Crowe

Smart decisions. Lasting value.™

Florida Board of Governors State University System

Florida Polytechnic University 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 Florida Polytechnic University (FPU) 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 FPU'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 FPU'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 opportunities for FPU 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 FPU management's responses can be found in the *Observations and Recommendations* section of this report.

FPU Observations Summary

Risk Category	Description	Risk Rating
Information Technology	**1. Information Security Governance – Policies and Procedures.** FPU has not documented information security policies and procedures for the sections pertaining to: 1) Data Protection, 2) Logging and Monitoring, 3) Risk Management, 4) Change Management Program 5) Patch Management and 5) Mobile Device Management. This increases the risk that tasks will be performed inconsistently.	Low
Information Technology	**2. Data Protection – Employee Removable Media.** FPU does not have a method to manage the use of removable media. Technical controls have not been implemented to protect the access and provide data protection, such as encryption and device authentication.	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 FPU. 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 FPU management. Based on this information, we developed a risk and control assessment, the results of which are 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 internal controls in place 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 ratings on the results of our research, discussions with management, and the supporting documentation they provided to help us analyze FPU’s control structure.

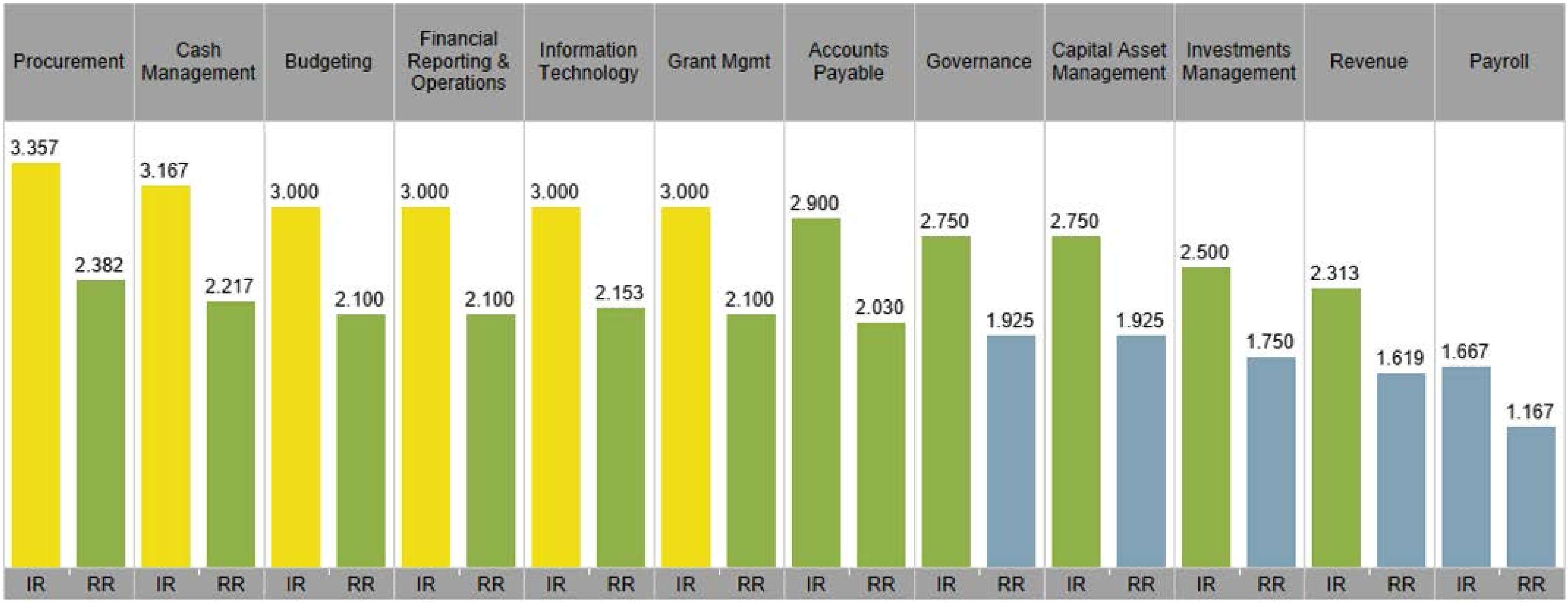
Residual Risk Assessment

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” 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. FPU’s three highest categories of residual risk were Procurement, Cash Management, and Information Technology. 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.

