Audit of Compliance with Donor Confidentiality and Intent

Report No. 20/21-02
November 3, 2020

FIU | Office of Internal Audit

Date: November 3, 2020

To: Howard R. Lipman, Senior Vice President Advancement and CEO, FIU Foundation, Inc.

From: Trevor L. Williams, Chief Audit Executive

Subject: **Audit of Compliance with Donor Confidentiality and Intent – Report No. 20/21-02**

We have completed an audit of Compliance with Donor Confidentiality and Intent for philanthropic gifts managed by the Florida International University Foundation for the period July 1, 2018, through January 31, 2020, and an assessment of the current practices through July 31, 2020. The primary objective of our audit was to determine whether: a) procedures and controls to ensure compliance with donor confidentiality and intent are adequate, b) philanthropic gifts are used properly and comply with donor intent, and c) appropriate controls are in place to protect donor's personally identifiable information.

The sole purpose of the Foundation is to encourage, solicit, receive, and administer gifts and bequests of property and funds for scientific, educational, and charitable purposes, all for the advancement of FIU and its mission. For the audit period July 1, 2018, through January 31, 2020, the Foundation recognized $50.2 million, net of the discount, in contribution revenues.

Overall, our audit found that the Foundation has adequate procedures and controls in place to ensure compliance with donors' confidentiality and intent. However, opportunities for improvement exist in the Information Technology controls, specifically identity access management, audit logs, and business continuity plan. The audit resulted in three recommendations, which management has agreed to implement.

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

Attachment

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

TABLE OF CONTENTS

Page

OBJECTIVES, SCOPE, AND METHODOLOGY

Pursuant to the Office of Internal Audit (OIA) approved annual plan for the 2019-2020 fiscal year and the request of Foundation management, we have completed an audit of the Florida International University Foundation's ("FIU Foundation" or "the Foundation") compliance with donor confidentiality and intent. Our audit entailed an examination of the Foundation's transactions and records generated between July 1, 2018, and January 31, 2020, and an assessment of current practices related to the area of audit coverage through July 31, 2020. The primary objective of our audit was to determine whether: a) procedures and controls to ensure compliance with donor confidentiality and intent are adequate, b) philanthropic gifts are used properly and comply with donor intent, and c) appropriate controls are in place to protect donor's personally identifiable information (PII).

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing,* promulgated by The Institute of Internal Auditors (IIA) and Special Publications issued by the National Institute of Standards and Technology (NIST). The audit included tests of the accounting records and such other auditing procedures, as we considered necessary under the circumstances. Audit fieldwork was conducted from March 2020 through August 2020.

During the audit, we:

- reviewed Foundation policies and procedures, and applicable Florida statutes, rules, and regulations;
- tested the adequacy of internal controls and processes for the Foundation and the applicable schools, colleges, or business units receiving gifted funds;
- reviewed gifted fund balances and expenditures to ensure they complied with donor intent; and
- analyzed IT system controls over the PII of donors to ensure donor confidentiality.

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

As part of the audit, we reviewed all internal and external audit reports and found no reports had been issued during the last three years with any applicable recommendations related to the scope and objectives of this audit, which otherwise would have required follow-up. An external audit of the Foundation's financial statements for the fiscal year ended

June 30, 2019, concluded that the financial statements were presented fairly, in all material respects.

BACKGROUND

The FIU Foundation, a non-profit corporation, is a Direct Support Organization (DSO) and a component unit of Florida International University (FIU). The sole purpose of the Foundation is to encourage, solicit, receive and administer gifts and bequests of property and funds for scientific, educational and charitable purposes, all for the advancement of FIU and its mission. The Foundation relies upon having a stream of consistent philanthropic revenue and responsible investing of the endowment, capital and operating funds to accomplish its mission. The FIU Foundation is registered by the State of Florida as a charitable organization and is approved by the U.S. Internal Revenue Service as a tax exempt 501(c)(3) organization. The Foundation has also been certified as a Direct Support Organization of Florida International University as defined in Florida Statue 1004.28.

