Florida Board of Governors State University System

Florida International University
Internal Management and Accounting Control and Business Process Assessment

November 2019

Florida Board of Governors State University System
Florida International University (FIU) Internal Management and Accounting Control and Business Process Assessment
November 2019

I. Executive Summary

The Board of Governors (the "Board" or "BOG") of the Florida State University System (SUS) engaged Crowe LLP to perform a system-wide "Internal Management and Accounting Control and Business Process Assessment". The purpose of this assessment was to evaluate the existing internal controls and review business processes to identify any areas of risk for the SUS.

The scope of our assessment was focused on financial and operational risks, and regulatory compliance risks among the twelve universities within the SUS.

We have presented the results of our assessment of the Florida International University (FIU) in this report. We used our risk rating methodology to evaluate and score sixty-two (62) risks statements grouped into twelve categories. Our conclusions were based on the level of residual risk and any control gaps or weaknesses noted during our assessment. Residual risk refers to the level of risk after considering the internal controls in place and other activities implemented to mitigate that risk. An in-depth discussion of our approach and rating methodology can be found in the *Assessment Overview* section of this report.

Conclusion

While the scope of our assessment precludes us from issuing an opinion on FIU's system of internal controls, based on our procedures we noted no risk categories with a high level of residual risk, or significant control gaps or weaknesses in FIU's control structure.

We concluded that seven of the twelve risk categories we evaluated had a minor residual risk rating, and five categories had a low residual risk rating. We also found a few opportunities for FIU to strengthen internal controls, identified as "observations" in the table below. We have highlighted these observations as specific opportunities to improve controls or risk mitigation activities. The risk rating for each observation is indicative of the risk to university objectives posed by this gap in internal controls and is separate and distinct from the residual risk ratings in each category. Additional information on these observations, our recommendations to address them, and FIU management's responses can be found in the *Observations and Recommendations* section of this report.

FIU Observations Summary

Risk Category	Description	Risk Rating
Information Technology	**1. Configuration Management – Configuration Management Program. –** FIU has not documented a Configuration Management Program, which includes documented policies and procedures for system baseline and security configurations (hardening). This increases the risk of inconsistencies across network security configurations, which may expose FIU to vulnerabilities. FIU's current plan covers some areas (such as network, wireless and host configuration) but is not detailed in all areas, such as authentication controls.	Moderate
Information Technology	**2. Data Protection – Employee Mobile Device Management Policy.** FIU has not documented a Mobile Device Management policy for employees and contractors which details requirements for mobile device security. This increases the risk that sensitive FIU information may be compromised if a malicious actor gains access to the phone or other mobile device.	Low
Information Technology	**3. Information Security Governance – Cybersecurity Risk Management Program.** FIU has not implemented an IT and Cybersecurity Risk Assessment Program that defines cybersecurity risks, inherent risk (impact, threats, likelihood), and residual risk. FIU's current security risk management review is limited to two general topics of "Failure to maintain security" and "Failure to maintain confidentiality of information". This increases the risk that the university may not identify areas of high inherent risk and take the appropriate steps to prioritize and implement the appropriate mitigating controls.	Low
Information Technology	**4. Data Protection – Data Handling and Classification Policy.** FIU has not formally documented a Data Handling and Classification policy to prioritize the security of systems and allocate protection resources based on sensitivity.	Low

II. Assessment Overview

The Board of Governors (the "Board" or "BOG") of the Florida State University System (SUS) engaged Crowe LLP to perform a system-wide "Internal Management and Accounting Control and Business Process Assessment". The purpose of this assessment was to evaluate the existing internal controls and review business processes to identify any areas of risk for the SUS. We performed these consulting services in accordance with the Standards for Consulting Services established by the American Institute of Certified Public Accountants. These services do not constitute an audit, review, or examination in accordance with standards established by the American Institute of Certified Public Accountants, and therefore, Crowe did not express an opinion on the accuracy or efficacy of the material assessed during the performance of these services.

