Crowe

Smart decisions. Lasting value.™

Florida Board of Governors State University System

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

November 2019

I. Executive Summary

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

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

We have presented the results of our assessment of Florida Atlantic University (FAU) 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 FAU’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 FAU’s control structure.

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

FAU Observations Summary

Risk Category	Description	Risk Rating
Information Technology	**1. Information Security Governance - Key Risk and Performance Indicators.** FAU has not formally defined a process to measure the effectiveness of the Information Security Program. Additionally, the effectiveness of the program is not reported to the Compliance group.	Moderate
Information Technology	**2. Data Protection – Employee Removable Media.** FAU 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
Information Technology	**3. Data Protection - Mobile Device Management Program.** FAU has not documented a Mobile Device Management policy for employees and contractors which details requirements for mobile device security. This increases the risk that sensitive FIU information may be compromised if a malicious actor gains access to the phone or other mobile device.	Low
Information Technology	**4. Physical Security - Clean Desk Policy.** FAU does not have a university-wide "clean desk" policy. This increases the risk that sensitive information may be viewed or accessed by unauthorized parties.	Low
Information Technology	**5. Logging and Monitoring - Logging and Monitoring Policy.** Although FAU maintains a centralized log and performs regular log reviews, a formalized program has not been documented around logging and monitoring to ensure consistent standards are applied.	Low
Information Technology	**6. IT Operations - Asset Tracking.** FAU has not compiled a complete listing of all IT assets held by the organization.	Low
Information Technology	**7. Employee Management – Employee Security Awareness Training.** FAU 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

This report is furnished solely for the information and use of Florida Atlantic 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 Florida Atlantic University (FAU). 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 FAU management. Based on this information, we developed a risk and control assessment, summarized below.

Inherent Risk Assessment

We developed an inherent risk assessment for each university in the SUS. The inherent risk assessments consisted of a list of risk factors which, based on our research and experience, are relevant, impactful, and likely to occur in a university environment. We rated some inherent risks differently across universities due to environmental or organizational variables (e.g. research-based universities, student enrollment, campus location(s), age of infrastructure, student housing, etc.). At this point in the assessment we did not yet consider the specific risk management and controls that each university had in place to mitigate these risks. It was designed to provide a baseline upon which to measure control effectiveness at the university level.

Risk Rating Scale

Impact	Score
Low	1
Minor	2
Moderate	3
High	4
Severe	5

Likelihood	Score
Remote	1
Improbable	2
Possible	3
Probable	4
Almost Certain	5

Risk Rating	Score
Low	1
Minor	2
Moderate	3
High	4
Severe	5

We established the threshold for reportable risk levels at a residual risk score of 4 or higher.

We established a risk rating methodology to assign a score to each risk factor in the assessment as illustrated above. Our risk rating methodology considered two criteria, “Impact” and “Likelihood”. The “Risk Rating” represents the average of those two scores. The impact criterion addressed the effect on financial, operational, or compliance objectives if the risk factor were to occur. The likelihood criterion addressed the probability that the risk would occur in the current environment. Our scores were based on a five-point rating scale with one (1) representing the lowest, and five (5) representing the highest risk score. We labeled the risk rating in the same manner as the impact criterion for the purpose of simplicity and consistency.

Control Ratings

We also rated the internal controls in place according to the three criteria below. The percentage assigned to each rating represents the reduction in perceived levels of risk and was used to calculate the residual risk score.

- No Observations Noted (30% reduction to the inherent risk rating),
- Needs Improvement (15% reduction to the inherent risk rating), or
- Inadequate (0%, no reduction to the inherent risk rating)

We based the control ratings on the results of our research, discussions with management, and the supporting documentation they provided to help us analyze FAU’s control structure.

Residual Risk Assessment

We assigned a control 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 seven categories to have a minor level of residual risk and five categories to have a low level of residual risk. FAU's three highest categories of residual risk were Cash Management, Information Technology, and Procurement. However, based on our methodology, all risk categories were below our threshold for a reportable observation.

The bar graph illustrates the difference between the average inherent and residual risk scores for each risk category. Please note that if an individual risk factor exceeded the threshold, we would have reported an observation and recommendation for those factors. However, we did not note any individual risk factors that exceeded the threshold, and these key functions/risk categories also have average residual risk scores below our threshold. This is an indicator that our observations identified were not systemic to the functional area.

