regulations.

a) Non-Foundation Expenditures

The Museum's non-Foundation related expenditures for the fiscal year 2012-13 totaling $1.7 million, are summarized below.



The areas of expenditures tested are discussed below.

1) Payroll Expenditures and Approval

The majority of the Museum's expenditures are related to compensation and employee benefits, which accounted for 73% of its expenditures or $1.3 million. As part of payroll test, we verified that the Museum's staff were all bona fide employees and required background checks sampled were completed. Also, except for the Museum's HR Liaison (Administrative Assistant)'s time entries we verified that the payroll approval process was properly followed. However, 100% of the time the HR Liaison's leave hours (52 transactions) for the pay period from December 22, 2012 through October 11, 2013 were not approved by her supervisor but were automatically approved by default by the HR Payroll Department.

2) Purchase and Credit Card Controls

The Museum's total operating expenditure, excluding payroll and auxiliary shared services fee (overhead), for the fiscal year 2012-13 was $452,678. We tested 68 disbursements totaling $195,845, including 36 credit card transactions, representing over 43% of the total annual operating costs. With few exceptions, the disbursements tested were allowable and related to the operation of the Museum. They were also properly approved by authorized personnel, and complied with University purchasing policies and applicable laws, rules and regulations.

3) Travel Authorization and Expenses

During the audit period the Museum incurred travel expenses totaling $7,272, which represented less than 2% of the Museum's total operational expenditures.

According to Florida Statute section 112.061(3)(a): "All travel must be authorized and approved by the head of the agency, or his or her designated representative, from whose funds the traveler is paid. . . ." Also, University Travel Expense Policy No. 1110.060 requires that: ". . . Travelers are not to make commitments to travel or to incur travel expenses without first obtaining the appropriate approval."

We tested two trips to Argentina and found that the airline tickets were purchased prior to obtaining an approved travel authorization. In order to ensure the propriety of travel and related expenditures, the Museum must align its practices with State and University requirements.

b) Foundation Expenses

The Museum expended $502,666 from FIU Foundation funds during the audit period for its operations, mainly for exhibitions. We tested 19 transactions, totaling $74,252, representing 15% of the Museum's total Foundation expenses. The transactions tested

were allowable and related to the operation of the Museum. They were also properly approved by authorized personnel, and complied with University/Foundation Purchasing policies and procedures and applicable laws, rules and regulations.

c) Use of Agency Fund

During the audit we observed that some of the Museum's credit card transactions, which were reimbursed by FIU Foundation, were recorded in an activity number (1240040001) under Fund 491 (Agency Fund), rather than Fund 604 (Transfers from Component Units). Fund 491 should only be used for agency activities, which account for resources held by the University acting as a fiscal agent on behalf of other organizations or individuals, not for the Museum's operating expenses whereas, Fund 604 is to be used for the direct support organization (foundation/component unit) reimbursement purpose. As of June 30, 2013, credit card transactions totaled $32,871, were recorded as expenses and a total of $33,443 was reimbursed by FIU Foundation were recorded in Fund 491.

While this practice resulted in a relatively immaterial misstatement of FIU's financial statements, it represents a departure from *Generally Accepted Accounting Principles.*[1] The Museum's Budget and Finance Manager informed us that this activity number was established as an agency fund by the Controller's Office. Effective July 1, 2013 many activity numbers in the agency fund, including the Museum's activity number, were changed from Fund 491 to 604, according to an Assistant Controller.

As of December 31, 2013, the Museum's had a $49,733 fund balance. The Museum's Budget and Finance Manager informed us that the Museum tries to maintain approximately $60,000 fund balance level to cover its expenses. However, Fund 604 should not carry a large fund balance, since it is only used for the Foundation reimbursement purpose**.**

[1] *Generally Accepted Accounting Principles* are the common set of accounting principles, standards and procedures that U.S. companies/universities use to compile their financial statements. They are a combination of authoritative standards and simply the commonly accepted ways of recording and reporting accounting information.

Recommendations

The Frost Art Museum should:	
3.1	Ensure that direct supervisors who have direct knowledge of their employees work and/or leave hours approve the biweekly payroll.
3.2	Ensure that employees obtain Travel Authorization prior to incurring travel expenses or traveling.
3.3	Work with the Controller's Office to ensure the proper use of the Museum's activity number/fund.