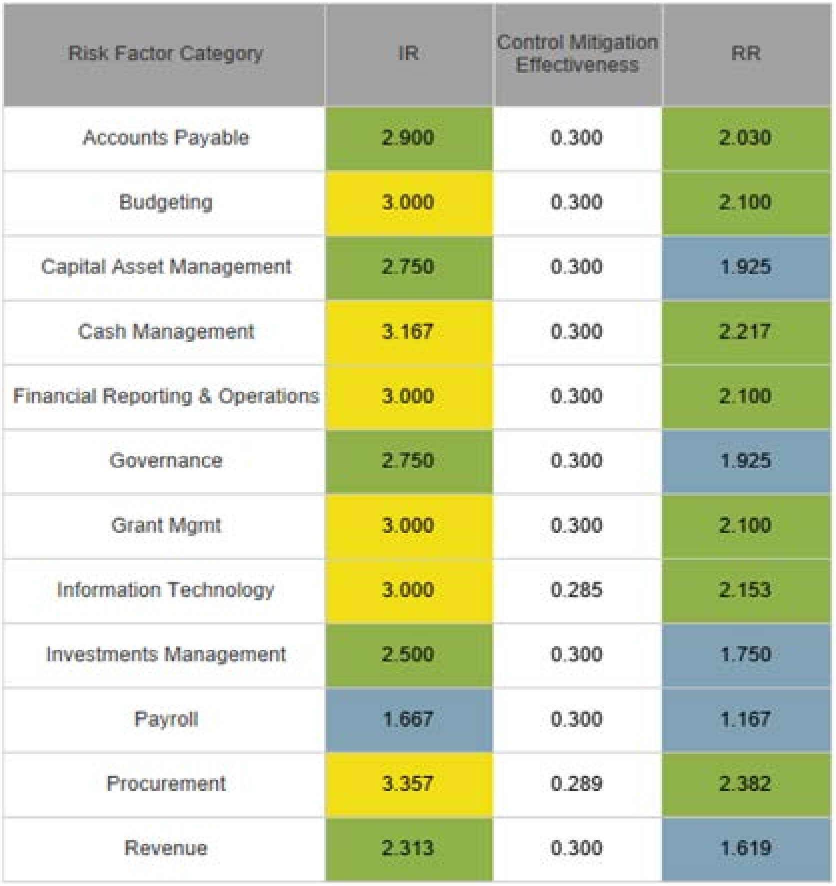
Exhibit 1: FPU Inherent vs. Residual Risk by Category



This report is furnished solely for the information and use of Florida Polytechnic University and the Florida Board of Governors. The report is not intended to be and should not be used by anyone other than these specified parties or entities.

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: FPU Inherent vs. Residual Risk with Control Rating



Risk Factor Category	IR	Control Mitigation Effectiveness	RR
Accounts Payable	2.900	0.300	2.030
Budgeting	3.000	0.300	2.100
Capital Asset Management	2.750	0.300	1.925
Cash Management	3.167	0.300	2.217
Financial Reporting & Operations	3.000	0.300	2.100
Governance	2.750	0.300	1.925
Grant Mgmt	3.000	0.300	2.100
Information Technology	3.000	0.285	2.153
Investments Management	2.500	0.300	1.750
Payroll	1.667	0.300	1.167
Procurement	3.357	0.289	2.382
Revenue	2.313	0.300	1.619

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 areas to improve risk management and control practices. Additional detail on these observations, our recommendations on how FPU could address these observations, and FPU management's responses to our recommendations have been provided in the *Observations and Recommendations* section of this report.