The scope of our assessment was focused primarily on financial and operational risks, and secondarily on regulatory compliance risks. It included the twelve universities within the SUS as follows:

- Florida Agricultural and Mechanical University (FAMU)
- Florida Atlantic University (FAU)
- Florida Gulf Coast University (FGCU)
- **Florida International University (FIU)**
- Florida Polytechnic University (FPU)
- Florida State University (FSU)
- New College of Florida (NCF)
- University of Central Florida (UCF)
- University of Florida (UF)
- University of North Florida (UNF)
- University of South Florida (USF)
- University of West Florida (UWF)

This report represents the results of our assessment of the Florida International University (FIU). As part of our assessment, we obtained an understanding of BOG regulations, university policies, procedures, processes and business requirements. In addition, we sent surveys and conducted interviews with various members of FIU management. Based on this information we developed a risk and control assessment, summarized below.

Inherent Risk Assessment

We developed an inherent risk assessment for each university in the SUS. The inherent risk assessments consisted of a list of risk factors which, based on our research and experience, are relevant, impactful, and likely to occur in a university environment. We rated some inherent risks differently across universities due to environmental or organizational variables (e.g. research-based universities, student enrollment, campus location(s), age of infrastructure, student housing, etc.). At this point in the assessment we did not yet consider the specific risk management and controls that each university had in place to mitigate these risks. It was designed to provide a baseline upon which to measure control effectiveness at the university level.

Risk Rating Scale

Impact	Score
Low	1
Minor	2
Moderate	3
High	4
Severe	5

Likelihood	Score
Remote	1
Improbable	2
Possible	3
Probable	4
Almost Certain	5

Risk Rating	Score
Low	1
Minor	2
Moderate	3
High	4
Severe	5

We established the threshold for reportable risk levels at a residual risk score of 4 or higher.

We established a risk rating methodology to assign a score to each risk factor in the assessment as illustrated above. Our risk rating methodology considered two criteria, “Impact” and “Likelihood”. The “Risk Rating” represents the average of those two scores. The impact criterion addressed the effect on financial, operational, or compliance objectives if the risk factor were to occur. The likelihood criterion addressed the probability that the risk would occur in the current environment. Our scores were based on a five-point rating scale with one (1) representing the lowest, and five (5) representing the highest risk score. We labeled the risk rating in the same manner as the impact criterion for the purpose of simplicity and consistency.

Control Ratings

We also rated the effectiveness of controls according to the three criteria below. The percentage assigned to each rating represents the reduction in perceived levels of risk and was used to calculate the residual risk score.

- No Observations Noted (30% reduction to the inherent risk rating),
- Needs Improvement (15% reduction to the inherent risk rating), or
- Inadequate (0%, no reduction to the inherent risk rating)

We based the control effectiveness ratings on the results of our research, discussions with management, and the supporting documentation they provided to help us analyze FIU’s control structure.

Residual Risk Assessment

We assigned a control rating to each control to arrive at a residual risk rating in a consistent manner. The residual risk assessment was intended to provide an overview of the university’s risk management and system of internal control. We recognized that each control and its related risk had unique components that would not be fully represented by the control or residual risk rating. Therefore, we developed an observation and recommendation for controls rated as “Needs Improvement” or “Inadequate” in order to provide additional insight into that specific matter.

We used the risk category ratings, as illustrated in **Exhibit 1** below, to summarize the sixty-two (62) risk statements which we evaluated and scored during this assessment. We assessed the risk factors from the perspective of "inherent risk" (i.e. prior to considering implementation of controls) and "residual risk" (i.e. after consideration of controls in place to mitigate the risk). In total we grouped risks into twelve categories and deemed seven categories to have a minor level of residual risk and five categories to have a low level of residual risk. FIU's three highest categories of residual risk were Information Technology, Investment Management, and Procurement. However, based on our methodology, all risk categories were below our threshold for a reportable observation.

The bar graph illustrates the difference between the average inherent and residual risk scores for each risk category. Please note that if an individual risk factor exceeded the threshold, we would have reported an observation and recommendation for those factors. However, we did not note any individual risk factors that exceeded the threshold, and these key functions/risk categories also have average residual risk scores below our threshold. This is an indicator that our observations identified were not systemic to the functional area.