Management Response/Action Plan:

3.1 Due to a system limitation in the payroll process, when a manager has delegated payroll approval to a direct report, the manager is unable to approve payroll for the direct report. Due to this, Human Resources has recommended that the "proxy print the employee's time card and has the supervisor sign the time card indicating approval of hours reported". In addition, an "e-mail from supervisor indicating approval of hours reported… should be maintained in the proxy's file for audit records". The Museum will implement this policy for this particular situation going forward.

Implementation date: Immediately

3.2 Although the Museum aims to follow travel policies and procedures to the best of its ability, there are certain instances where travel arrangements may have to be made at a moment's notice. However, the Museum will continue to ensure that travel authorizations are approved prior to incurring travel expenses or traveling in a more consistent manner.

Implementation date: Immediately

3.3 Activity number 12400 4 0001 fund was changed to 604 during the audit period. We look to the Controller's Office to provide an acceptable fund balance for this account and implement the change.

Implementation date: May 2014

4. Asset Management

Per the University's asset management system, the Frost Art Museum had 129 capital assets with associated cost totaling $2.6 million. The Museum's capital asset inventory as recorded in the system is up to date. We also confirmed with the Assistant Controller for Asset Management that they did not observe any missing capital assets while taking their annual physical inventory in 2013.

In addition to capital assets, the University's Property Control Manual defines attractive property as "…University property costing less than the threshold amount of $5,000, but which are particularly vulnerable to theft and misuse." The Property Control Manual recognizes that "Attractive" property items may vary from department to department, the manual offers such things as laptops, iPads, or video recorders as examples. In evaluating "attractiveness" in the context of their own environment the factors they are asked to consider include the security of the property location, the size and portability of the item, and its potential resale value if stolen. Attractive items are to be marked as University property and catalogued by the user department. Special property tags are available upon request from Property Control.

During the audit, we noted that the Museum did not maintain and track its attractive property. The lack of accountability over attractive or sensitive property increases the likelihood of waste, fraud and abuse.

Recommendation

The Frost Art Museum should:	
4.1	Establish a procedure and track all attractive/sensitive property owned by the Museum.

Management Response/Action Plan:

4.1 Now that the Museum has a full-time IT position, we will be able to make this a priority to ensure all attractive/sensitive property is tracked and procedures are in place for its use.

Implementation date: August 2014

Section II. INFORMATION TECHNOLOGY CONTROLS

(page intentionally left blank)

Our Governance, Risk and Compliance (GRC) approach to Information Technology (IT) testing covered five major categories: Information Systems, Identity Access, Network Security, Business Continuity, and Facilities Security.

By using achievement rating measures[2] we identified the level of established internal controls effectiveness in protecting the Frost Art Museum (see Figure 1). Higher rated processes that rated "Fully" or "Largely" achieved are determined to be more reliable whereas "Partially" or "Not" achieved are less reliable and need to be improved to ensure the control's effectiveness in protecting the Museum's data.

Overall improvements to IT controls would increase the effectiveness of the confidentiality, integrity, and availability of the Museum's data security.

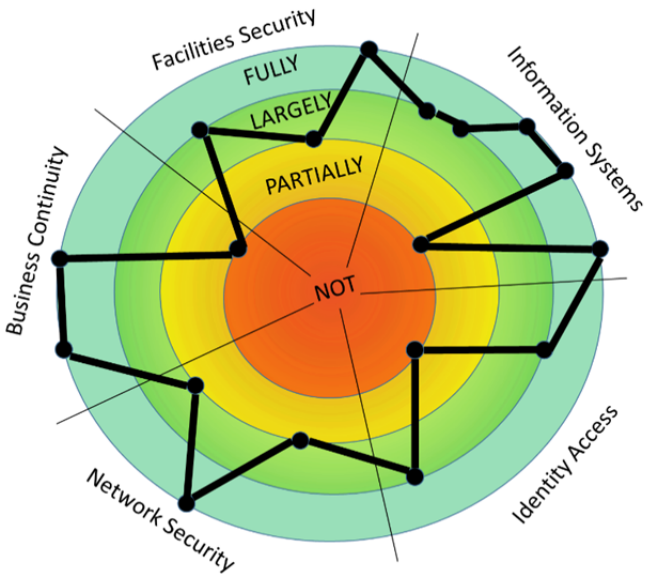


Figure 1- Information Technology Achievement Rating.