The Foundation is governed by a Board of Directors, whose time, leadership, and financial resources play a significant role in the development of the University as a major educational, cultural, and economic resource, and in advancing the University's mission.

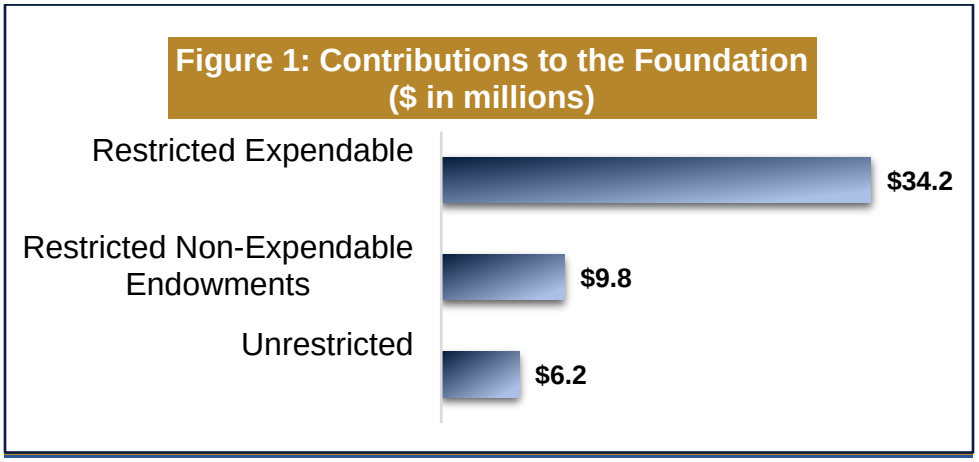
There are various forms of philanthropic gifts that can be made to the Foundation for the benefit of the University, such as, cash contributions, sponsorships, grants, pledges, in-kind gifts/real estate, and stocks. Contribution revenues are recognized for financial statement purposes under Governmental Accounting Standards Board (GASB) when the donor makes a cash donation and/or an unconditional promise to give to the University. Unconditional promises to give are recorded at their estimated fair value and discounted to present value. In addition, endowment pledges are not recognized under the GASB accounting framework. Only additions to the permanent endowment are recognized upon the receipt of cash. Contribution revenue is categorized into one of three classifications: unrestricted, restricted expendable, or restricted nonexpendable endowments.

- Unrestricted contribution revenues represent philanthropic gifts that are available without restriction for carrying out the Foundation's objective to support the University.

- Restricted expendable contribution revenues represent philanthropic gifts that a donor or grantor has placed restrictions on the use and includes the expendable portion of endowment funds.

- Restricted nonexpendable endowment contributions represent the nonexpendable portion (corpus) of endowment funds that are subject to donor or grantor restrictions for the benefit of various programs at the University. These programs primarily include endowed chairs and professorships, research funding, and student scholarships.

Contribution revenues totaling $50.2 million were recognized, net of the discount, by the Foundation from July 1, 2018, through January 31, 2020. The classification of contribution revenues, net of the discount, recognized are detailed in Figure 1 below.



Source: FIU Foundation

Our audit focused on donor restricted expendable contributions received by the Foundation to ensure their distribution to and use by the schools, colleges, or business units are compliant with the donor's intent.

The Foundation develops relationships with potential donors and manages the depositing and distribution of contributions received. Restricted gifts are managed by the Foundation and the schools, colleges, or business units are designated as the beneficiary of the contributions received. The schools, colleges, or units administer the use of the contributions in accordance with the donor's designation or intent.

The Foundation uses a software called Raiser's Edge to perform donor management tasks such as storing donor contact information, philanthropic giving history, prospective donor research, relationships, and more. An external vendor, Blackbaud, provides the Raiser's Edge software. Raiser's Edge provides clients with the option to host data via Blackbaud cloud services, or via their own on-premises solutions. Currently, the donor data in Raiser's Edge resides on the University premises. The Foundation is preparing to migrate to a new version of Raiser's Edge called Raiser's Edge NXT, where donor data will be stored using Blackbaud cloud services.

