Florida Board of Governors State University System

Summary Report
Internal Control and Business Process Assessment

December 2019

Florida Board of Governors State University System
Internal Control and Business Process Assessment
Summary Report
December 2019

I. Executive Summary

The Board of Governors (the "Board" or "BOG") of the Florida State University System ("SUS") engaged Crowe LLP ("Crowe") to perform a system-wide "Internal Control and Business Process Assessment". The objective of this assessment was to evaluate the existing internal controls and review business processes to identify areas of risk for the SUS and to provide recommendations to enhance internal control over the system. 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 does not express an opinion on the accuracy or efficacy of the material reviewed during the performance of these services.

The scope of the assessment was business process risks among the twelve universities within the SUS.

We have presented a summary of the overall results of our assessments of the twelve universities within the SUS in this report. We used our risk rating methodology to evaluate and score business process risks 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 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

Based on our procedures performed, we noted no risk categories with a high level of residual risk, or significant control gaps or weaknesses in any of the twelve universities' control design structures.

We found opportunities to strengthen controls at 11 of the 12 universities (we noted no observations for the University of South Florida ("USF")). We have highlighted these observations as specific opportunities to improve controls or further mitigate risks. The risk rating for each observation is indicative of the risk to university objectives posed by a specific gap in internal controls. This means that an observation is focused on a specific issue and not on an entire function or entity. Conversely, we also assigned ratings to entire risk categories (e.g. Accounts Payable, Procurement, Information Technology, etc.). These ratings represent the average score of all individual risks within that category. Additional information on these observations, our recommendations, and university management responses can be found in each university report.

We also noted several observations and "themes" which were common throughout the SUS, and we have formed recommendations to address these areas for the BOG's consideration. The themes that were consistent throughout the SUS are summarized below.

1. Each university carries a risk that management override of controls and/or collusion to bypass controls may adversely impact universities' compliance with existing rules and regulations as well as operating objectives. In our experience, this risk is difficult to address solely through the implementation of controls. Alternatively, an organization's culture, values, and its focus on ethics, compliance, and risk management tend to be a more effective and holistic approach to addressing this threat.

   We noted that the BOG and each of the universities has implemented clear mission and values statements and has focused on ethics and compliance as a key function of senior management (e.g. the establishment of the Compliance and Ethics Officer position). We also believe that the SUS could benefit from establishing an enterprise risk management framework and program which would be embedded within the BOG and each university in order to strengthen risk management practices and internal controls.

2. The universities could benefit from enhanced information security controls. Information security is becoming increasingly critical function, with new cyber risks and threats emerging that can impact the universities financially, reputationally and strategically.
3. The universities could benefit from strengthening their third-party risk management practices, including vendor setup and contract management roles and responsibilities. Strong monitoring and oversight activities are especially important for vendors who have been granted access to sensitive or personally identifiable information.
4. The universities could benefit from additional guidance and clarification on how to interpret the active BOG regulations. It became apparent in our discussions with various members of university management and trustees, that they sought additional clarity, especially those regulations that pertained to the use of Educational and General (E&G) funds, since the regulations were being interpreted in different ways.

We have provided additional information on these key observations and recommendations for the SUS in the *Conclusion* section of this report. A common thread, or connection among these themes is effective communication and the exchange of information. We believe that with an increased focus on this area, as outlined in this report, the SUS will be able to leverage significant enhancements to its risk management practices and system of internal controls.

II. Assessment Overview

The objective and scope of this assessment, to evaluate existing controls and business processes to identify areas of risk for the SUS, covered a broad range of university functions and corresponding risk factors. In order to manage the scope more effectively we identified inherent risk factors across these functional areas. Based on our experience and industry knowledge, we identified sixty-five risk statements that represent relevant risks to the business process objectives within our scope. We have listed the twelve functional areas (i.e. risk categories) covered within our risk assessment as follows:

- Accounts Payable
- Budgeting
- Capital Asset Management
- Cash Management
- Financial Reporting
- Governance
- Grant Management
- Information Technology
- Investment Management
- Payroll
- Procurement
- Revenue

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 universities management. Based on this information, we developed risk and control assessments for each university. A summary of our ratings for each functional risk area is included in the *Observations and Themes* section of this report.