These areas include the:

- timely update to antivirus mechanisms;
- discontinued use of local and application non-unique user accounts;
- reduction of system administrator access to the MuseumPlus application;
- encryption and limited user availability of the File Transfer Protocol (FTP) connection;
- addition of the IT database server to the backup schedule;
- inclusion of the University Technology Services (UTS) Disaster Recovery Services with periodic testing of the Business Continuity Plan; and
- regular reviews of the facility alarm monitoring and physical access logs,

Details of our IT findings and recommendations follow:

[2] See Appendix A – Achievement Rating Levels

5. 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's data and protect them from malware, brute force attacks and unauthorized access (see Figure 2 – Information Systems Testing).

a) Malicious Code Protection

The Museum applies a layered approach using the McAfee On-Access Scanner (OAS), Host Intrusion Protection for desktops, hard drive encryption and the Microsoft Software Removal Tool to protect its endpoint devices. Also, the Museum has configured its antivirus application to automatically clean the file when a threat or unwanted program is found. If that action fails, the file is automatically removed. Once a file is removed it sits in a quarantine folder and is automatically deleted from the system after 45 days.

Normally, University Technology Services' Network Systems Security Engineering Department (NSSE) centrally manages the Museum's endpoint devices. However, two devices, including the Budget & Finance Manager's workstation were not actively managed by NSSE. Of the 19 endpoints tested, 2 did not have a properly functioning OAS throughout the audit period including 1 workstation that was assigned to the IT Specialist, which presents a greater overall risk to the information systems due to his elevated access privileges.

In addition, 12 endpoint devices' antivirus signature definitions had not been updated for 264 days on average and 7 were missing Windows security updates. The Museum's antivirus mechanisms are reduced in their effectiveness if they are not maintained and kept current with the latest security updates and signature files.

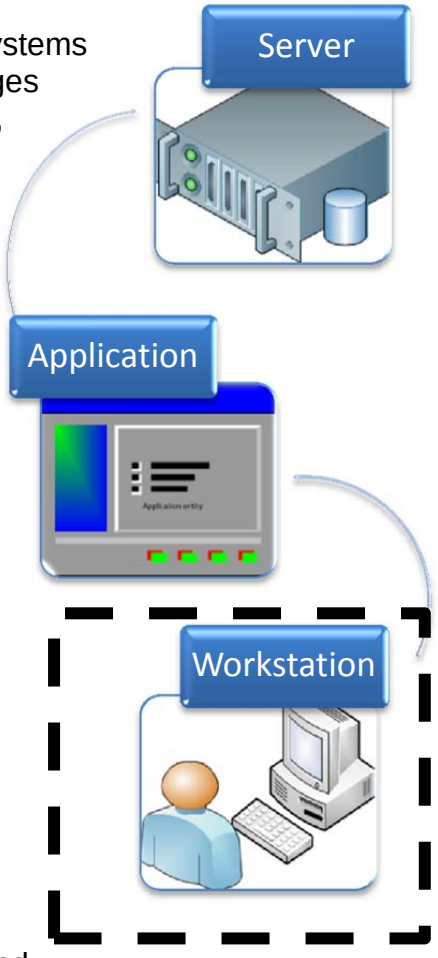


Figure 2- Information Systems Testing

b) Endpoint Security

There were 17 endpoint devices, which had non-unique user accounts with administrative privileges. By ensuring each user is uniquely identified, instead of using one ID for several employees, the Museum can maintain responsibility for individual user actions; increase the audit trail's effectiveness; and help speed issue resolution and containment in the event of misuse or malicious user intent.

Also, 16 endpoint devices had user accounts with non-expiring passwords. Since one of the first steps a malicious individual may take to compromise an endpoint device is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.

Recommendations

The Frost Art Museum should:	
5.1	Ensure that the two endpoint devices are centrally managed by the UTS Network Systems Security Engineering group.
5.2	Work with the FIU Windows Team to install the Microsoft Windows security update patches and ensure the antivirus mechanisms are updated in a timely manner.
5.3	Ensure the OAS antivirus mechanisms are properly functioning on the identified endpoint devices.
5.4	Review and appropriately disable non-unique endpoint user accounts.

