Crowe

Smart decisions. Lasting value.™

Florida Board of Governors State University System

Florida Agricultural & Mechanical University Internal Management and Accounting Control and Business Process Assessment

December 2019

I. Executive Summary

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

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

We have presented the results of our assessment of the Florida Agricultural and Mechanical University (FAMU) 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 procedures precludes us from issuing an opinion on FAMU’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 FAMU’s control structure.

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

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

FAMU Observations Summary

Risk Category	Description	Risk Rating
Information Technology	**1. Data Protection – Employee Security Awareness Training.** FAMU does not provide reoccurring security awareness training to its employees. This increases the risk that employees may not understand how to identify and respond to emerging and evolving security threats (e.g. phishing scams).	Low
Information Technology	**2. Information Security Governance – Policies and Procedures.** FAMU has not documented information security policies and procedures for the sections pertaining to: 1) Malicious Code Detection and Integrity, 2) Physical Security, 3) Risk Management, 4) Patch Management and 5) Configuration Management. This increases the risk that tasks will be performed inconsistently.	Low
Information Technology	**3. Data Protection – Employee Removable Media.** FAMU has not implemented technology controls to manage employees' and contractors' use of removable media, (i.e. USB drives). This increases the risk of unauthorized disclosure of confidential, personally identifiable, or other sensitive information through loss or misuse of the storage media.	Low

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

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 reviewed 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 FAMU. 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 FAMU 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 FAMU’s control structure.

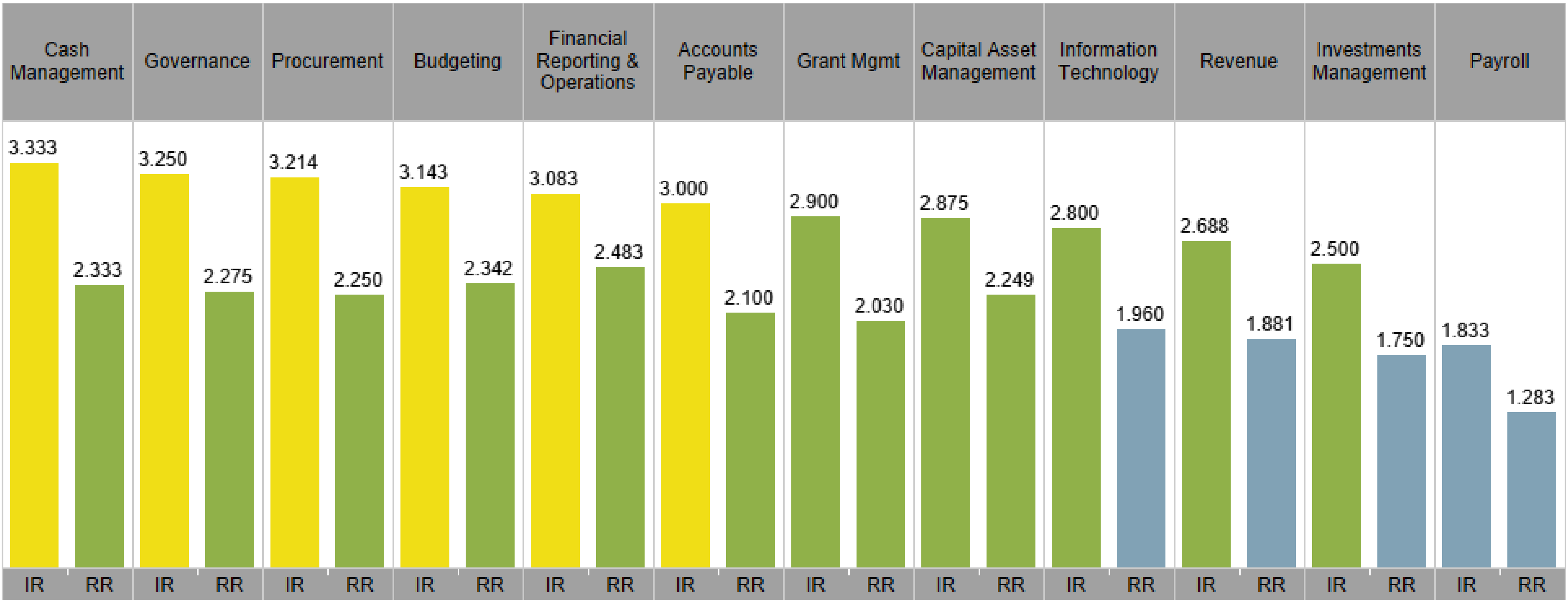
Residual Risk Assessment

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 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.