Exhibit 1: FAU Inherent vs. Residual Risk by Category

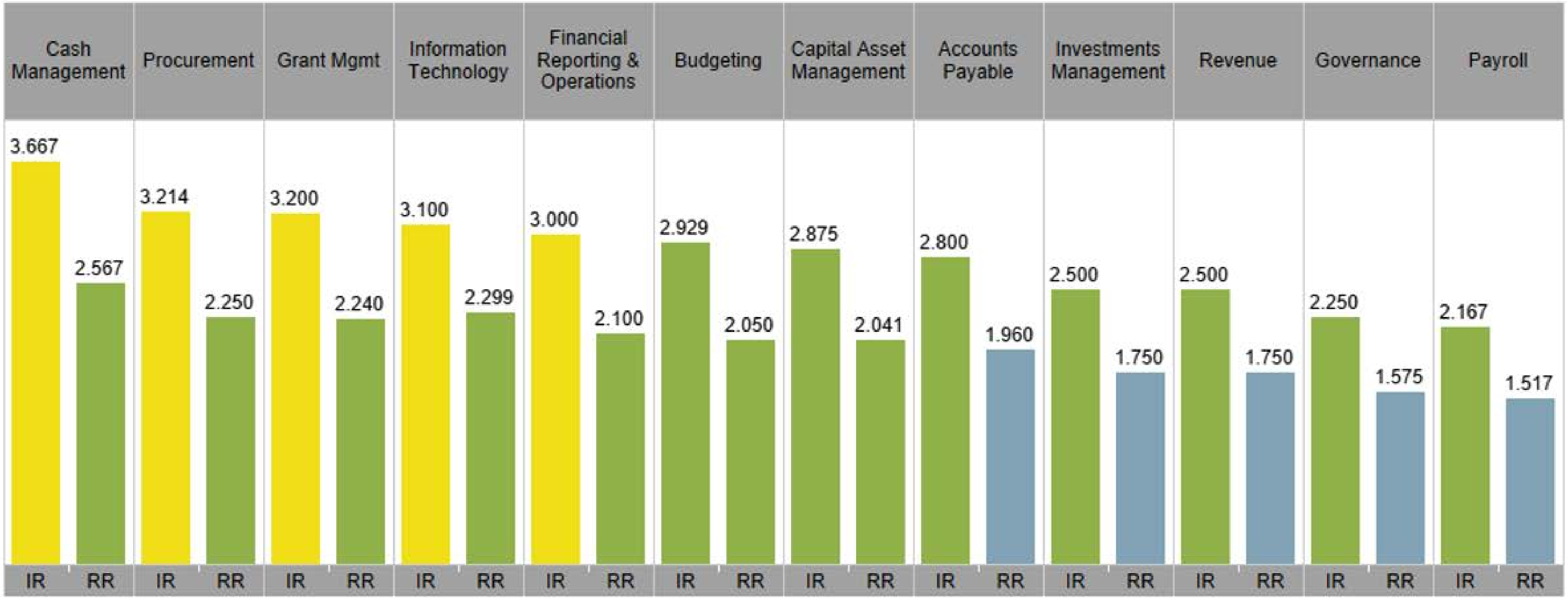
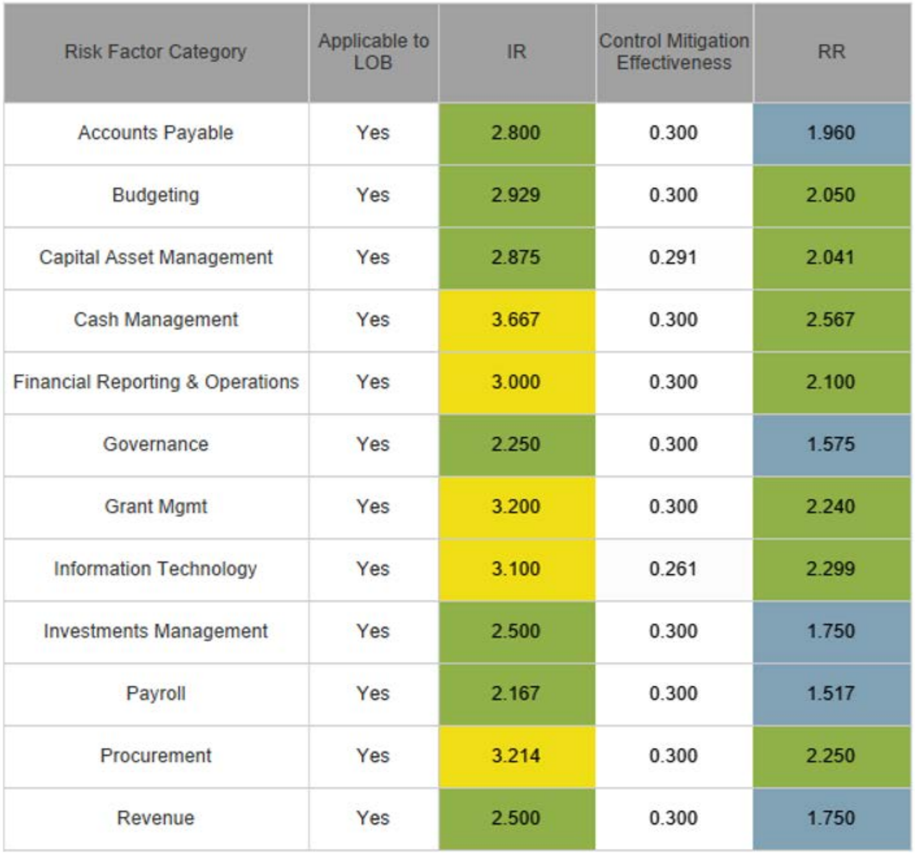