Management Response/Action Plan:

5.1 The new IT person will work with the UTS Network Systems Security Engineering group to ensure that the two endpoint devices are centrally managed by UTS.

Implementation date: May 2014

5.2 The new IT person will work with FIU Windows Team to install the Microsoft Windows security update patches and ensure the antivirus mechanisms are updated in a timely manner.

Implementation date: May 2014

5.3 The new IT person will ensure the OAS antivirus mechanisms are properly functioning on the identified endpoint devices.

Implementation date: May 2014

5.4 The new IT person will disable non-unique endpoint user accounts wherever appropriate.

Implementation date: May 2014

6. Identity Access Management

Identity Access Management includes unique identification, least privileged access, and segregation of duties testing of the MuseumPlus application (see Figure 3 - Identity Access Management Testing). User identity and logical access, according to NIST sp800-53A Rev.1 AC-6.1, should be managed to ensure that all application users have access rights in accordance with their business requirements. Additionally segregation of duties of individual user accounts is necessary to prevent malevolent activity without collusion through assigned information systems access controls.

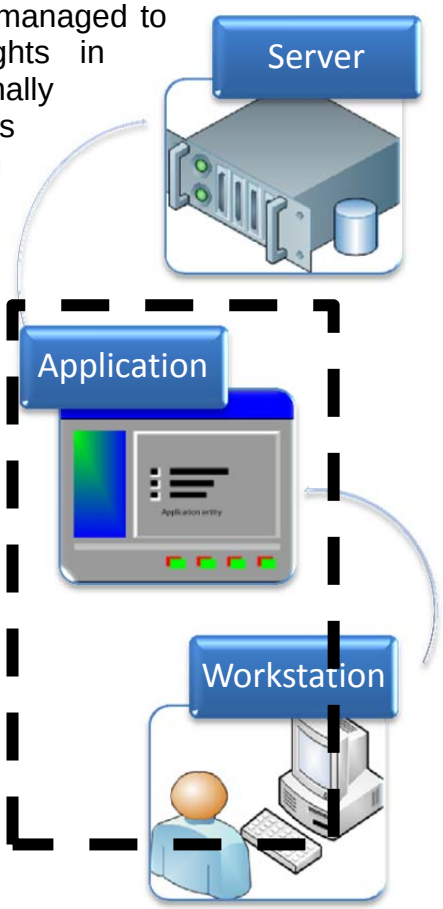


Figure 3- Identity Access Management Testing

a) Unique Identification

According to FIU Policy No. 1930.020a, Data Stewardship, electronic data must be accessed by way of unique name or number for identifying and tracking user identity. Five of the 18 MuseumPlus user accounts tested were generically named user IDs and one intern's workstation had shared user ID and passwords, which displayed in a note form within open sight. The use of the generically named user accounts and shared user credentials increase the risk of unauthorized access to the MuseumPlus application.

b) Least Privileged Access

According to COBIT 5.0 DSS05.04.01 and DSS06.03.03, user access privileges should be allocated and maintained based on what is only required to perform their job activities, business functions and process requirements. There were 14 non-IT users with system administration access to the MuseumPlus application, thereby weakening the application's built-in least privileged access controls. Additionally, the Assistant Curator of Collections and Administrative Assistant had administrative privileges to their assigned workstations. Assigning access in a least privileged manner will help users from incorrectly or accidently changing collection data or altering its security settings.

c) Segregation of Duties

The MuseumPlus application had 25 separate tasks as part of its built-in segregation of duties access controls. There were 4 generically named user accounts, which have system administration privileges and may be used by unauthorized users to bypass existing segregation of duties controls. In addition, there was 1 Visitor Services user that formerly worked in the Collections department that still had access to 19 of the 25 Museum Plus privileges which is identical to the 3 Collections department users. The

effectiveness of the MuseumPlus application's segregation of duties controls may be weakened by the use of generically named accounts with system administrative privileges and access remaining active after a user transfers departments.

Recommendations

The Frost Art Museum should:	
6.1	Review and appropriately disable non-unique user accounts to the MuseumPlus application.
6.2	Discontinue the use of shared user IDs and passwords.
6.3	Review and reduce system administration access only to appropriate personnel.
6.4	Review and reduce, where applicable, the number of active tasks for individual user accounts

Management Response/Action Plan:

6.1 The Collections Manager has disabled any non-unique user accounts to the MuseumPlus application.

Implementation date: Immediately

6.2 The Collections staff has discontinued the sharing of user IDs and passwords. The password for the shared ID has been changed and we created user accounts for individuals requiring access within the MuseumPlus application.