We also noted that the university would likely benefit from an enhanced focus in the Information Technology risk category. While we have addressed specific risks in our observations and recommendations, this is an area in which FPU could benefit from a more holistic approach to risk management. A strong risk management framework is critical to maintain pace with the threats that have emerged alongside technological advances. These threats pose not only financial risks, but may also impact reputation, safety, and strategic initiatives. FPU should consider strengthening their risk management practices through a more formal, systematic approach in order to provide an added level of assurance to its Board of Trustees and to the Board of Governors that the university has taken reasonable measures to manage the risks it faces in the course of pursuing its mission.

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 FPU, and to provide observations and recommendations to the FPU Board of Trustees, FPU 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 FPU:

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

This report is furnished solely for the information and use of Florida Polytechnic University and the Florida Board of Governors. The report is not intended to be and should not be used by anyone other than these specified parties or entities.

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 FPU 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 FPU'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 FPU 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 two (2) 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. Information Security Governance – Policies and Procedures**	Low
Information Technology	**2. Data Protection – Employee Removable Media**	Low

This report is furnished solely for the information and use of Florida Polytechnic University and the Florida Board of Governors. The report is not intended to be and should not be used by anyone other than these specified parties or entities.

Observations and Recommendations

Observation 1	Process Area	Priority Rating
Information Security Governance – Policies and Procedures	Information Technology	Low

Condition: Several policies and procedures have not been documented or need enhancement to reflect the current security configurations and industry standards. The following policies and procedures have not been documented:

- **Data Protection** – The organization does not maintain a documented data protection program which includes requirements for data inventory, data protection, and data sanitization.
- **Logging and Monitoring** – The organization does not maintain a documented logging and auditing requirements that includes the system types to be logged, procedures for log review, alerting thresholds, log retention requirements, and personnel to be alerted.
- **Risk Management** – The organization does not maintain a documented risk management program which includes documented risks, threats, and vulnerabilities.
- **Change Management Program** – The organization does not maintain a change management program with requirements which include documented change control criteria, functional testing, back-out procedures, and reporting.
- **Patch Management** – The organization does not maintain a documented patch management program that defines requirements for patch documentation, approvals, patch installation frequency, testing, exceptions, and emergency and critical patch processes.
- **Mobile Device Management** – The organization does not maintain a documented mobile device management program which includes standards for securing mobile devices and requirements for users to access company data from their mobile devices.

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

Root Cause: FPU has not yet prioritized resources to complete the development of the policies and procedures noted in the Condition above.

Implication: Lack of policies and procedures may result in potential conflicts when performing tasks due to inconsistent and/or lack of documentation. Policies help constitute what is acceptable behavior and formalized and up-to-date procedures provide guidance and clearly defined steps on how to execute the necessary task in a consistent manner.

Recommendation: FPU should develop policies and procedures around the noted program areas. These policies and procedures should, at a minimum, include the purpose, scope, roles and responsibilities, policy standards, violations, approval and ownership, and references (if applicable). Once the policy has been defined with approved security standards, Management should document procedures to verify the enforcement of the documented standards. At a minimum, Management should perform a yearly review, update, and approval of the policies and if applicable, the procedures, to reflect the current industry security standards and practices.

Management Response:

Management agrees. As a smaller institution, we mitigate risks by close managerial supervision. Based on Crowe's recommendation and their low-risk assessment, we have prioritized resources to complete the documentation of the policies and procedures noted in the Crowe observation by December 31, 2019.

Planned for implementation by January 2020.

Observation 2	Process Area	Priority Rating
Data Protection – Employee Removable Media	Information Technology	Low

Condition: FPU does not have a method to manage the use of removable media. Technical controls have not been implemented to protect the access and provide data protection, such as encryption and device authentication.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 MP-1, MP-2, MP-5, MP-7 as the criteria upon which to evaluate these controls.