Exhibit 1: FIU Inherent vs. Residual Risk by Category

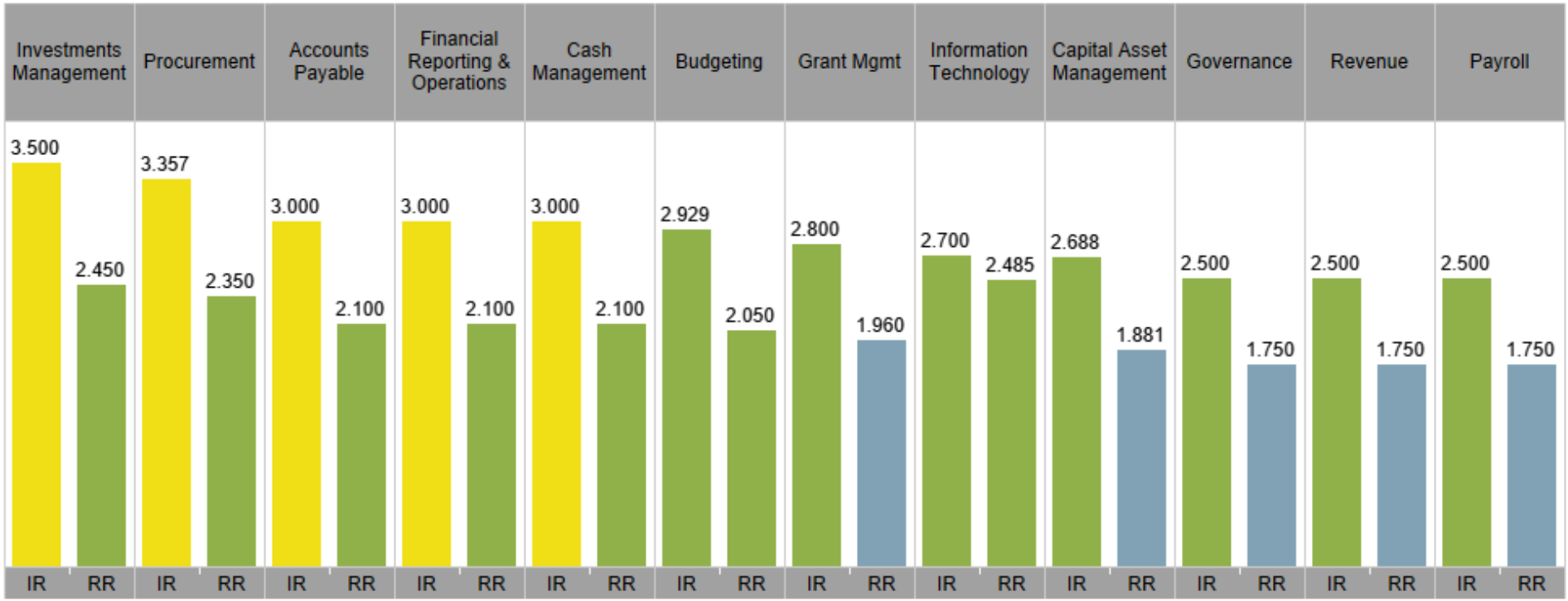

Exhibit 2 highlights similar information but uses different visualizations to illustrate how the control rating reduced the level of inherent risk (i.e. resulting in the residual risk score). The inherent risk represents the baseline score in each category prior to considering internal controls. The control mitigation score represents our assessment of the controls in each category. The residual risk score is the net result of the two scores and is used to indicate whether the control structure was adequately designed to mitigate the associated risks to a reasonable level. Again, this exhibit indicates that all risk categories had average residual risks below our threshold for reportable observations.

Exhibit 2: FIU Inherent vs. Residual Risk with Control Effectiveness Score

Risk Factor Category	IR	Control Mitigation Effectiveness	RR
Accounts Payable	3.000	0.300	2.100
Budgeting	2.929	0.300	2.050
Capital Asset Management	2.688	0.300	1.881
Cash Management	3.000	0.300	2.100
Financial Reporting & Operations	3.000	0.300	2.100
Governance	2.500	0.300	1.750
Grant Mgmt	2.800	0.300	1.960
Information Technology	2.700	0.175	2.485
Investments Management	3.500	0.300	2.450
Payroll	2.500	0.300	1.750
Procurement	3.357	0.300	2.350
Revenue	2.500	0.300	1.750

Conclusion

Based on our procedures, we noted no individual risk factors which arose to the level of a reportable observation (i.e. a residual risk score of 4 or greater). However, our risk and control assessment enabled us to identify a few areas to improve risk management and control practices. Additional detail on these observations, our recommendations on how FIU could address these observations, and FIU management's responses to our recommendations have been provided in the *Observations and Recommendations* section of this report.

