Florida Board of Governors State University System

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

December 2019

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

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

FSU Observations Summary

Risk Category	Description	Risk Rating
Information Technology	**1. Information Security Governance – Key Risk and Performance Indicators.** FSU does not have a policy for measuring key risk and performance indicators within its information security program, making it difficult to determine the program's effectiveness.	Moderate
Information Technology	**2. Configuration Management – Configuration Management Program.** FSU has not documented a Configuration Management Program, which includes documented policies and procedures for system baseline and security configurations (hardening). This increases the risk of inconsistencies across network security configurations, which may expose FSU to vulnerabilities.	Moderate
Information Technology	**3. Data Protection** – **Employee Removable Media.** FSU does not require employees to use only authorized, encrypted removable devices. This increases the risk of unauthorized disclosure of sensitive data due to theft or loss.	Low
Information Technology	**4. Data Protection – Sensitive Data-Tracking.** FSU has not established a process to identify and track sensitive data across university systems to verify that appropriate security controls are in place. This increases the risk of a data breach occurring in an inadequately secured system.	Low
Information Technology	**5. Third Party Risk Management – Monitoring of Third-Party Service Providers.** FSU has not established a process to identify and track third party service providers with access to university information systems. This increases the risk that a vendor may retain access to sensitive data after it is no longer necessary or appropriate.	Low
Information Technology	**6. Employee Management – User Termination and Role Change.** FSU does not have an established notification process to terminate user access within a twenty-four-hour period, which is a timeframe commonly recommended by security practices and standards.	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 (FSU)

This report represents the results of our assessment of Florida State University (FSU). 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 FSU 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 FSU’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 eleven categories to have a minor level of residual risk and one category to have a low level of residual risk. FSU's three highest categories of residual risk were Revenue, Information Technology, 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: FSU Inherent vs. Residual Risk by Category

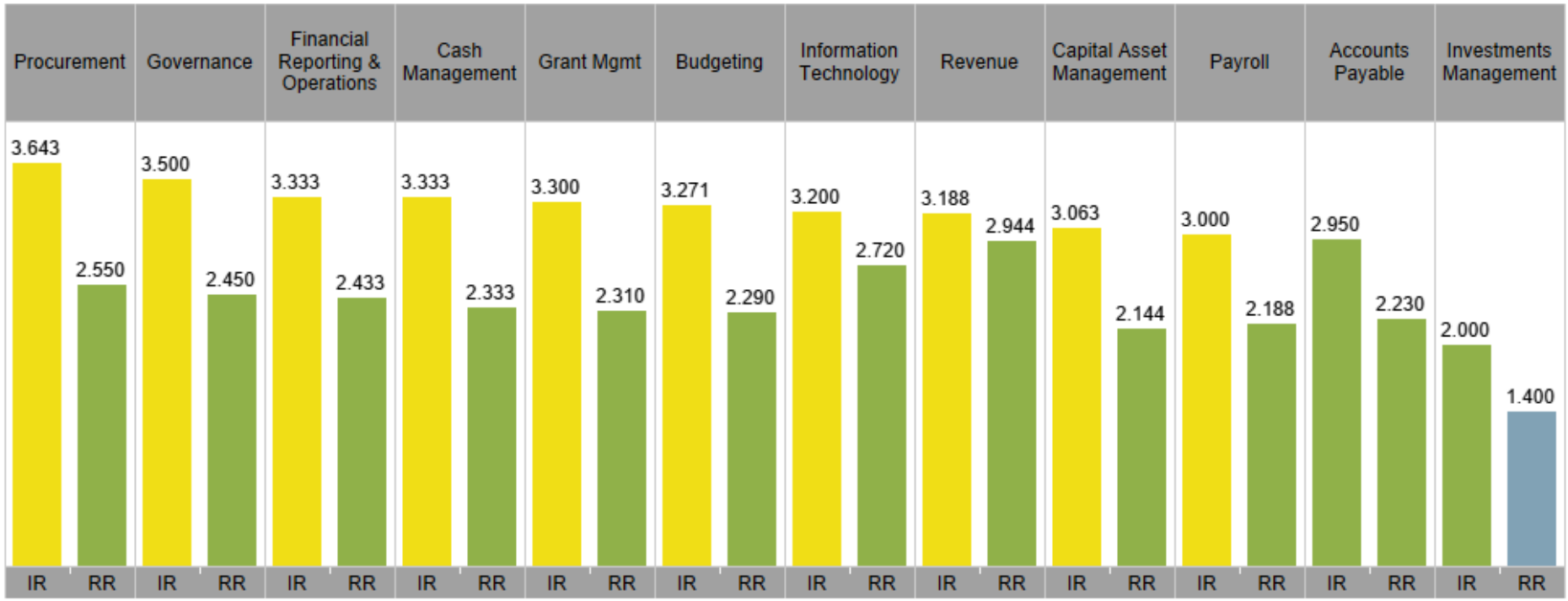

Exhibit 2 highlights similar information but uses different visualizations to illustrate how the control rating reduced the level of inherent risk (i.e. resulting in the residual risk score). The inherent risk represents the baseline score in each category prior to considering the internal controls.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