Blackbaud software complements Raiser's Edge with Fundraiser Performance Management (FPM). This platform is a shared management system for college and university fundraising campaigns. This solution combines interactive reporting, predictive modeling, training, advice, and research to assist institutions in raising funds. FPM, a web-based application, displays the donor data received from Raiser's Edge in a user-friendly manner. Development officers can be assigned prospective donors and interactions can be uploaded to FPM. This allows the department to monitor the engagement between development officers and prospects.

In addition, Blackbaud also provides software called, ResearchPoint. This is a stand-alone tool apart from Raiser's Edge. Whereas Raiser's Edge allows an organization to manage its constituents, ResearchPoint is a database driven product used by various organizations to perform research on current and potential donors by aggregating public data from various data sources. The information obtained from Research Point can provide a development officer with a prospective donor's total publicly identifiable wealth, real estate, business, and philanthropic giving history.

Responsibility of the FIU Foundation

Once a prospective donor is contacted and a potential philanthropic gift is arranged, the Development Office works with Writing and Editorial Services (WES) to draft and edit a proposal, if requested by the prospective donor. The Development Office may solicit input on proposals by consulting with the following departments: Corporate and Foundation Relations, Donor Relations, Planned Giving, FIU General Counsel, and Office of the Provost. After the review process is complete, a final proposal is submitted to the donor who may either accept or reject it.

Gifts under $25,000 with no special criteria or restrictions may be documented using a pledge transmittal form. Gifts of $25,000 or greater or with donor-imposed restrictions must be supported with a gift agreement drafted by the Development Officer in coordination with WES. WES is responsible for routing the final draft agreement for review and approval by the:

- Assistant Vice President of FIU Foundation Finance and Constituent Records Management,
- Associate Vice President of Development,
- Director of Donor Relations,
- Director of Constituent Records Management, and
- FIU General Counsel

Once accepted, WES is responsible for uploading the final gift agreement to DocuSign for the electronic signature of the Foundation CEO, the dean or director, if applicable, and the donor(s). The agreement may also be routed in paper format if the donor does not want to use electronic signatures. Executed copies of the gift agreement are then provided to all signing parties, as well as to the:

- Chief Development Officer,
- Associate Vice President of Development,
- Senior Executive Director of Development,
- Office of Senior Vice President,
- Director of Donor Relations and Donor Relations Manager,
- Foundation Finance Office,
- Campaign Communications Office, and
- Research and Prospect Management Office.

All disbursements of contributions received are processed and approved by the Foundation Finance Office to ensure proper use in accordance with the donor's designation or intent.

Responsibility of the School, College, or Business Unit

Restricted contribution revenues in excess of $2,000 are typically tracked via a unique project in PantherSoft. Each project is assigned to a school, college, or business unit based on the donor's purpose and restrictions. The school, college, or business unit makes use of these funds to support the educational, research, and public service mission of the University and in accordance with the donor's designation or intent. Deans and faculty members often work with the Foundation Development Office during the solicitation of potential donors. The school, college, or business unit utilizing these funds are aware of the donor's designation or intent and are responsible for adhering to these restrictions. The school, college, or business unit serves as the first level of approval before any request for disbursement is submitted to the Foundation Finance Office.

OBSERVATIONS AND RECOMMENDATIONS

Our overall assessment of internal controls is presented in the table below. In summary, we noted that the Foundation has adequate procedures and controls in place to ensure compliance with donor confidentiality and intent. However, opportunities for improvement exist in the Information Technology controls, specifically identity access management, audit logs, and business continuity plan. The areas tested during the audit and our observations and recommendations are detailed on the following pages.

