Florida Board of Governors State University System

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

November 2019

Florida Board of Governors State University System
University of Florida (UF) 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 University of Florida (UF) 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 UF'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 UF's control structure.

We concluded that five of the twelve risk categories we evaluated had a minor residual risk rating, and seven categories had a low residual risk rating. We also found several opportunities for UF 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 UF management's responses can be found in the *Observations and Recommendations* section of this report.

UF Observations Summary

Risk Category	Description	Risk Rating
Information Technology	**1. Employee Management – Termination and Role Changes.** Currently, UF has not formally documented a procedure for the timely notification of IT of role changes or terminations to prompt removal of access within a timely manner (i.e. 24 hours) and user access reviews to ensure compliance with the principle of least privilege.	Low
Information Technology	**2. Employee Management – Employee Security Awareness Training.** UF requires training for employees before role access is granted to specific Restricted Data types, but UF has not established an Information Security Training Program to provide all employees with training on-hire and on an annual basis.	Low

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

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 University of Florida (UF). 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 UF 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.

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

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 UF’s control structure.

Residual Risk Assessment

We assigned a control effectiveness 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.

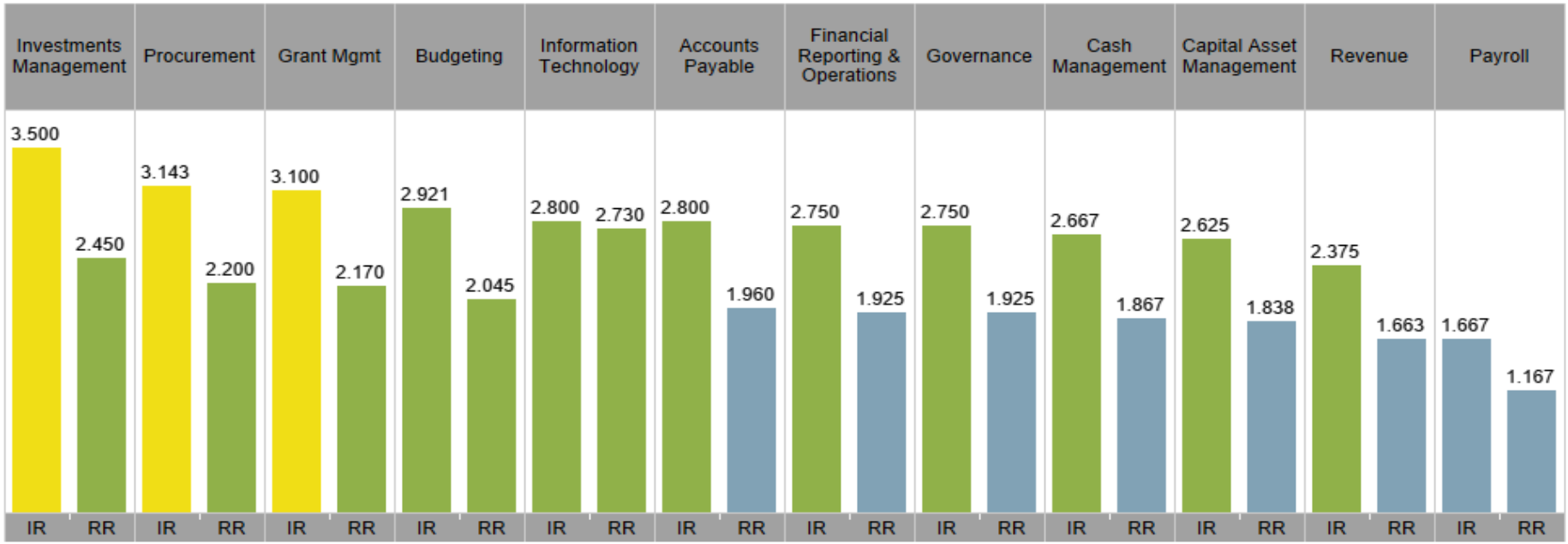
© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

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 five categories to have a minor level of residual risk and seven categories to have a low level of residual risk. UF'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: UF Inherent vs. Residual Risk by Category



© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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: UF Inherent vs. Residual Risk with Control Rating

Risk Factor Category	IR	Control Mitigation Effectiveness	RR
Accounts Payable	2.800	0.300	1.960
Budgeting	2.921	0.300	2.045
Capital Asset Management	2.625	0.300	1.838
Cash Management	2.667	0.300	1.867
Financial Reporting & Operations	2.750	0.300	1.925
Governance	2.750	0.300	1.925
Grant Mgmt	3.100	0.300	2.170
Information Technology	2.800	0.050	2.730
Investments Management	3.500	0.300	2.450
Payroll	1.667	0.300	1.167
Procurement	3.143	0.300	2.200
Revenue	2.375	0.300	1.663

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

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 UF could address these observations, and UF management's responses to our recommendations have been provided in the *Observations and Recommendations* section of this report.