Risk Factor Category	IR	Control Mitigation Effectiveness	RR
Accounts Payable	2.950	0.300	2.230
Budgeting	3.271	0.300	2.290
Capital Asset Management	3.063	0.300	2.144
Cash Management	3.333	0.300	2.333
Financial Reporting & Operations	3.333	0.300	2.433
Governance	3.500	0.300	2.450
Grant Mgmt	3.300	0.300	2.310
Information Technology	3.200	0.150	2.720
Investments Management	2.000	0.300	1.400
Payroll	3.000	0.275	2.188
Procurement	3.643	0.300	2.550
Revenue	3.188	0.300	2.944

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

We also noted that the university would likely benefit from an enhanced focus in the Information Technology risk category. While we have addressed specific risks in our observations and recommendations, this is an area in which FSU could benefit from a more holistic approach to risk management. A strong risk management framework is critical to maintain pace with the threats that have emerged alongside technological advances. These threats pose not only financial risks, but may also impact reputation, safety, and strategic initiatives. FSU 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 FSU, and to provide observations and recommendations to the FSU Board of Trustees, FSU 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 FSU:

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 FSU 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 FSU'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 FSU 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 six (6) observations which are summarized in the table below. These observations represent areas where we determined that controls were absent or were not adequate to mitigate the associated risk to an acceptable level. In the following section we have provided details and recommendations to address each of these observations. Management's responses to each of our recommendations are also included in this section.

Risk Category	Description	Risk Rating
Information Technology	**1. Information Security Governance – Key Risk and Performance Indicators**	Moderate
Information Technology	**2. Configuration Management – Configuration Management Program**	Moderate
Information Technology	**3. Data Protection – Employee Removable Media**	Low
Information Technology	**4. Data Protection – Sensitive Data-Tracking**	Low
Information Technology	**5. Third Party Risk Management – Monitoring of Third-Party Service Providers**	Low
Information Technology	**6. Employee Management – User Termination and Role Change**	Low

Observations and Recommendations

Observation 1	Process Area	Priority Rating
Information Security Governance – Key Risk and Performance Indicators	Information Technology	Moderate

Condition: Although the organization does report key risk / performance indicators to Information Technology Services (ITS), the Chief Information Officer, Provost, and the Vice President of Finance and Administration, the metric included within the report does not indicate an acceptable level of risk tolerance and the actions required to be taken to measure the effectiveness of their information security program.

Criteria: We relied on the National Institute of Standards and Technology SP 800-53 r5 (NIST) PM-6 as the criteria upon which to evaluate these controls.

Root Cause: FSU has not yet prioritized resources to complete the development of information security program metrics.

Implication: In the absence of clear metrics for monitoring risk and performance, the risk increases that management's response to threats will be inconsistent, and the overall effectiveness of the information security program will be unclear.

Recommendation: FSU should take a holistic look at the threat landscape applicable to organization and the existing information security program to enumerate key risk and key performance indicators (KRI / KPI). These indicators can be used to determine how well FSU is managing its information security risk. Once these indicators have been determined, a process should be implemented for compiling data used and quantifying these indicators to measure KRI / KPIs on a periodic basis to measure performance over time. Management should implement a tracking mechanism to document and report on KRI / KPIs.

This data should be used as a resource for updating the Board of Trustees or other governance committees on the information security program's effectiveness. This will assist the board or governance committee to provide proper guidance around cybersecurity risk.

Some common key risk indicators include, but are not limited to:

1. Number of missing patches / patch exceptions
2. Number of vulnerabilities identified and trending over time (remediated and un-remediated)
3. Number of social engineering (i.e. phishing) attempts or emails received in a given period.
4. Number of security alerts generated by monitoring tools (SIEM, IPS/IDS, etc.) (actionable vs non-actionable)
5. Number of cybersecurity Incidents trending over time.
6. Number of new risk and emerging threats

Management Response:

Disagree.

The FSU Information Security and Privacy Office does take a holistic look at threat landscape and measures Key Performance Indicators (KPI) for security management, risk management and vulnerability management. We track the specific metrics recommended in the observation. These reports are provided to ITS leadership on a monthly basis. The CIO and CISO report metrics as appropriate or requested by senior management. The Information Security and Privacy Advisory Committee, made up of leaders from academic, research and administration, meets quarterly, and selected information is presented as appropriate.