CRITERIA	SATISFACTORY	OPPORTUNITES TO IMPROVE	INADEQUATE
Process Controls	X		
Policy & Procedures Compliance	X		
Effect	X		
Information Risk	X		
External Risk		X	

INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**OPPORTUNITES TO IMPROVE**	**INADEQUATE**
Process Controls (Activities established mainly through policies and procedures to ensure that risks are mitigated and objectives are achieved.)	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance (The degree of compliance with process controls – policies and procedures.)	Non-compliance issues are minor	Non-compliance issues may be systematic	Non-compliance issues are pervasive, significant, or have severe consequences
Effect (The potential negative impact to the operations- financial, reputational, social, etc.)	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk (The risk that information upon which a business decision is made is inaccurate.)	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 (Risks arising from events outside of the organization's control; e.g., political, legal, social, cybersecurity, economic, environment.)	None or low	Potential for damage	Severe risk of damage

Areas Within the Scope of the Audit Tested Without Exception:

Compliance with Donor Intent

Use of Gifted Funds

A total of $104.9 million was recognized in contribution revenues, net of the discount, for the period July 1, 2016, through January 31, 2020. We selected a sample of 25 projects, with contributions totaling $39.2 million, to determine if donors' philanthropic gifts were used according to donor intent and did not remain dormant in Foundation accounts. Based on our review:

- Twenty-three (23) of 25 projects selected reflected ongoing activity.

- For the two (2) remaining projects, we noted that although there was no activity during the period reviewed, plans were in place to use those funds for specifically timed activity. We offer the following details related to these two projects:

    - As of January 31, 2020, the Medina Aquarius project for the College of Arts and Sciences and Education (CASE) had a fund balance of $286,020, which had not been used from July 1, 2017, through January 31, 2020. CASE Management is aware of the remaining funds and has plans to use the remaining funds to remove the underwater laboratory that is approaching the end of its life. We reviewed the gift agreement and noted the funds are meant to support operating expenses of the Aquarius undersea laboratory and no time limitations had been placed on the use of funds. Although not required per the agreement, we noted that no supporting documentation was provided, for instance, a quote of estimated costs or communication by management where this carryforward balance plan is discussed.

    - As of January 31, 2020, Phase II of the Steven J. Green School of International & Public Affairs (SIPA) building project had a fund balance of $15 million with no use of funds of the project from July 1, 2016, through January 31, 2020. We reviewed the gift agreement and noted the funds are meant for the construction of the SIPA building Phase II. Per management, SIPA is aware of the remaining funds. In October 2019, FIU broke ground for Phase II of the SIPA Building. Construction has not yet begun; however, it is expected to start next year. Appropriate support was provided to show plans for the use of funds going forward.

Expenditures

We selected 42 expenditure transactions, totaling $2.8 million, from the sample projects to review for compliance with the donor agreements. Of the 42 transactions selected, there were 14 payroll transactions, totaling $235,475. We reviewed these transactions to ensure the employees paid reported to the appropriate department and the expenditures were in conformance with the gift agreement and donor intent. The remaining 28 expenditure transactions, totaling $2,593,902, were reviewed to ensure adherence with University policy and procedures, appropriate business units and Foundation Finance Office approvals were obtained, and the expenditure was in conformance with the gift agreement and donor intent.

We determined that controls related to the disbursement of funds were appropriate, as employees reported to the correct department and expenditures were in conformance with the gift agreement and donor intent.

Information Technology Controls

Segregation of Duties

According to NIST SP800-53A (Rev. 4) AC-5, *Separation of Duties*, an organization should:

- identify duties of employees that should be separated;
- separate organization-defined duties of individuals; and
- define information system access authorizations to support separation of duties.

We observed the definition of 18 distinct roles created in Raiser's Edge to support segregation of duties. The roles observed in the application allow privilege separation by allowing for defining and delineating application roles and tasks so that access is only granted to specific, discrete parts of systems or data, as is necessary.