The risk assessment methodology used during this assessment was designed to maintain consistency and comparability across the twelve, distinct universities within the SUS. Our approach included an assessment of inherent risks, control design effectiveness, and residual risks. An explanation of these components is included in the paragraphs 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 Effectiveness 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 each university’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 control effectiveness. We recognized that each control and its related risk had unique components that would not be fully represented by the control effectiveness 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.

III. Procedures Performed

A summary of the procedures we completed during our assessment of each university have been summarized in the table below. Please note that internal controls are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur, and that operations 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.

Summary of Procedures
1. We reviewed BOG regulations, university policies, procedures, processes and business requirements.
2. We prepared a risk assessment, which includes risks arising from our review of the documents referenced in procedure number 1, 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 each university'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 our university reports as observations and recommendations.
7. We have confirmed with university management the factual basis for our observations and recommendations. Management's written responses are included for each recommendation in the reports.

IV. Observations and Themes

Our procedures identified opportunities to strengthen controls at 11 of the 12 universities (i.e. we noted no observations for USF). These opportunities were documented as "observations" and are summarized 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. While the specific observations and recommendations can be seen in the tables below, we have identified a few themes that were persistent across the universities:

- **Information Security Controls.** We noted that almost all universities would benefit from an enhanced focus in the Information Technology risk category. While we have addressed specific risks in our observations and recommendations, overall the universities in the SUS could benefit from a more standardized approach to information security risk management.
- **Third Party Risk Management Practices.** We noted a common theme throughout our assessment that many universities would likely benefit from an enhanced focus in the areas where third-party risk management and data protection intersect. While we have addressed specific risks in our observations and recommendations, we understand that this is an area in which many universities are expanding or will be planning to expand their operational activities. Since the number of providers and types of services in this area is rapidly expanding, consequently, so are the associated risks. For example, student support centers, call centers, and collection agencies are commonly granted access to student account information. Payroll service providers receive and transmit data electronically, and cloud-based storage services are becoming an increasingly efficient and inexpensive way in which to manage large amounts of data, including personally identifiable and sensitive data.
- **Interfund Transfers.** While this issue was noted in only two universities, there has been increased scrutiny throughout the SUS over the proper use of funds at the university level. Strengthening controls over fund transfers would benefit the SUS by providing an additional level of assurance that the funds are used for their intended purpose. Again, the use of existing technology may enable universities to implement automated workflows to verify that transfers are appropriate and properly approved. System-assigned roles may also be implemented to allow only authorized individuals to make fund transfers. While we noted no specific occurrences of improper use of funds, we have identified this issue as one example of how management override of controls or collusion could adversely impact university operating and compliance objectives and also result in reputational damage.

Our overall recommendation in the *Conclusion* section of this report focuses on enterprise risk management as a way to address the themes noted above, as well as numerous other risks to the SUS. We consider the theme noted below to be a separate issue and our recommendation is focused on a more direct approach to addressing that area of focus.

- **Clarity of the BOG Regulations regarding the Use of E&G Funds.** In speaking with various university Board of Trustees members, as well as with university management, it was stated that this area of the BOG regulations was not completely clear and may be interpreted in various ways. In addition, the SUS may benefit from further clarification and distinction between the role and responsibilities of the BOG and the University Trustees in terms of fiscal governance and oversight duties. We have provided our analysis and recommendations to enhance the clarity of the regulations in the *Conclusion* section of this report.

Summary of Observations by Risk Category

The themes noted above were driven and supported by our observations. We noted a total of 21 distinct observations which included two (2) observations from the Financial Reporting risk category, two (2) from Procurement, one (1) from Grant Management, and sixteen (16) from Information Technology.

From the perspective of frequency of occurrence, Information Technology had the most observations and the most occurrences noted across the SUS, comprising 16 of the 21 (76%) distinct observations and 39 of the 45 (87%) occurrences noted. However, the majority of these observations (13 of 16, or 81%) were rated as "Low" risk.