We believe that FIU would benefit from strengthening its control structure over Information Technology risks with a few policy and program enhancements. Areas where we identified gaps included enhancing to a comprehensive baseline and security configuration program, in addition to a more thorough cybersecurity risk management program. A policy should also be established for enterprise-wide mobile device management, as well as data handling and classification. These policies will assist the university in prioritizing security.

III. Objectives and Scope

The purpose of this assessment was to evaluate the existing internal controls and review business processes to identify any areas of risk for the SUS. We accomplished this by completing a risk and control assessment for each university within the SUS, which enabled us to identify gaps or weaknesses in internal controls and make recommendations to the university and the BOG for improvement. In summary, our objectives were to evaluate the risks, controls, and business processes related to financial accounting and operations at FIU, and to provide observations and recommendations to the FIU Board of Trustees, FIU leadership, and the BOG on improving the risk management, controls, and business processes within the university.

The scope of our assessment included the following activities and processes at FIU:

1. Internal Management and Accounting Controls over:
    a. Accounting Operations (e.g. Accounts Payable, Accounts Receivable, Payroll)
    b. Financial Statement Preparation and Issuance
    c. Grant Management
2. Business Processes and Operations, including:
    a. Procurement
    b. Budget Management and Oversight (Capital and Operating)
    c. Capital Program and Asset Management
    d. Information Systems Management
    e. Cyber Security
    f. Contract Management
3. Compliance matters, including:
    a. Data Privacy rules and regulations
    b. Federal and State Grant reporting requirements
    c. Financial Aid regulations

IV. Procedures Performed

It should be recognized that internal controls are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur, and that procedures are performed in accordance with management's intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal controls. In the performance of most control procedures, errors can result from misunderstanding of instructions, mistakes in judgment, carelessness, or other factors. Internal control procedures can be circumvented intentionally by management with respect to the execution and recording of transactions, or with respect to the estimates and judgments required in the processing of data. Controls may become ineffective due to newly identified business or technology exposures. Further, the projection of any evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, and that the degree of compliance with procedures may deteriorate A summary of the procedures we completed during our assessment of FIU have been summarized in the table below.

Summary of Procedures
1. We reviewed BOG regulations, university policies, procedures, processes and business requirements.
2. We prepared an inherent risk assessment, which includes risks arising from our assessment of the above, as well as our experience in common risks within higher education, specific to financial and operational issues.
3. We analyzed risk/control questionnaires completed by university management and identified key controls in place to manage the risks identified above.
4. We conducted interviews onsite with university management for insight into risk management and control perspectives and activities.
5. We evaluated FIU's risk management and control structure based on the information gathered above.
6. We have identified gaps in controls and process improvement opportunities. These have been documented in this report as observations and recommendations.
7. We have confirmed with FIU management the factual basis for our observations and recommendations. Management's written responses are included for each recommendation in this report.

V. Observations and Recommendations

Our procedures yielded four (4) observations which are summarized in the table below. These observations represent areas where we determined that controls were absent or were not adequate to mitigate the associated risk to an acceptable level. In the following section we have provided details and recommendations to address each of these observations. Management's responses to each of our recommendations are also included in this section.

Risk Category	Description	Risk Rating
Information Technology	**1. Configuration Management – Configuration Management Program**	Moderate
Information Technology	**2. Data Protection – Employee Mobile Device Management Policy**	Low
Information Technology	**3. Information Security Governance – Cybersecurity Risk Management Program**	Low
Information Technology	**4. Data Protection – Data Handling and Classification Policy**	Low

Observations and Recommendations

Observation 1	Process Area	Priority Rating
Configuration Management – Configuration Management Program	Information Technology	Moderate

Condition: FIU has not documented a Configuration Management Program, which includes documented policies and procedures for system baseline and security configurations (hardening). This increases the risk of inconsistencies across network security configurations, which may expose FIU to vulnerabilities. FIU's current plan covers some areas (such as network, wireless and host configuration) but is not detailed in all areas, such as authentication controls.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 CM-1 as the criteria upon which to evaluate these controls.