Implementation date: Immediately

6.3 The Collections Manager has reviewed the users with system administration access and reduced access only to designated Collections staff and the IT position.

Implementation date: Immediately

6.4 The Collections Manager will review and reduce, where applicable, the number of active tasks for individual user accounts within the MuseumPlus application.

Implementation date: June 2014

7. Network Security

Network Security includes defining and protecting internal and external boundaries, limiting access points to the boundaries through the use of firewalls and intrusion protection systems (see Figure 4- Network Security Testing). Firewall rules should be configured by default to "deny all" access through the firewalls and should be approved with supporting documentation. Sensitive data should be encrypted in transit and when transported outside of controlled areas.

a) Firewall Controls

Firewalls and routers are key components of the architecture that controls entry into and from the Museum's network. Limiting the number of access points allows for more comprehensive monitoring of network traffic along with blocking unwanted ingress and egress access. Our review of the 15 firewall rule sets disclosed that 12 had inadequate authorized documentation. Due to the lack of formal firewall requests provided, the rule sets should be periodically reviewed to ensure that active network connections are appropriate and adequately authorized.

b) Encryption in Transit

The firewall was adequately configured to implicitly deny all inbound and outbound network traffic. However, there was 1 firewall rule that left an open unencrypted FTP connection allowing unlimited access throughout the University network to one of the Museum's servers. The FTP connection should be encrypted and limited to appropriate Museum personnel.

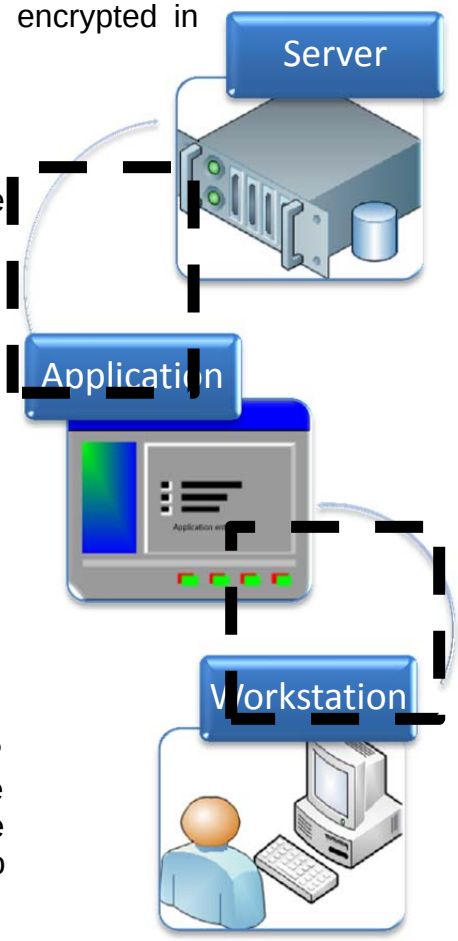


Figure 4- Network Security Testing

Per COBIT 5.0 DSS05.02.07 trusted mechanisms should be implemented to support the secure transmission and receipt of information over all methods of connectivity. Outside connection to the Museum's data is available through the use of a Virtual Private Network (VPN). Three of the 4 VPN users, including the VMWare Operations Systems Administrator, Museum IT Specialist and the UTS Enterprise Team were appropriately assigned to access data from remote locations. However, the 4th VPN user, a PeopleSoft Database Administrator, was improperly assigned, although he never used the Museum's VPN and was unaware of having a remote access to the Museum. The lack of periodic reviews of VPN user access increases the risk of inappropriate access.

Recommendations

The Frost Art Museum should:	
7.1	Encrypt and limit the FTP connection to appropriate personnel.
7.2	Periodically review firewall rule sets to ensure active connections are appropriate and adequately authorized.
7.3	Remove the PeopleSoft Database Administrator's VPN access and periodically review a VPN user access list to ensure the access is appropriate.

Management Response/Action Plan:

7.1 The new IT person will work with FIU Division of IT Networking Services (NSSE) to ensure that the FTP connection is encrypted to appropriate personnel.

