Florida Board of Governors State University System

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

November 2019

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

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

UNF Observations Summary

Risk Category	Description	Risk Rating
Information Technology	**1. Data Protection – Mobile Device Management.** UNF 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 UNF information may be compromised if a malicious actor gains access to the phone or other mobile device.	Low
Information Technology	**2. Information Security – Clean Desk Policy.** UNF does not have a university-wide "clean desk" policy. This increases the risk that sensitive information may be viewed or accessed by unauthorized parties.	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 UNF. 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 UNF 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 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 UNF’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” 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 one category to have a minor level of residual risk and eleven categories to have a low level of residual risk. UNF's three highest categories of residual risk were Grant Management, Procurement, and Governance. 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: UNF Inherent vs. Residual Risk by Category

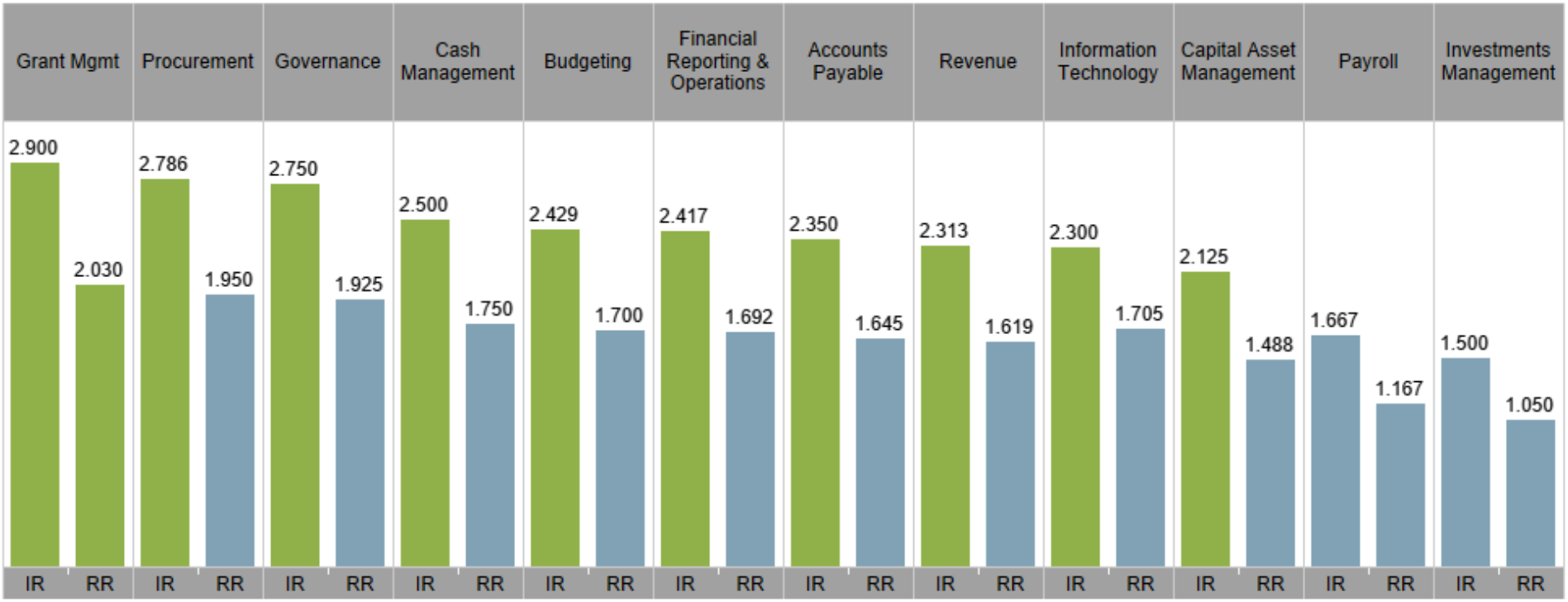

Exhibit 2 highlights similar information but uses different visualizations to illustrate how the control rating reduced the level of inherent risk (i.e. resulting in the residual risk score). The inherent risk represents the baseline score in each category prior to considering internal controls. The 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: UNF Inherent vs. Residual Risk with Control Rating

Risk Factor Category	IR	Control Mitigation Effectiveness	RR
Accounts Payable	2.350	0.300	1.645
Budgeting	2.429	0.300	1.700
Capital Asset Management	2.125	0.300	1.488
Cash Management	2.500	0.300	1.750
Financial Reporting & Operations	2.417	0.300	1.692
Governance	2.750	0.300	1.925
Grant Mgmt	2.900	0.300	2.030
Information Technology	2.300	0.265	1.705
Investments Management	1.500	0.300	1.050
Payroll	1.667	0.300	1.167
Procurement	2.786	0.300	1.950
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 several areas to improve risk management and control practices. Additional detail on these observations, our recommendations on how UNF could address these observations, and UNF management's responses to our recommendations have been provided in the *Observations and Recommendations* section of this report.