In addition, we selected a sample of 40 user accounts from 158 (25%) total active Raiser's Edge users as of July 31, 2020, and obtained copies of available PantherSoft position descriptions and titles. We determined that the duties of all individuals were defined and that the users were granted the appropriate level of access to read only, run queries, export data, and make global changes that aligned with their job duties. None of the users examined could bypass the applications controls to create user accounts. This function is reserved for administrative users.

To verify the enforcement of segregation of duties within the Raiser's Edge application, we selected one user with Level 2/Development access and one user with Supervisor access as of July 31, 2020, and conducted a walkthrough. We observed that both users were assigned the appropriate level of access in Raiser's Edge and could only

access specific parts of the system for which they were authorized, based on their job functions. Therefore, the Foundation demonstrated proper segregation of duties.

Least Privilege

The NIST SP800-53A (Rev. 4) AC-6, *Least Privilege*, recommends that an organization employ the principle of least privilege. This principle allows only authorized access for users that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

To verify that the principle of least privilege was applied, the same sample of 40 active users were reviewed. We verified that there was an adequate and effective onboarding and offboarding process that provided appropriate roles which aligned to the employees' job responsibilities.

We observed that the position descriptions of the selected users matched the current level of access in Raiser's Edge and conform with the principle of least privilege. Additionally, due to their inherent risk of extraneous access privileges, we selected the accounts of all three Raiser's Edge administrators and determined that their levels of access were appropriate based on their job responsibilities. In addition, all access for transferred and terminated users appears to be appropriate under current employment conditions. All terminated users access to Raiser's Edge were disabled. No deficiencies were found.

User Training

To protect the confidentiality, privacy, and integrity of data processed through Raiser's Edge and to gain access to the system, the Foundation's Standard Operating Procedures (SOP) mandates that new employees attend Raiser's Edge Level 1 training. Further, additional access is granted if employees attend additional trainings.

The level of training completed by a user will typically correspond to their assigned role in Raiser's Edge. Features of the role must match the employee's job description within the University. There are three different training levels:

- Level 1 – View
- Level 2 – Queries
- Level 3 – Bio Updates

We obtained a copy of the Foundation's Raiser's Edge onboarding procedures, training material, and a list of all active users. We selected all 17 users who were added to Raiser's Edge between January 1, 2020, and July 31, 2020, and noted the date each user was added and the current permission level. This information was crossed-referenced to information contained on the training logs (courses offered and dates of attendance), along with corresponding emails, and we found that all the users received training prior to obtaining access to Raiser's Edge.

As a result, we determined that the Foundation is following its established SOP to preserve the integrity of data and reduce the risk of exposing donor information.

Security Breach Incident Response

Blackbaud provides a software solution that is widely used for fundraising and alumni or donor engagement efforts at non-profits, universities, healthcare organizations and foundations nationwide. On July 16, 2020, Blackbaud notified the Foundation that in May 2020, they discovered and stopped a ransomware attack affecting many of their clients worldwide, including the FIU Foundation. Blackbaud's investigation concluded that the cybercriminal removed data from their systems, intermittently, between February 7, 2020, and May 20, 2020. Blackbaud stated the cybercriminal was paid to ensure the backup file was permanently destroyed and that they had no reason to believe that any data went beyond the threat actor, was or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud confirmed that a copy of FIU's ResearchPoint backup was part of the incident. The compromised information consisted of 960 donors' first name, last name, address, and in some cases date of birth.

In accordance with FIU Policy 1930.021, *Incident and Breach Response*,

> *"This Plan should be used by a Responding Party whenever he or she develops a reasonable basis to anticipate that an incident or a series of incidents may have resulted in a Privacy Breach. The Incident Response Team should be notified as soon as possible, but no more than 24 hours after discovery. In the event that the Responding Party needs to address immediate concerns related to the Privacy Breach, it shall be within the discretion of the Responding Party to modify the timelines in order to protect the individuals impacted by the Privacy Breach; however, there is no Privacy Breach scenario that bypasses the requirement to notify the Incident Response Team. Florida has a 30-day notification requirement, so timely engagement of the Incident Response Team is critical. Further, communications should be limited to the Incident Response Team and others on a need to know basis only with careful consideration as to what should be communicated verbally or documented in writing."*

Upon receiving notification from Blackbaud of the data breach, the Foundation immediately notified the University's Chief Information Security Officer, who in turn, immediately activated the Incident Response Team (IRT). The IRT confirmed the data breach and that no FIU donor data hosted on premises were lost or corrupted. The IRT and University ensured the required notifications were issued to the affected parties, in accordance with the foregoing FIU policy.