Implementation date: May 2014

7.2 FIU Division of IT Networking Services (NSSE) is responsible for and manages all firewalls for FIU. The new IT person will work with FIU's Division of IT to ensure firewall rules are appropriate.

Implementation date: May 2014

7.3 The new IT person will remove VPN access from the PeopleSoft Database Administrator and will review the VPN user access list on a periodic basis to ensure access is appropriate.

Implementation date: May 2014

8. Business Continuity

The purpose of Business Continuity is to establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operations of critical business processes at a level acceptable to the Museum (see Figure 5- Business Continuity Testing).

The Museum's Emergency/Disaster Preparedness and Recovery Plan (Plan) was last updated on July 30, 2013. The Plan assists in recovering collections from events ranging from a minor emergency to a major disaster. The Plan adequately addresses its purpose, roles and responsibilities, coordination among different entities and recovery procedures.

The Plan identifies two critical IT servers, which store the Museum's collection data, collection database, and user data files, are located at the UTS Data Center. Our review disclosed that one server was not included in the UTS backup schedule and the other server, per log documentation provided, was not adequately backed up. Also, UTS did not provide Disaster Recovery services for the Museum in the event of a disaster.

The Plan has not been tested. It is a good practice to test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcome. This will allow solutions to be developed and also help to verify over time that the plan will work as anticipated. Without proper testing, key steps may not function correctly thereby reducing the effectiveness of the Museum's Plan.

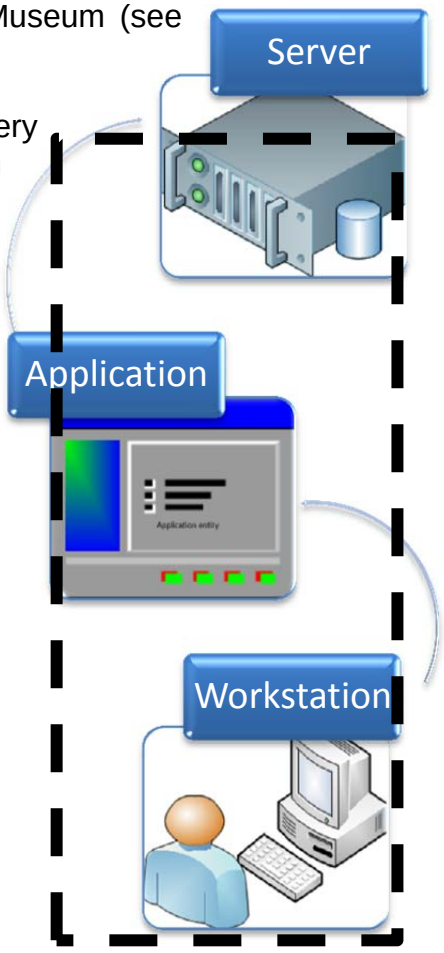


Figure 5- Business Continuity Testing

During the audit we were informed that the Museum's HVAC has not been working when there is a power outage, despite having an emergency generator. Consequently, the Museum's collections may be at risk if a power failure occurs for an extended time, especially in the event of a disaster. We contacted the University's Facilities department to test the Museum's emergency generator. On February 14, 2014 it was tested and a defect was identified, which we were told will be repaired.

Recommendations

The Frost Art Museum should:	
8.1	Work with UTS to include IT servers in the backup schedule and Disaster Recovery process.
8.2	Periodically review backup log files to ensure backups have successfully completed.
8.3	Work with Emergency Management to conduct a tabletop exercise to test components of its Emergency/Disaster Preparedness and Recovery Plan.
8.4	Work with the Facilities department to ensure that the emergency generator is periodically tested and working as intended.

Management Response/Action Plan:

8.1 The new IT person will work with Division of IT to ensure that our servers are in the backup schedule and Disaster Recovery process.

Implementation date: June 2014

8.2 The new IT person will review backup log files periodically to ensure backups are being performed successfully.

Implementation date June 2014

8.3 Table top exercises have been scheduled with the entire museum staff and the Director from the Department of Emergency Management.