We believe that UF would benefit from several high-value enhancements, such as establishing an Information Security Training Program to provide to employees with training on-hire and on an annual basis. An evolving, annual Security Training Program is critical to maintain pace with the threats that have emerged alongside the continuous advances in technology. These threats pose not only financial risks, but may also impact reputation, safety, and strategic initiatives.

Finally, we conclude that the university can improve administrative efficiencies with established policies and procedures. A couple areas where we noted a need for improvement was in an enterprise-wide established clean desk program and procedures for timely notification to IT of employee role changes/terminations. A clean desk policy established enterprise-wide can enhance the workplace security. Procedures over notifying IT of role changes and terminations can hold university employees to established standards to ensure timely offboarding of access.

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

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

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

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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 UF 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 UF'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 UF management the factual basis for our observations and recommendations. Management's written responses are included for each recommendation in this report.

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

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. Employee Management – Termination and Role Changes**	Low
Information Technology	**2. Employee Management – Employee Security Awareness Training**	Low

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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
Employee Management – Termination and Role Changes	Information Security	Low

Condition: UF has not formally documented a procedure for the timely notification of IT of role changes or terminations to prompt removal of access within a timely manner (i.e. 24 hours) and user access reviews to ensure compliance with the principle of least privilege. A process will be implemented by the end of calendar year 2019 to provide a report to the Departmental Security Administrators for all terminated and transferred employees that will assist a timely removal of roles and access granted at the departmental level.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 PS-4 as the criteria upon which to evaluate these controls.

Root Cause: UF has not prioritized documenting its practices for terminations and role changes due to its reliance on experienced staff members with substantial institutional knowledge.

Implication: Employees may retain permissions related to their old roles or maintain access to the organization's systems after the termination of their employment.

Recommendation: UF should continue the project plan for the implementation of a periodic report that will be provided to Departmental Security Administrators to facilitate a timely removal of roles and reconfiguration of access. Additionally, this process should be documented within a procedure to verify consistence for the removal or modification of access.

Management Response:

UF management disagrees with the observation. NIST 800-53 r5 referenced in this audit has not been released in a final version and is still under review by the Office of Management and Budget, Office of Information and Regulatory Affairs. Instead, UF conforms to the most current version, NIST 800-53 r4.

As stated previously, the university has documented standards and procedures for removal of inappropriate access upon termination of employees:

- The UF Account Management Standard requires that accounts and authorizations be promptly modified when a user's job duties change. https://it.ufl.edu/policies/information-security/related-standards-and-documents/account-management-standard/
- The UF HR Employee Exit Checklist includes steps to disable accounts. https://hr.ufl.edu/wp-content/uploads/2018/04/exit_checklist.pdf
- The information security risk assessment process addresses all aspects of data protection, including access management, using controls selected from NIST 800-53r4.
- Roles require an annual re-certification by the Departmental Security Administrator to verify the continued need for access.

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

UF began a multi-phase project in 2018 to implement improved processes for prompt removal of access rights. The first phase was implemented on January 30, 2019, to automate removal of roles that grant access to HR, Finance and Student systems the morning after a termination date occurs in PeopleSoft. The second phase, a report to Departmental Security Administrators (DSAs) of transferred employees to facilitate timely removal of inappropriate roles and access granted at the departmental level, was implemented October 31, 2019. As part of the second phase, an email was sent to all DSAs informing them of their responsibility to review and update enterprise security roles for transferred employees. The third and final phase is on target to be completed by December 31, 2019. Phase 3 will enhance the report to DSAs to include terminated employees.

It is important to note that many former employees retain their account access after separating from the university to services such as: Library, email, etc. Instances in which this is the case include retired faculty that are guaranteed continuing access by contract, and alumni that need the ability to access their educational records. Because of this, the university is focused on processes to remove roles, rights, and permissions that are no longer appropriate rather than termination of accounts.

Crowe Comment:
During our assessment, UF provided a standard and a checklist. They did not provide documented procedures, which is what the condition has referenced. While management's response indicates the basis for procedures that UF may utilize; based on the evidence provided there were no procedures for how the university or each business unit actually adhered to the standards provided.