From a risk ratings perspective, the observations pertaining to financial controls (e.g. interfund transfers and grant draw-down procedures) and third-party risk management controls (e.g. vendor oversight and shared services arrangements) were rated as "Moderate" risk, which was the highest ranking given during our assessment. The single observation in the Grant Management risk category was deemed to be Low risk. A summary of our observations by risk category is included in the table below.

Risk Category: Financial Reporting

Observation	Risk Rating	Number of Occurrences SUS-Wide: (3)
Restricted Funds – Interfund Transfers	Moderate	2
Monitoring of Budget-to-Actual Performance	Low	1

Risk Category: Procurement

Observation	Risk Rating	Number of Occurrences SUS-Wide: (2)
Contract Management - Shared Services Agreements	Moderate	1
Policies and Procedures – Vendor Setup and Monitoring	Moderate	1

Risk Category: Grant Management

Observation	Risk Rating	Number of Occurrences SUS-Wide: (1)
Segregation of Duties: Grant Drawdown Process	Moderate	1

Risk Category: Information Technology

Observation	Risk Rating	Number of Occurrences SUS-Wide (39)
Configuration Management Program	Moderate	3
Business Continuity Management – Incident Classification	Moderate	1
Information Security Governance Key Risk and Performance Indicators (2) Cybersecurity Risk Management Program (2) Policies and Procedures (2) "Clean Desk" Policy (4)	Low - Moderate	10
Employee Security Awareness Training	Low	6
Data Protection – Employee Removable Media (6) Employee Mobile Device Management Policy (5) Sensitive Data-Tracking (1) Data Handling and Classification (1) Data Center Moisture Detection Systems (1)	Low	14
Logging and Monitoring Policy	Low	1
Monitoring of Third-Party Service Providers	Low	1
User Termination and Role Changes	Low	2
IT Operations – Asset Tracking	Low	1

Summary of Observations by University

The table below illustrates the 21 observations by university. It is intended to show how the issues were spread across the various universities within the SUS, and further clarify our summary of observations and themes. Specifically, this illustrates the concentration of Information Technology observations at a Low risk rating, and fewer observations in the other risk categories with a higher risk rating of "Moderate".

Risk Category	Observation	UWF	FSU	UNF	UF	UCF	FAMU	FPU	USF	NCF	FIU	FAU	FGCU
Financial Reporting	Monitoring of Budget-to-Actual Performance									Low			
Financial Reporting	Restricted Funds – Interfund Transfers					Moderate				Moderate			
Procurement	Contract Management - Shared Service Contracts	Moderate											
Procurement	Policies and Procedures - Vendor Setup and Monitoring	Moderate											
Grant Management	Segregation of Duties - Grant Drawdown Process												Moderate
Information Technology	Business Continuity Management - Incident Classification	Moderate											
Information Technology	Configuration Management - Configuration Management Program		Moderate			Moderate					Moderate		
Information Technology	Data Protection - Data Handling and Classification Policy										Low		
Information Technology	Data Protection - Employee Mobile Device Management Policy	Low		Low						Low	Low	Low	
Information Technology	Data Protection – Employee Removable Media	Low	Low			Low	Low	Low				Low	
Information Technology	Data Protection - Sensitive Data-Tracking		Low										
Information Technology	Employee Management – Employee Security Awareness Training	Low			Low	Low	Low					Low	Low
Information Technology	Employee Management - User Termination and Role Change		Low		Low								
Information Technology	Information Security Governance – Clean Desk Policy			Low		Low				Low		Low	
Information Technology	Information Security Governance - Cybersecurity Risk Management Program					Low					Low		
Information Technology	Information Security Governance - Key Risk and Performance Indicators		Moderate									Moderate	
Information Technology	Information Security Governance - Policies and Procedures						Low	Low					
Information Technology	Logging and Monitoring - Logging and Monitoring Policy											Low	
Information Technology	Data Protection - Data Center Moisture Detection									Low			
Information Technology	IT Operations - Asset Tracking											Low	
Information Technology	Monitoring of Third-Party Service Providers		Low										

V. Conclusion

The themes emphasized in this report and supported by our observations have led us to make two recommendations for the SUS to help strengthen risk management and control practices system-wide. We conclude our report with these recommendations as outlined in the paragraphs below.