Crowe Comment:
We acknowledge FSU's efforts to monitor their information security risk landscape, as stated above. However, despite our requests, we did not receive the requested evidence from FSU to support the implementation of these control and performance management activities. As a result, this item remains an observation in our report.

Observation 2	Process Area	Priority Rating
Configuration Management – Configuration Management Program	Information Technology	Moderate

Condition: FSU has not documented a Configuration Management Program, which includes documented policies and procedures for system baseline and security configurations (hardening). This increases the risk of inconsistencies across network security configurations, which may expose FSU to vulnerabilities.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 CM-9 as the criteria upon which to evaluate these controls.

Root Cause: FSU has not yet prioritized resources to complete the configuration management documentation.

Implication: Information systems may not be configured with industry security standards, resulting in configuration inconsistencies across the network increasing the risk of vulnerabilities.

Recommendation: FSU should formally document the organization's configuration requirements based on industry best practices.

FSU should implement a process to document information system baseline standards (e.g. operating system [OS] images or checklists) when deploying information system assets. These baselines or checklists should be proactively updated for information system assets (e.g. networking devices, servers, and workstations) on a periodic basis. Additionally, security configuration standards (i.e. hardening guidelines) should be referenced when developing system baselines. Information system baselines should be updated during the following conditions:

- Operating system updates;
- Critical software updates;
- New software implementation; and
- New security tool implementation(s).

Security configuration standards should also be applied to all baselines. Following security configuration standards helps to mitigate risk to systems before systems are implemented on the network.

FSU should also ensure that configuration management activities are included in the system development life-cycle (SDLC) process.

Management Response:

Agree.

FSU Information Security Policy 4-OP-H-5 requires a documented standard configuration to be used to harden IT resources. The FSU Information Security and Privacy Office offers Center for Internet Security (CIS) Benchmark resources for baseline security configurations for desktops, servers, network devices, and other IT resources. However, FSU does not have documented procedures for a Configuration Management Program. The university will develop formal configuration management procedures to remediate this observation.

Planned Remediation Date: June 2021

Observation 3	Process Area	Priority Rating
Data Protection – Employee Removable Media	Information Security	Low

Condition: Although FSU 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: FSU 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: FSU 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:

Disagree.

The encryption of data can be handled in two ways; centrally or “de-centrally”. The University has opted to take a decentralized approach and this has served the university well. University Policy, 4-OP-H-5 Information Security Policy requires each University entity to bear responsibility for protecting its data. This policy requires encryption for private and protected data. The university utilizes preventive controls to limit and monitor access to sensitive data. Information Technology Services coordinates periodic risk assessments to monitor compliance with this policy. If circumstances would change, the University will reassess its current policy.

Crowe Comment:

Although we recommend a centralized approach, we understand that an organization may choose to manage data encryption from a decentralized approach and accept the associated levels of risk. However, FSU did not provide evidence that there were mitigating controls in place (i.e. the periodic risk assessments stated above) to enable us to confirm their risk management approach. As a result, this item remains an observation in our report.

Observation 4	Process Area	Priority Rating
Data Protection – Sensitive Data-Tracking	Information Security	Low

Condition: While FSU has documented policy standards within the Information Security Policy 4-OP-H-5, which requires data owner or designated data manager to maintain a list of the data and information collected, processed, transmitted, or stored by the units under his/her purview; however, since the implementation of the requirements, a process has not been implemented to re-assess / audit all pre-existing information systems to track sensitive data stored.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 CM-12 as the criteria upon which to evaluate these controls.

Root Cause: FSU has not prioritized resources to create a tracking mechanism for sensitive data across university systems.

Implication: If FSU is unaware of the location and storage of sensitive data, the university may not be able to effectively secure it in accordance with industry security controls (e.g. NIST). This could lead to a data breach if data is left improperly secured within university systems.

Recommendation: FSU should perform a review of university information systems to identify and create an inventory of where sensitive data resides. These systems should be categorized and risk-ranked based on data type and number of records. Based on the results of this assessment, FSU should determine if additional security controls are required for the identified systems and system security plans should be developed or updated to include these additional controls.

1. They should be categorized, and risk ranked (criticality rating) based on type of data and number of records.
2. Evaluation should occur to determine if additional security controls are necessary based on the criticality rating of the information system(s).
3. System security plans should be documented or enhanced to include additional security controls based on the criticality of the system.

Management Response:

Disagree.

FSU Information Security Policy 4-OP-H-5 requires each data owner or designated data manager to maintain a list of the data and information collected, processed, transmitted, or stored by the units under his/her purview. The university has preventive controls in place to manage access to sensitive data by utilizing restricted security roles within the Enterprise Resource System. Supervisors and role owners evaluate access needs and approve or deny requests accordingly. Periodic reviews of security roles assigned to employees are conducted by supervisors and role owners.