Implementation date: May 2014

8.4 Generator will be tested on a weekly basis. We will implement a quarterly disaster recovery test going forward.

Implementation date: Immediately

9. Facilities Security

The purpose of Facilities Security is to prevent unauthorized persons from gaining access to sensitive areas and potentially steal, disable, disrupt or destroy art collection. The Museum's Facility Security includes (1) the use of video camera and the monitoring of individual physical access to sensitive areas, (2) an electronic key card swipe, and (3) an alarm monitoring system (see Figure 6- Facilities Security Testing).

The Museum has a total of 57 video cameras recording 24 hours a day. According to the Security Manager, the video cameras are monitored 7 days a week. Video logs are kept on the server for up to 6 months. The Museum's electronic key card swipe system is intended to prevent unauthorized physical access to sensitive areas. There are 9 secured areas, which include the loading dock, museum inventory rooms, video surveillance room and interior and exterior doors. In addition, alarm codes are needed to gain access to the high risk areas such as inventory rooms and loading dock.

Figure 6- Facilities Security Testing

Our review of 26 active user accounts (key card swipe system) disclosed 5 users were still active 436 days on average after their termination. Also, facilities access expiration date for all employees including temporary employees was given until December 31, 2199.

The alarm monitoring system is the 3rd layer of facilities security. There were 4 individual users with administrator privileges, which have the ability to modify alarm settings including the cancelation of alarms. Our review of these 4 users disclosed that 1 terminated security guard was still active.

Security log files were not reviewed by the Museum's security department. The log file reviews should be performed by the security department on a defined basis to ensure that controls are functioning properly.

Recommendations

The Frost Art Museum should:	
9.1	Remove or disable terminated users' facilities access in a timely manner.
9.2	At minimum modify temporary users' facilities access expiration date to more accurately reflect their anticipated time with the Museum.
9.3	Review facility security log file on a defined basis to ensure that controls are functioning properly.

Management Response/Action Plan:

9.1 Since we have been made aware of this issue, we have since removed facilities access to terminated users. Going forward we will implement a standard procedure for timely review and removal of terminated users.

Implementation date: Immediately

9.2 At this time, expiration dates are not able to be modified and is a standard date for all users. This is overseen by Facilities Key Bank and is a system-wide issue that they are working on to resolve. We will continue to work with Key Bank to ensure that this issue is resolved.

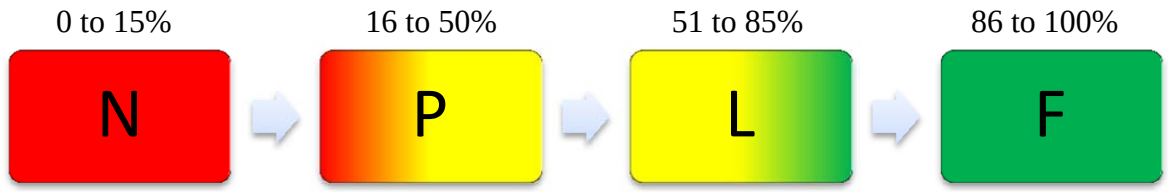
Implementation date: Immediately

9.3 At this time, expiration dates are not able to be modified and is a standard date for all users. This is overseen by Facilities Key Bank and is a system-wide issue that they are working on to resolve. We will continue to work with Key Bank to ensure that this issue is resolved.

Implementation date: Immediately

Appendix A – IT Achievement Rating Levels

Achievement ratings measure the level of established internal controls effectiveness as compared to control activities outlined in COBIT 5.0, NIST special publications, and FIU policies. Higher rated processes are determined to be more reliable.



Achievement rating scale consists of the following:

N = Not achieved (0 to 15%)

- Achieved 15% or less of our sample testing, which indicates internal controls are either deficient or non-existent. These controls need improvement to ensure their reliability.

P = Partially achieved (16 to 50%)

- Achieved more than 15% and up to 50% of our sample testing, which indicates there is some evidence of the processes in place. At this level, some aspects may be unpredictable and unreliable.

L = Largely achieved (51 to 85%)

- Achieved more than 50% and up to 85% of our sample testing, which indicates there is evidence of a systematic approach and significant achievement of the assessed process. At this level, some weaknesses may exist and improvements can be made further for more reliability.

F = Fully achieved (86 to 100%)

- Achieved over 85% of our sample testing, which indicates there is evidence of a complete and systematic approach and full achievement of the assessed process. No significant weaknesses are found and these controls are considered very reliable.