Exhibit 2 highlights similar information but use a different visualization to illustrate how the control rating reduced the level of inherent risk (i.e. resulting in the residual risk score). The inherent risk represents the baseline score in each category prior to considering internal controls. The control mitigation score represents our assessment of the controls in each category. The residual risk score is the net result of the two scores and is used to indicate whether the control structure was adequately designed to mitigate the associated risks to a reasonable level. Again, this exhibit indicates that all risk categories had average residual risks below our threshold for reportable observations.

Exhibit 2: FAU Inherent vs. Residual Risk with Control Rating



Risk Factor Category	Applicable to LOB	IR	Control Mitigation Effectiveness	RR
Accounts Payable	Yes	2.800	0.300	1.960
Budgeting	Yes	2.929	0.300	2.050
Capital Asset Management	Yes	2.875	0.291	2.041
Cash Management	Yes	3.667	0.300	2.567
Financial Reporting & Operations	Yes	3.000	0.300	2.100
Governance	Yes	2.250	0.300	1.575
Grant Mgmt	Yes	3.200	0.300	2.240
Information Technology	Yes	3.100	0.261	2.299
Investments Management	Yes	2.500	0.300	1.750
Payroll	Yes	2.167	0.300	1.517
Procurement	Yes	3.214	0.300	2.250
Revenue	Yes	2.500	0.300	1.750

Conclusion

Based on our procedures, we noted no individual risk factors which arose to the level of a reportable observation (i.e. a residual risk score of 4 or greater). However, our risk and control assessment enabled us to identify several areas to improve risk management and control practices. Additional detail on these observations, our recommendations on how FAU could address these observations, and FAU 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 FAU 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. FAU should consider strengthening their risk management practices through a more formal, systematic approach 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 FAU, and to provide observations and recommendations to the FAU Board of Trustees, FAU 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 FAU:

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

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

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. The procedures we completed during our assessment of FAU 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 FAU'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 FAU management the factual basis for our observations and recommendations. Management's written responses are included for each recommendation in this report.

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

V. Observations and Recommendations

Our procedures yielded seven (7) 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. Data Protection – Employee Removable Media**	Low
Information Technology	**3. Data Protection – Employee Mobile Device Management Policy**	Low
Information Technology	**4. Physical Security - Clean Desk Policy**	Low
Information Technology	**5. Logging and Monitoring - Logging and Monitoring Policy**	Low
Information Technology	**6. IT Operations - Asset Tracking**	Low
Information Technology	**7. Employee Management – Employee Security Awareness Training**	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 within the compliance report, 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 in part 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: FAU has not yet prioritized resources to complete the development of information security program metrics.

Implication: If the Compliance group is not aware of the effectiveness of the Information Security Program, the organization cannot effectively identify and mitigate its risk.

Recommendation: FAU should identify key performance indicators such as number of incidents, incident response times, results of risk and technical security assessments, etc. These metrics should be performed to the Compliance group on a regular basis (quarterly or annually). These metrics should be compared to past metrics to determine the overall status of the program and if any changes are necessary.