Crowe Comment:

FSU did not provide evidence that there were mitigating controls in place (i.e. the periodic security role assessments stated above) to enable us to confirm their risk management approach. As a result, we were unable to remove this observation from the report.

Observation 5	Process Area	Priority Rating
Third Party Risk Management – Monitoring of Third-Party Service Providers	Information Security	Low

Condition: FSU has not formally documented a list of all third-party service providers and external information system connections that are required for critical business functionality. Additionally, FSU does not preform access reviews for third parties to ensure that access is appropriate for their function.

Criteria: We relied on the National Institute of Standards and Technology (NIST) Cybersecurity Framework ID.SC-2 as the criteria upon which to evaluate these controls.

Root Cause: FSU has not prioritized resources to compile and maintain a list of third-party vendors and their level of access in order to facilitate this assessment.

Implication: If FSU is not aware of all third parties that are accessing FSU systems, the risk of a breach due to malicious intent or negligence is increased. This is especially true if third party access is not reviewed regularly.

Recommendation: FSU should build a procedure into the vendor setup/onboarding process to document a data flow diagram of external connections. Once all third-party access is identified, roles and responsibilities should be assigned to management to review the appropriateness of that access on a regular basis. Mechanisms should also be established to remove that access as soon as management has deemed it no longer necessary (e.g. contract expiration or termination, or changes to vendor role).

Management Response:

Disagree.

The procurement process requires review and approval by Information Technology Services via and IT Software Checklist for requisitions of IT software and services. In a 2018 Florida State University conducted a Business Impact Analysis, which identified all critical third-party service providers. The university uses preventive controls to limit access to critical third-party service providers. Periodic reviews are conducted to monitor the appropriateness of access.

Crowe Comment:

In their response, FSU has not addressed our recommendation to build a procedure into the vendor setup/onboarding process to document a data flow diagram of external connections. Additionally, FSU did not provide evidence of the Business Impact Analysis or the third-party review process, stated above. As a result, this item remains an observation in our report.

Observation 6	Process Area	Priority Rating
Employee Management – User Termination and Role Change	Information Security	Low

Condition: While FSU does have automated processes for termination through their ERP system, they do not have a consistent process to terminate user access with 24 hours of the end of employment.

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: FSU has not established mechanism to enable terminations and role change notifications to be submitted within 24 hours.

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

Recommendation: FSU should document a procedure and implement a process to notify the security team in the event of a role change or termination. In the event of a termination, access should be removed within 24 hours of the notification. For role changes, an access review should be performed in a timely manner to identify the required permissions for the new role and remove any access that is no longer necessary.

Management Response:

Partially Agree.

FSU Separation from Employment Policy and Procedures 4-OP-C-7-D11, requires employees and departments to submit the necessary termination forms and actions in advance of an employee's termination date. When FSU Human Resources terminates an employee in the University's PeopleSoft Human Capital Management (HCM) System, an automated process is initiated to remove all roles within the University's Online Management of Networked Information (OMNI) systems except those required for basic employee services such as accessing the employee's W2 or changing the employee's mailing address. The university will conduct a study to evaluate the effectiveness of this control.

Planned Remediation Date: June 2021

VI. Appendix - List of Interviewees at FSU

The following individuals were interviewed during our onsite visit to FSU the week of July 8, 2019. The name, title, and interview subject are included below.

1. Operating and Capital Budget Management: Michael Lake, Chief Budget Officer.
2. Procurement and Contract Management:
    a. Rosey Murton, Chief Procurement Officer
    b. Karen Gibson, Associate Director Procurement
    c. Casey Laurienzo, Contract Administrator
3. Financial Accounting:
    a. Sandra Scanlan, Controller
    b. Judd Enfinger, Senior Associate Controller
    c. Carla Daniels, Associate Controller
    d. Daniel Pearce, Associate Controller
4. Information Technology and Security:
    a. Jane Livingston, Chief Information Officer
    b. Bill Hunkapillar, Chief Information Security Officer
    c. Joe Brigham, PCI Compliance Officer
    d. Byron Menchion, Senior Director of Enterprise Applications
5. Grants Management: Pamela Ray, Senior Director Sponsored Research Administration
6. Compliance and Ethics: Robyn Blank, Chief Compliance and Ethics Officer
7. Internal Audit and Governance: Sam McCall, Chief Audit Officer
8. Office of Financial Aid Management: Somnath Chatterjee, Associate Director
9. Risk Management and Insurance Practices:
    a. Thomas Jacobson, Director Environmental Health and Safety
    b. Laymon Gray, Associate Director Environmental Health and Safety