Root Cause: FPU has not prioritized resources to address the risk of employees using removable media.

Implication: Without restrictions and the protection of data confidentiality on the use of removable storage media through device encryption, there is the risk of unauthorized disclosure of business and customer information through the loss or misuse of the storage media.

Recommendation: To ensure the confidentiality and integrity of electronic data stored on a removable media, FPU personnel should only use encrypted devices and their use should be restricted (for both read and write capabilities) to only authorized individuals who have a legitimate business need. Removable media should also be centrally managed, and only company devices should be used. To account for all files that may be considered sensitive, technical controls should be implemented to force removable media encryption and reduce the risk of sensitive files being lost. Removable media encryption solutions are listed below:

USB Encryption Solutions	
DiskCryptor	https://diskcryptor.net/wiki/Main_Page
Rohos Disk Encryption	https://www.rohos.com/products/rohos-disk-encryption/
PGP Disk	http://www.symantec.com/encryption/
Gilisoft USB Stick Encryption	http://gilisoft.com/product-usb-stick-encryption.htm
Kakasoft USB Security	http://www.kakasoft.com/usb-security/
Iron Key (Encrypted USB)	http://www.ironkey.com/en-US/

Alternatively, if there is no business need for removable media, it can be restricted using third party tools or through Microsoft Group Policy. The following article provides a walkthrough on how this can be accomplished:

- https://technet.microsoft.com/en-us/library/Cc772540(v=WS.10).aspx

Management Response:

Management partially agrees. All University employees receive and sign written guidance on the proper handling of removable media. The University adopted Data Classification and Protection Policy FPU-11.00122P that requires that the “highest level of access and security controls and protection will be applied both in storage and in transit,” and we have trained University employees on that policy. Based on Crowe’s recommendations, the University partially agrees and is exploring removable media management software to determine if the benefit exceeds the cost, considering the low-risk assessment noted by Crowe.

Timeline for implementation has not yet been determined.

This report is furnished solely for the information and use of Florida Polytechnic University and the Florida Board of Governors. The report is not intended to be and should not be used by anyone other than these specified parties or entities.

VI. Appendix - List of Interviewees at FPU

The following individuals were interviewed during our onsite visit to FPU the week of July 29, 2019. The name, title, and interview subject are included below.

1. Accounts Payable & Procurement:
    a. David O’Brien– Director of Procurement
    b. Treasa McLean – Assistant Director of Procurement
    c. Laura Marrone – Associate Director of Procurement
    d. John Irvine – Director of Finance and Accounting, Accounts Payable, & Construction
2. Cash Management:
    a. Derek Horton – University Controller
    b. John Irvine – Director of Finance and Accounting, Accounts Payable, & Construction
3. Budget and Financial Reporting:
    a. Regina Siewart, Budget Officer
    b. Derek Horton, University Controller
    c. John Sprenkle, Director of Finance and Accounting for Financial Reporting
4. Capital Asset Management:
    a. John Irvine – Director of Finance and Accounting, Accounts Payable, & Construction
    b. David Calhoun, Assistant Vice President of Facilities and Safety Services
5. Grants Management: Nicole Tardiff, Director of Sponsored Programs
6. Internal Audit and Compliance: David Blanton, Chief Compliance Officer and Chief Audit Executive
7. Information Technology: Ben Beachy, Chief Information Officer
8. Student Billing:
    a. Derek Horton, University Controller
    b. John Sprenkle, Director of Finance and Accounting for Financial Reporting
    c. Andrew Strazi, Director of Reporting and Analytics
9. Governance: FPU Board of Trustees Chair, Don Wilson

This report is furnished solely for the information and use of Florida Polytechnic University and the Florida Board of Governors. The report is not intended to be and should not be used by anyone other than these specified parties or entities.