Root Cause: FIU has not prioritized the standardization of forming a Configuration Management Program.

Implication: Information systems may not be configured with industry security standards, resulting in configuration inconsistencies across the network increasing the risk of vulnerabilities.

Recommendation: FIU should formally document the organization's configuration requirements based on industry best practices. FIU should implemented a process to document information system baselines standards (Operating System [OS] images or checklist) when deploying information system assets. These baselines or checklists should be pro-actively updated for information system assets (networking devices, servers, and workstations) on a periodic basis. Additionally, security configuration standards (hardening guides) should be referenced when developing system baselines. Information system baselines should be updated during the following conditions:

- Operating system updates;
- Critical software updates;
- New software implementation; and
- New security tool implementation(s).

Security configuration standards should also be applied to all baselines. Following security configuration standards helps to mitigate risk to systems before systems are implemented on the network.

Management Response:

Management agrees. FIU will document our configuration management requirements by December 31, 2019 and will have a configuration management policy in place by March 31, 2020.

Planned for implementation by April 2020.

Observation 2	Process Area	Priority Rating
Data Protection – Employee Mobile Device Management Policy	Information Technology	Low

Condition: FIU has not formally documented a Mobile Device Management policy, which details requirements for the security of mobile devices, specifically phones as FIU users access their FIU email with their personal phones.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 AC-19 as the criteria upon which to evaluate these controls.

Root Cause: FIU has not prioritized formally documenting a Mobile Device Management policy.

Implication: Users who use FIU email on their phones without adequate protections, are at risk of compromising FIU information if an attacker gains access to the phone or other mobile device, both physically and remotely.

Recommendation: To ensure the confidentiality and integrity of electronic data stored on mobile devices, FIU should develop a policy to inform users of the required security controls to use FIU email on their personal phones. This should include, but not limited to, full disk encryption, a secure PIN, and a lockout policy.

Management Response:

Management partially agrees. FIU does have documentation on required security controls to use the FIU VPN. FIU will develop a Mobile Device Policy and have it effective by March 31, 2020.

Planned for implementation by April 2020.

Observation 3	Process Area	Priority Rating
Information Security Governance – Cybersecurity Risk Management Program	Information Technology	Low

Condition: FIU has not implemented an IT and Cybersecurity Risk Assessment Program that defines cybersecurity risks, inherent risk (impact, threats, likelihood), and residual risk.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 PM-9 as the criteria upon which to evaluate these controls.

Root Cause: FIU has not prioritized resources to create a Cybersecurity Risk Management Program.

Implication: The organization may not be able to identify areas of high inherent risk and take the appropriate steps to prioritize and implement the appropriate mitigating controls.

Recommendation: FIU should institute a cybersecurity risk assessment process to determine compliance with the company's security requirements and controls. The risk assessment program should include requirements for determining risk, performing assessments to measure control effectiveness, and establishing a risk tolerance threshold.

The cybersecurity risk assessment process should consider:

1. The criticality of the system;
2. The sensitivity of the information processed;
3. The value of the system or application;
4. The threats associated with the system or application;
5. The likelihood of the threats occurring, and the potential damage of an incident derived from the threat;
6. The system's exposure to the threat;
7. The system's or application's vulnerabilities; and
8. The system interfaces and extent of system interconnections, including internal and external dependencies.

The result(s) of the risk assessment should include:

9. Residual risk and risk level (i.e., high, moderate, or low, for each risk).
10. Findings identified based on lack of controls or non-compliance with required controls to reduce the inherent risk.
11. Finding Action Plan – The action taken to remediate, transfer, mitigate or accept the risk.

The annual security assessment should be performed for all information systems to determine the control effectiveness of the security controls and ensure that they are functioning properly. FIU should use the outcome of this assessment to prioritize information security initiatives to reduce the overall risk profile.

Management Response:

Management partially agrees. FIU does have a risk registrar for IT-related risks and inherent risk. FIU will formalize and document the Cybersecurity Risk Management Program by June 30, 2020.

Planned for implementation by July 2020.

Observation 4	Process Area	Priority Rating
Data Protection – Data Handling and Classification Policy	Information Security	Low

Condition: FIU has not formally documented a data handling and classification policy.