1. Establish an Enterprise Risk Management Program for the SUS

We recommend that the BOG work collaboratively with university trustees and management to establish an enterprise risk management program for the SUS. This recommendation addresses the following themes:

- Information Security
- Third-Party Risk Management
- Management Override of Controls or Collusion

Based on our experience, we noted that the establishment of an enterprise risk management ("ERM") program may be an effective approach to addressing the themes noted above. An effective ERM program can be a powerful tool to help the SUS maintain pace with the threats that have emerged and continue to evolve in Higher Education. These threats pose not only financial risks, but may also impact reputation, compliance with regulatory requirements, safety, and strategic initiatives. The paragraphs below provide specific examples of how ERM may help the SUS address the themes noted during our assessment.

Information Security

Crowe used a proprietary set of security standards which were based on well-known and utilized frameworks and best practices (e.g. NIST) throughout the public sector, including Higher Education. We found that universities varied on the extent to which they based their information security policies and practices on an established framework or a set of standards. Consequently, we noted a relatively high number of observations indicating gaps in information security control best practices.

The implementation of an ERM framework would enable universities to clearly state their risk appetite and tolerances accompanied by the standards they wish to be measured against. This statement could be evaluated by the BOG or other designated body to determine its reasonableness and alignment with an overall SUS risk appetite for information security.

Once an agreed-upon standard has been established, the relevant controls could be more easily identified and tested periodically to determine if the university is meeting its desired security objectives and maintaining an acceptable level of risk.

Third-Party Risk Management

The observations pertaining to third-party risk management were partially focused on the need to document policies and procedures, but more importantly on the absence of clearly defined roles and responsibilities for overseeing vendor setup and maintenance as well as data protection when vendors are granted access to sensitive or personally identifiable information.

From a data protection perspective, this area is related to the information security observations; however, this is not solely an "IT issue". There are many employees across each university who are involved in some aspect of third-party risk management ranging from the individuals who manage a contract, to those who add or update vendor information, and those who approve access to systems.

An ERM approach may be effective here because there must be a risk response, or action plan, associated with the identified risk. A key component of any action plan is an assigned risk owner and specific roles, responsibilities, and tasks that must be taken to address or "respond" to that risk. In this case, the risk response and action plan would identify the owner(s) of each risk and associated tasks ranging from contract management to procurement to user access management. Again, the existence of the plan would enable a clear line of measurement against which to evaluate the university's performance in this area.

Management Override of Controls or Collusion

While we did not identify any occurrences of management override of controls or employee collusion to bypass controls, this risk always remains relatively high from an inherent perspective due to the potential impact these could cause. This risk is further increased when an entity is facing budgetary constraints. In this case, an ERM framework can be an effective tool to consolidate existing statements, bylaws, regulations, and policies (e.g. mission, values, code of ethics) into an actionable mechanism. Additionally, risk appetite statements for an organization typically reference these components to clarify the entity's position on what actions it is willing to take, and what actions it is not willing to take in pursuit of its mission and objectives. Specific examples such as inappropriate use of designated funds can be added to a risk appetite statement for clarity.

While there are many established frameworks, such as the model established by the *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), to establish an ERM program, it is considered a best practice to develop a tailored program that fits the organization's unique culture, structure, and environment. We see an opportunity to develop a sustainable ERM program across the SUS, which could be established from the top-down and embedded into the decision-making practices at the BOG level, the university Board of Trustee levels, and into the management structure. There are many benefits that a sustainable ERM program could provide to the SUS, including:

- Improvement to decision-making and deployment of resources based on an established risk appetite and prioritized risk rankings.
- Integration of risk assessments with strategy, objective setting, and performance.
- Encouragement of open communication about significant risks and reduction of gaps and inconsistencies with the management of process level objectives.
- Enhancement of knowledge management and information sharing.
- Benchmarking and collaboration with other mature universities and similar organizations with an established risk management structure.
- Introduction of a collaborative approach to identifying and addressing the top SUS priorities from a risk-based perspective.
- Creation of a common language for communicating and reporting on risk and risk management activities.