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 eight categories to have a minor level of residual risk and four categories to have a low level of residual risk. FAMU’s three highest categories of residual risk were Financial Reporting & Operations, Cash Management, 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.

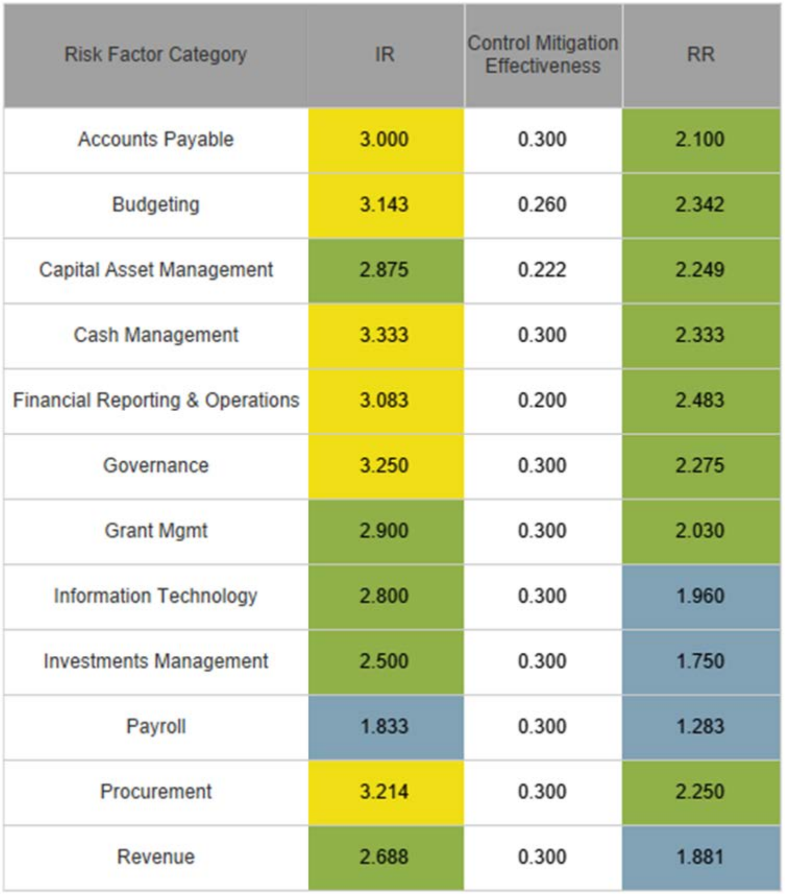
Exhibit 1: FAMU Inherent vs. Residual Risk by Category



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



Risk Factor Category	IR	Control Mitigation Effectiveness	RR
Accounts Payable	3.000	0.300	2.100
Budgeting	3.143	0.260	2.342
Capital Asset Management	2.875	0.222	2.249
Cash Management	3.333	0.300	2.333
Financial Reporting & Operations	3.083	0.200	2.483
Governance	3.250	0.300	2.275
Grant Mgmt	2.900	0.300	2.030
Information Technology	2.800	0.300	1.960
Investments Management	2.500	0.300	1.750
Payroll	1.833	0.300	1.283
Procurement	3.214	0.300	2.250
Revenue	2.688	0.300	1.881

Conclusion

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

We believe that FAMU would benefit from several low-cost, high-value enhancements such as automating controls over fund transfers and integrating the asset inventory and accounting function with maintenance and disposal. Additionally, the university could strengthen its control structure over Information Technology risks with several process and procedural enhancements as well as additional security best practices training for employees.

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

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 FAMU 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 FAMU'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 FAMU 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 three (3) 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 – Employee Security Awareness Training**	Low
Information Technology	**2. Information Security – Policies and Procedures**	Low
Information Technology	**3. Data Protection – Employee Removable Media**	Low

Observations and Recommendations

Observation 1	Process Area	Priority Rating
Data Protection – Employee Security Awareness Training	Information Technology	Low

Condition: Although FAMU provides security training to new users upon hire and has held security awareness training events, annual or frequent employee security awareness training is not required.

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: FAMU has not prioritized resources to provide annual security training to all employees.

Implication: If users are not provided with periodic training, at hire and annually, they may not be prepared to identify emerging threats and tactics and exposes the organization to an increased risk of a breach.

Recommendation: FAMU should provide annual security awareness training to users. This training should be updated at least annually to cover current cybersecurity risks and threats. Users should be required to sign an acknowledgement of this training and these acknowledgements should be tracked. In the absence of a robust Learning Management System, universities may consider the use of readily available mobile applications that can be used to track attendance at training events.