Areas Within the Scope of the Audit Tested With Exception:

1. Identity Access Management

FIU IT Security Procedure 1930.02b, states the following:

> *"Individuals who have been granted physical or electronic access to a University IT resource by being personally issued a specific access code or codes shall not share the access code(s) with any other person. No individual should ask you for your access code(s) for any purpose.*
>
> *No one should access any University IT resource using another person's access code(s) and must read and adhere to the Guidelines for Password Management."*

As part of Identity Access Management, we reviewed policies and procedures to verify that user identity and logical access is managed and that all account access is appropriately established, modified, and disabled in a timely manner in accordance with NIST SP 800-53A (Rev. 4) AC-2, *Account Management*.

During the audit, we performed a walkthrough at a college that uses Raiser's Edge and FPM software to manage donor information. Our walkthrough disclosed that FPM allows two employees (development and support staff) of this college to run queries on the Raiser's Edge database to identify suitable donors and determine fundraising performance at FIU. We observed that the employees did not have the ability to create or modify any donor, prospect, or gift data within the platform. The two users selected, both have Level 2 access in Raiser's Edge that permit them to run queries on Raiser's Edge donor data. Therefore, their level of access to donor data in Raiser's Edge aligns with that in FPM.

However, during the walkthrough of FPM we discovered that the two employees shared the same credentials (i.e., username and password) to access the platform. While both users share the same Level 2 privileges and are authorized to view donor data within the Raiser's Edge database, the practice of sharing credentials to access FPM violates FIU IT Security Procedure 1930.020b.

Recommendation

The FIU Foundation should:	
1.1	Communicate with fundraising units throughout the University to reinforce the importance that users must refrain from sharing credentials in accordance with FIU IT Security Procedure 1930.020b and develop a mechanism to monitor compliance periodically.

Management Response/Action Plan

1.1 We concur with the auditor's recommendation. On September 18, 2020, the Division's IT Director sent an email to the Advancement Division (including fundraising units) regarding password security and management. This email included the IT Security Procedure 1930.020b and communicated the importance of strict adherence to this procedure. Management will review the available licenses to FPM and re-evaluate access accordingly.

Implementation date: November 30, 2020

Complexity rating: 1 - Routine

2. Audit Logs

Audit logs are chronological records of security-relevant data that document the sequence of activities affecting an operation, procedure, event, file, or document. A benefit of having audit logs is the ability to detect anomalies in systems' use and provide accountability.

We conducted a walkthrough of the Raiser's Edge application to determine if audit logs are available that would capture changes made by users to donor data. The software allows management to run queries that can assist in tracking user activity. We confirmed the existence of daily, weekly, monthly, and quarterly audit queries setup in the system to review missing, invalid, or changed attributes, such as city, gender, and address.

We observed the following:

- **Incomplete Audit Logs** - While the information in the Raiser's Edge query can be used to track down the user who last modified a record, the query is not granular. We observed the execution of a constituent query that allows an employee to view all modified constituent records within a specified time frame. The results of the query provide details such as when that constituent record was last modified by a particular user. However, the query results do not identify the specific attribute(s)/field(s) within the record that were modified. If two parties were to modify the same constituent record, we could not determine which fields either party modified. Furthermore, administrative actions taken using an administrator's credentials is not captured. In the event that an administrative account is compromised, having complete audit logs in place could aid in detecting the actions taken on the system with that account.

- **Deletion of records** - Raiser's Edge does not track deleted records. Keeping track of deletions would be beneficial to capture any errors leading to the deletion of data.