We believe that UNF would benefit from several low-cost, high-value enhancements such as:

1. Strengthening security policies around mobile computing,
2. Communicating policies and best practices for securing sensitive information (e.g. a clean desk policy), and
3. Training employees to be aware of and properly respond to security threats.

Finally, we conclude that with continuous advances in technology, universities can exponentially improve the level and reach of services to its students and increase administrative efficiencies. However, a strong risk management framework is critical to maintain pace with the threats that have emerged alongside the advances. These threats pose not only financial risks, but may also impact reputation, safety, and strategic initiatives. UNF 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 UNF, and to provide observations and recommendations to the UNF Board of Trustees, UNF 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 UNF:

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 UNF 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 UNF'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 UNF 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. Data Protection – Mobile Device Management**	Low
Information Technology	**2. Information Security – Clean Desk Policy**	Low

Observations and Recommendations

Observation 1	Process Area	Priority Rating
Data Protection – Mobile Device Management	Information Technology	Low

Condition: UNF has not documented a Mobile Device Management policy for employees and contractors, which details requirements for the security of mobile devices.

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: UNF has not prioritized resources to develop a mobile device management policy for its employees and contractors who use their personal mobile devices to access UNF email or other applications.

Implication: Employees or contractors who use UNF email on their phones without security protections are at risk of compromising UNF information if a malicious actor gains access to the phone, both physically or remotely.

Recommendation: UNF should develop a policy to inform users of the security controls that are required through the information security program for the user of UNF email on their personal phones. Information security standards should include, but not limited to, full disk encryption, a secure PIN, and a lockout policy. UNF should also consider using a Mobile Device Management solution. For example, while we do not endorse any specific products, the VMware ® AirWatch is one of many solutions that may be implemented to enforce these controls and remotely wipe devices in the event that they are lost or stolen.

Management Response:

We agree with the recommendation for a Mobile Device Management (MDM) policy. Accordingly, we are working toward updating our current policies to incorporate these issues. We should have these policy statements in place by the Spring of 2020. We also agree with the suggestion for a MDM solution. To that end, we had already initiated a project to implement such as solution.

Implementation Plan: We expect this project to be completed by Fall 2020 or Spring 2021.

Observation 2	Process Area	Priority Rating
Information Security – Clean Desk Policy	Information Technology	Low

Condition: Although some departments have clean desk programs, UNF has not created an enterprise wide clean desk program to enforce the standards across the organization.

Criteria: The audit evaluated controls utilizing regulator guidance and industry best practices, including the National Institute of Standards and Technology (NIST), NIST Cybersecurity Framework and SANS Critical Security Controls.

Root Cause: UNF has not yet prioritized resources to develop a university-wide clean desk policy.

Implication: Lack of a clean desk program can result in users leaving sensitive information where it can be viewed or stolen by unauthorized parties.

Recommendation: UNF should develop a policy to address how physical artifacts deemed sensitive in nature located around an employee's workspace need to be securely stored at the end of each day, or when the employee is away from their desk. The policy should be inclusive of all items that relate to private customer information, passwords, transaction records, private employee information, etc. Suggested requirements include, but are not limited to:

Management Response:

We agree with the recommendation for a Clean Desk Policy. We have already drafted a policy that is currently in the management review stage. Implementation Plan: We expect to have this policy published by Spring 2020.

VI. Appendix - List of Interviewees at UNF

The following individuals were interviewed during our onsite visit to UWF the week of June 24, 2019. The name, title, and interview subject are included below for reference.

1. Accounts Payable & Procurement:
    a. Valerie Stevenson, University Controller
    b. Shawn Asmuth, Director of Procurement
2. Budgeting and Financial Management:
    a. Valerie Stevenson, University Controller
    b. Devany Grooves, Budget Director
3. Governance:
    a. Shari Shuman, Vice President for Administration and Finance
    b. Scott Bennett, Chief Information Officer
4. Grants Management: John Kantner, Associate Vice President for Research
5. Information Technology: Scott Bennett, Chief Information Officer
6. Payroll:
    a. Valerie Stevenson, University Controller
    b. Carrie Guth, Director of Human Resources
7. Cash Management and Invetments:
    a. Valerie Stevenson, University Controller
    b. Mike Neglia, University Treasurer
8. Student Billing: Valerie Stevenson, University Controller
9. Capital Asset Management:
    a. Valerie Stevenson, University Controller
    b. John Hale, Associate Vice President for Administration and Finance