Management Response:

AGREE: FAMU can enhance its Employee Security Awareness Training by enforcing an annual requirement. Efforts taken to date include FAMU Information Technology Services (ITS) contracting with a firm to make a training platform available and initiating training in October of 2017. Since this was the initial awareness training ITS extended it to October of 2018. At the conclusion of that training FAMU initiated a contract with a new vendor at the beginning of 2019 and began training efforts in July 2019. ITS has continually provided Cybersecurity info-graphic materials to the user community as well as cyber threat intelligence to key members of administration (Provost, VPs, Deans, etc.). FAMU Board of Trustees Policy Number 2008-01a entitled Enterprise Information Systems Security and Controls was established on March 20, 2008. This Policy speaks to the role of the Chief Information Security Officer (CISO) in providing adequate Security Awareness Training for University employees and students. FAMU's CISO provides security awareness training during our annual management seminars and the Faculty Senate meetings. The CISO also sends out security awareness information over FAMUINFO to all employees, students, and alumni. The enhanced Employee Security Awareness Training is planned for implementation in March 2020.

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

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

Condition: Although FAMU has documented an administrative policy to require encryption for removable media (i.e., USB drive), their use is not managed. Furthermore, technical controls have not been implemented to restrict access and provide data protections, such as encryption and device authentication outside of the PCI and NIST 800.171 environments.

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: FAMU has not prioritized resources to address the risk of employees using removable media.

Implication: Without restrictions on personnel's' use of removable storage media through device encryption, there is the risk of unauthorized disclosure of confidential, personally identifiable, or other sensitive information through the loss or misuse of the storage media.

Recommendation: FAMU 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 based on the risk of data and systems. Removable media should also be centrally managed, and only company devices should be used, where possible and appropriate. 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 can be reduced.

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:

We agree that FAMU has not implemented technology controls to manage employee’s and contractors’ use of removable media. FAMU will evaluate further the costs and benefits of implementing technology controls and/or policy related to the usage of removable media. This is planned for implementation by May 2020.

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

Observation 3	Process Area	Priority Rating
Information Security – Policies and Procedures	Information Technology	Low

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

- **Malicious Code Detection and Integrity** – The organization does not maintain a documented malicious code detection and integrity program that includes the organization's requirements for endpoint and network level protection.
- **Physical Security** – The organization does not maintain a documented physical security program which includes standards for physical security surrounding IT assets such as the datacenter and networking closets.
- **Risk Management** – The organization does not maintain a documented risk management program which includes identification and evaluation of risks, threats, and vulnerabilities.
- **Patch Management** – The organization does not maintain a documented patch management program that defines requirements for patch documentation, approvals, patch installation frequency, testing, exceptions, emergency and critical patch processes.
- **Configuration Management –** The organization does not maintain a documented configuration management program that includes the organization's requirements and standards around configuration management activities.

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: FAMU has not prioritized resources to address this issue.

Implication: Lack of policies and procedures may result in potential conflicts when performing tasks due to inconsistent and/or lack of documentation. If an individual is unable to perform his or her duties, a formalized and up-to-date procedure will provide guidance for another individual to complete the necessary task.

Recommendation: FAMU should develop the missing program areas and should include, but not limited to, 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 program and if applicable, procedures to reflect the current industry security standards and practices.

Management Response:

We agree that FAMU does not currently have documented information security policies and procedures related to the above areas. Management will work to establish the appropriate policies and procedures to govern malicious code detection and integrity, physical security, risk management, patch management, and configuration management. This is planned for implementation by May 2020.

This report is furnished solely for the information and use of Florida Agricultural and Mechanical 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 FAMU

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

1. Accounts Payable and Procurement:
    a. Keisha Franklin, University Controller
    b. Terrica Coleman, Accounting, Payment Distribution Services, & Travel
    c. D’Andrea Cotton, Associate Controller for Student Financial Services
    d. Mattie Hood, Assistant Controller for Disbursements & Warrant Distribution
2. Budgeting and Financial Management: Nichole Reese, Assistant Budget Director
3. Capital Asset Management: Jahan Momen, Assistant Controller for Asset Management Accounting
4. Cash Management: Keisha Franklin, University Controller
5. Grants Management: Pamela Blount, Director of Contracts & Grants
6. Student Billing: Keisha Franklin, University Controller
7. Payroll: Joyce Ingram, Chief Human Resources and Diversity Officer
8. Audit and Compliance: Rica Calhoun, Compliance Officer
9. Information Technology: Ronald Henry II, Associate Vice President and Chief Information Officer

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