We found that these queries cannot provide full accountability for the modification of critical donor data and actions taken within the application. Without appropriate audit logs, activities can go undetected, and unauthorized actions taken by a user can be difficult to track.

Recommendation

The FIU Foundation should:	
2.1	Design and enable a formal audit logging detection control. This control should capture changes/deletions in critical fields and changes in user privileges, providing for accountability. In addition, there should be a documented management review of this process.

Management Response/Action Plan

2.1 We concur with the auditor's recommendation. Management is currently developing a process that captures changes/deletions to the donor database. In addition, a procedure will be created to document the review of these logs.

Implementation date: February 15, 2021

Complexity rating: 3 - Complex

3. Business Continuity and Disaster Recovery Plan

The purpose of a Business Continuity Plan (BCP) is to establish and maintain a plan to respond to incidents and disruptions to continue operations of critical business processes at an acceptable level in accordance with NIST SP800-53A Rev. 4, CP-1, *Contingency Planning Policy and Procedures*. On the other hand, the goal of a Disaster Recovery Plan (DRP), a significant part of the BCP, is to have a plan in place that allows for the restoration of critical data and applications that enable the institution to operate normally. Periodic review and testing of internal and external disaster recovery plans for information systems that are critical to the daily operations are essential to ensure the confidentiality, integrity, and availability of application data.

To prepare for, respond to, and recover from disasters, effectively, business units of the University are expected to execute a BCP and maintain procedures that are intended to accomplish the following:

- Where possible, prevent disasters through hazard mitigation planning.
- When disasters cannot be prevented, mitigate the impact to the University community resulting from such occurrences.
- Prepare staff to respond to disasters through training, outreach, and education.
- Restore essential University functions as quickly as possible to bring the Foundation back to operational status.

While we confirmed that the Foundation does perform scheduled backups of Raiser's Edge donor data that could potentially allow for the recovery of data in the event of an incident, we did not observe a written plan in place to enforce compliance with NIST SP800-53A Rev. 4, CP-1, *Contingency Planning Policy and Procedures*.

FIU Foundation was not able to provide a copy of their backup strategy and disaster recovery procedures. Documented restoration procedures for any database servers, access control servers, in-house applications servers, and third-party applications such as Raiser's Edge and Fundraiser Performance Management were not provided.

Recommendation

The FIU Foundation should:	
3.1	Design and formally document a BCP/DRP to ensure that it can respond to incidents and disruptions to continue operations of critical business processes.

Management Response/Action Plan

3.1 We concur with the auditor's recommendation. The current procedures and plans will be formalized in a comprehensive written document

Implementation date: January 2, 2021

Complexity rating: 2 - Moderate

Appendix I – Complexity Ratings Legend

Legend: Complexity of Corrective Action	
1	**Routine:** Corrective action is believed to be uncomplicated, requiring modest adjustment to a process or practice.
2	**Moderate:** Corrective action is believed to be more than routine. Actions involved are more than normal and might involve the development of policies and procedures.
3	**Complex:** Corrective action is believed to be intricate. The solution might require an involved, complicated, and interconnected process stretching across multiple units and/or functions; may necessitate building new infrastructures or materially modifying existing ones.
4	**Exceptional:** Corrective action is believed to be complex, as well as having extraordinary budgetary and operational challenges.

Appendix II – OIA Contact and Staff Acknowledgment:

OIA contact:

Joan Lieuw 305-348-2107 or jlieuw@fiu.edu

Contributors to the reports:

In addition to the contact named above, the following staff contributed to this audit in the designated roles:

Stephanie Price (auditor in-charge);
Henley Louis-Pierre (IT auditor in-charge);
Samual Pawlowski (assistant – student intern);
Tranae S. Rey (audit manager and reviewer);
Maria Rosa Lopez (IT audit manager and reviewer); and
Vivian Gonzalez (supervisor and reviewer).

Definition of Internal Auditing

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