Establishing a sustainable ERM framework and program requires a significant investment of time and resources; however, the benefits fit the issues that we have encountered during the course of our assessment.

2. Clarification of BOG Regulations

Throughout the course of our assessment we noted that, given the number and complexity of the active BOG regulations, even university employees who are highly knowledgeable expressed confusion and had come to varying conclusions on how to interpret the appropriate use of E&G funds. We completed an analysis of the active regulations at the time of our review in an attempt to recommend potential solutions to the varying interpretations and confusion.

After a search of the State University System of Florida Board of Governors Active Regulations, we found that E&G spending rules are outlined within BOG 9.007. State University Operating Budgets. Subsections 3(a)1-8 outline eligible uses of and reporting on E&G funds as summarized below.

- E&G operating activities such as, but not limited to general instruction, research, public service, plant operations and maintenance, furniture, fixtures, and equipment, student services, libraries, administrative support, and other enrollment-related and stand-alone operations of the universities.
- Non-recurring expenditures. This is not defined further within the regulation.
- Carryforward expenditures included in the university's E&G Carryforward Spending Plan, some of which include capital outlay project expenditures as defined under BOG 14.0025. Action Required Prior to Fixed Capital Outlay Budget Request.

We have outlined several suggestions on areas where the active regulations may be clarified to guide the interpretation of how these funds may be spent.

- **Provide a Comprehensive List of E&G Operating Activities.** Section 9.007.3(a)1 provides a list of eligible uses of E&G funds; however, it qualifies the list with the phrase, "but not limited to", which implies that there are other eligible uses for E&G funds not stated in the active regulations. Providing a comprehensive list of eligible E&G fund uses may help alleviate confusion or varying interpretations of this regulation.
- **Clearly State E&G Cannot Be Used for Capital Projects**. If the BOG wants to designate E&G funds as ineligible for use on capital projects, the wording could be improved by adding an additional point that very clearly states E&G is not to be used for capital projects and remove all references that may indicate otherwise. For example, BOG 9.007.3(a)4 allows some exceptions to the rule; however, these exceptions may contribute to the universities' varying interpretations.
- **Clearly Define Capital Thresholds for Renovation.** A gray area exists related to the use of E&G funds for plant operations and maintenance. Specifically, at what point does building renovation turn into a capital project? Some sort of threshold would be useful to define this. Following is an example from another university:

  "Structural remodeling/renovation and additions are capitalized when they enhance the use of or extend the life of the building beyond its original estimated useful life, and the total cost equals or exceeds $100,000 or 20% of the building's cost, whichever is less."

- **Clearly Define Plant Operations and Maintenance.**

  In addition, more clarity around what is included in plant operations and maintenance would narrow its interpretation. Adding it to the Definitions Section 9.001 would be of benefit. The Integrated Postsecondary Education Data System definition may help in this regard. It is:

  "Operation and maintenance of plant (O&M): An expense category that includes expenses for operations established to provide service and maintenance related to campus grounds and facilities used for educational and general purposes. Specific expenses include: janitorial and utility services; repairs and ordinary or normal alterations of buildings, furniture, and equipment; care of grounds; maintenance and operation of buildings and other plant facilities; security; earthquake and disaster preparedness; safety; hazardous waste disposal; property, liability, and all other insurance

relating to property; space and capital leasing; facility planning and management; and central receiving. This expense does include amounts charged to auxiliary enterprises, hospitals, and independent operations. Also includes information technology expenses related to operation and maintenance of plant activities if the institution separately budgets and expenses information technology resources (otherwise these expenses are included in institutional support)."

- **Establish a Discussion Forum**

  Establishing an open forum for university management, trustee members, and BOG members to share questions and interpretations on active or proposed regulations may be an effective tool for identifying and prioritization regulatory issues for clarification. It may also help enhance the frequency of communications SUS-wide helping to resolve potential problems before they occur.

This concludes our report. We thank the Board of Governors, the various University Board of Trustee members, and the many members of university management who have given this opportunity and assisted us throughout this engagement.