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

Observation 2	Process Area	Priority Rating
Employee Management – Security Awareness Training	Information Security	Low

Condition: Although UF requires training for employees before role access is granted to specific Restricted Data types, UF has not established an Information Security Training Program to provide all employees with training on-hire and on an annual basis.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 AT-3 as the criteria upon which to evaluate these controls.

Root Cause: UF has not prioritized resources to address the risk of employees not receiving security awareness training.

Implication: Cybersecurity is a constantly changing field. If employees are not provided with continuous training, they may not be prepared to identify newer threats and tactics and can expose the organization to risk.

Recommendation: UF should implement an on-hire and annual security training program for all employees. This training should be updated at least annually to cover current cybersecurity threats. This program should include a holistic approach, with both periodic security awareness exercises and specialized training for IT skill development. Employees should be required to sign an acknowledgement of this training and these acknowledgements should be tracked to ensure compliance.

Management Response:

UF management partially agrees with the observation. NIST 800-53 r5 referenced in this audit has not been released in a final version and is still under review by the Office of Management and Budget, Office of Information and Regulatory Affairs. Instead, UF conforms to the most current version, NIST 800-53 r4.

As stated previously, UF requires role-based training for employees working with specific data types. This training is privacy-focused but includes security content. UFIT offers optional security awareness training in a variety of formats, including just-in-time, online and classroom delivered content.

UF provides the following required online role-based training:

- HIPAA & Privacy – General Awareness
- FERPA Basics
- FERPA for Faculty
- Protecting Social Security Numbers & Identity Theft Prevention
- Payment Card Security Awareness Training
- UF also provides optional security awareness training, available at https://training.it.ufl.edu/training/:
- UF Restricted Data Training
- Cyber Security at UF

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.

As an example, in calendar year 2019 alone, UFIT offered the following security awareness messaging to all employees:

- 10 UFIT News stories, published on https://news.it.ufl.edu/
- 5 stories in email (such as Faculty Update) sent to all faculty
- 7 stories in email (such as Gator Times) sent to all students
- 4 stories in email (such as UF at Work) sent to all staff
- 109 social media posts (Facebook, Twitter and Instagram)
- 5 live training events
- Various other placements, including The Alligator, UF Health Post, and UFH Villager

Additionally, UF has purchased KnowBe4 security awareness training, and will conduct simulated phishing exercises against faculty, staff and students and deliver just-in-time training. UF will provide mandatory security awareness training to all new hires. UF will also provide training to employees who demonstrate the need for additional training. UF will start mandatory training in July 2020.

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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 UF

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

1. Payroll – Alan West, Assistant VP and Controller, Brad Bennett, Sr. Assoc Controller, Scott Easton, Assoc. Controller
2. Bursar/Student Account/Billing/Student AR - Alan West, Assistant VP and Controller, Brad Bennett, Sr. Assoc Controller, Terry Wooding
3. Cash Management & Investments – Mike McKee, CFO, Alan West, Assistant VP and Controller, Brad Bennett, Sr. Assoc Controller, Shane Anderson, Asst. Controller Ed Kelly, UFICO
4. Budget – George Kolb, Asst. VP
5. Accounts Payable – Alan West, Assistant VP and Controller, Randy Staples, Assoc. Controller
6. Planning, Design and Construction – Gene Herring, Director of Capital Programs and Financial Management, Curtis Reynolds, VP of Business Affairs
7. Construction Accounting & Capital Asset Management – Alan West, Assistant VP and Controller, Brenda Harrell, Asst. Controller, Ryan Parris, Asst. Controller
8. Preparation/Issuance of Audit Financial Statements – James House, Asst. Controller, Patrice Lecomte, Assoc. Controller, Alan West, Asst. VP and Controller
9. Revenue/Accounts Receivable – Patrice Lecomte, Assoc. Controller, Alan West, Asst. VP and Controller
10. Internal Audit – Joe Canella, Internal Audit
11. Information Technology – Rob Adams, CISO
12. Procurement – Lisa Deal, Asst. VP and Chief Procurement Officer, Nicola Heredia, Director
13. Grant & Regulatory Reporting Compliance – Tiffany Schmidt, Director of Sponsored Programs, Stephanie Gray, Asst. VP Sponsored Programs
14. Sponsored Program Accounts Receivable – Tiffany Schmidt, Director of Sponsored Programs, Stephanie Gray, Asst. VP Sponsored Programs
15. UF Board of Trustees Finance Committee Chair, Thomas Kuntz

© 2019 Crowe LLP

This report is furnished solely for the information and use of University of Florida 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.