Criteria: We relied on the ISO 27001 A 8.2.1 as the criteria upon which to evaluate these controls.

Root Cause: FIU has not prioritized resources to create a data handling and classification policy.

Implication: A lack of formal data classification and handling program can result in data being mishandled and exposed to unauthorized people.

Recommendation: FIU should define a data classification scheme to help prioritize the security of systems and allocate protection resources based on sensitivity. An example of a data classification scheme could be:

- Public – types of information that should be open to the public for viewing and has no legal ramifications. Examples include press releases or job postings.
- Internal – types of information that should only be viewed from an employee perspective and although it is not illegal to disclose, it should be restricted. Examples include employment information such as salaries and benefits.
- Confidential – types of information that are disclosed on a need-to-know basis and have legal ramifications if exposed in an inappropriate manner. Examples include payment information and product designs.

By classifying data in such a way, FIU can more easily assess the risk and impact of data loss based on the respective classifications. Classification information should be incorporated into “bottom-up” risk assessment activities and the asset inventory so that personnel have a clear understanding of the potential security impact if a system or information is compromised.

To help facilitate safe data handling, Information Security should utilize the classification scheme to define handling requirements associated with the sensitivity and type of media (e.g. paper, email, etc.) being transferred. Classification information can also be used during the system hardening process and establish the minimum set of technical controls required to protect information of a given classification to outline what, where, and how data is stored and who should have access.

Once a clear classification scheme has been created, security tools that monitor data should be adjusted to match governance standards.

Management Response:

Management agrees. FIU does currently have a data classification draft policy which is currently under review. FIU will finalize and implement the data classification policy by March 31, 2020.

Planned for implementation by April 2020.

VI. Appendix - List of Interviewees at FIU

The following individuals were interviewed during our onsite visit to FIU the week of August 12, 2019. The name, title, and interview subject are included below for reference.

1. Capital Asset Management - John Cal, Associate VP, Facilities Management, Aime Martinez, Associate Vice President, Business and Finance, Edward Brozic, Director of Budget, Katharine Brophy, Controller, Alexandra Mirabal, Deputy Controller, Ramon Duenas, Associate Controller
2. Financial Operations and Reporting - Katharine Brophy, Controller, Alexandra Mirabal, Deputy Controller, Bonnie Bair, Asst. Controller
3. Cash Management - Katharine Brophy, Controller, Alexandra Mirabal, Deputy Controller, Jose Zumimendi, Assistant Controller, Leslie-Anne Triana, Professional Accountant III, Benjamin Jarrell, Treasurer
4. Investment Management - Katharine Brophy, Controller, Alexandra Mirabal, Deputy Controller, Bonnie Bair, Asst. Controller, Aime Martinez, Associate Vice President, Benjamin Jarrell, Treasurer
5. Payroll - Alexandra Mirabal, Deputy Controller, Ciro Castro, Assistant Controller, Carlos Flores, Assistant VP, HR Operations Compliance & Systems, Idorys Calvo, Director of Payroll
6. Revenue - Katharine Brophy, Controller, Alexandra Mirabal, Deputy Controller, Jose Zumimendi, Assistant Controller, David Snider, Assistant VP Auxiliary and Enterprise Development
7. Student Billing - Katharine Brophy, Controller, Natassia Martinez, Director, Student Financial Services & Systems
8. Internal Audit - Trevor Williams, CAE
9. Procurement - Katharine Brophy, Controller, Kelly Loll, Executive Director, Procurement
10. Accounts Payable - Katharine Brophy, Controller, Alexandra Mirabal, Deputy Controller, Ramon Duenas, Associate Controller
11. Information Technology - Robert Grillo, CIO, Carlos Varona, Director, Enterprise and Applications, Helvetiella Longoria, Interim Chief Info Security Officer
12. Grant Management - Andres Gil, VP, Research, Tonja Moore, Associate VP, Strategic Planning & Operations, Roberto Gutierrez, Assistant VP Research
13. Budgeting - Aime Martinez, Associate Vice President, Business and Finance
14. Governance – Jennifer LaPorta Baker, Chief Compliance Officer
15. FIU Board of Trustees Finance Committee Chair, Leonard Boord