Management Response:

FAU disagrees with this finding. The finding indicates that FAU was evaluated against NIST 800-53 which is a standard developed by the Federal government and is stated directly in the standard that it is only applicable to systems operated by the Federal government. Furthermore, the revision used to assess FAU is still in a draft form and has not yet been finalized. The current non-draft version of NIST 800-53 (Revision 4) states the following in section 1.1: “1.1 PURPOSE AND APPLICABILITY The purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. ” REF: NIST800-53r4 available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf This is similarly worded in the draft version of NIST 800-53 Revision 5 (DRAFT) under the same section with the following wording: “1.1 PURPOSE AND APPLICABILITY This publication establishes controls for federal information systems and organizations. The use of these controls is mandatory, in accordance with the provisions of the Federal Information Security Modernization Act (FISMA), which require the development and maintenance of minimum controls to protect federal information and information systems. “REF: NIST 800-53r5 (DRAFT) which is available at: https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf A similar standard, NIST 800-171 may be used to assess FAU on certain requirements as NIST 800-171 is applicable to the protection of sensitive data provided by the Federal government and can be applied to any organization. This is the closest equivalent for systems not directly operated by the Federal government. NIST 800-171 would generally not be applicable to the entire institution as a hard requirement, it is a good standard to apply to an information security program on certain requirements. NIST 800-171 does not list the requirement or recommendation we are being assessed on. However, FAU does maintain and report metrics and KPIs for tracking certain indicators of effort and performance from the Information Security program above and beyond what would be required in NIST 800-171.

Crowe Comment:

Although the NIST 800.53 criteria was utilized as one of the authoritative sources, our assessment is built upon a variety of industry excepted standards including ISO, NIST, FFIEC, etc. The controls assessed during this review considered these standards; however, were derived from Crowe subject matter experts and industry experience. Although the University may not be required to adhere to the NIST standard, based on our experience and the requirements within multiple security standards we concluded that a risk is present based on the review of information provided.

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

Condition: Although FAU has implemented a process to request an encrypted removable media (i.e., USB drive) their use is not managed. Furthermore, technical controls have not been implemented to protect the access and provide data protection, such as encryption and device authentication.

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

Implication: Without restrictions and the protection of data, confidentiality, on the use of removable storage media through device encryption, there is the risk of unauthorized disclosure of business and customer information through the loss or misuse of the storage media.

Recommendation: To ensure the confidentiality and integrity of electronic data stored on a removable media, FAU 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. 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:

FAU partially agrees with this finding.   FAU has the toolsets available and deployed in areas with sensitive data; however, in many cases the removable media functionality is not deployed. The reason for this is many employees serve dual roles as employees and instructors in the classroom. However, FAU is working on solutions over the next year that will allow for securing these devices without impacting the ability to deliver instruction.

Planned for implementation by December 2020.

Observation 3	Process Area	Priority Rating
Data Protection – Employee Mobile Device Management Policy	Information Technology	Low

Condition: FAU has not formally documented a Mobile Device Management policy, which details requirements for the security of mobile devices, specifically phones as FAU users access their FAU email with their personal phones.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 AC-19 as the criteria upon which to evaluate these controls.

Root Cause: FAU has not prioritized formally documenting a Mobile Device Management policy.

Implication: Users who use FAU email on their phones without adequate protections, are at risk of compromising FAU information if an attacker gains access to the phone or other mobile device, both physically and remotely.

Recommendation: To ensure the confidentiality and integrity of electronic data stored on mobile devices, FAU should develop a policy to inform users of the required security controls to use FAU email on their personal phones. This should include, but not be limited to, full disk encryption, a secure PIN, and a lockout policy.

Management Response:

FAU partially agrees with this finding. The criteria mentioned, NIST 800-53 recommendations for Federally operated systems which are not present at FAU. Applying NIST 800-171 recommendations which cover non-Federally operated systems to FAU recommends that the University controls connections of mobile devices. FAU accomplishes this through many means, including treating wireless network connections as untrusted communications. Mobile devices owned by university or brought to the university in a BYOD fashion do not gain elevated access to university resources. Users are required to connect via applicable secure channels such as VPN to access internal university resources.

FAU does have a specific mobile device management policy for our HIPAA covered components and the technology is deployed there. For the remaining population FAU has mitigating controls such as the one described above. Additional examples of these controls include; DLP (Data Loss Protection), and controls in financial systems for sensitive data for remote workers. Because email is a public record at State Universities the confidentially of email conversations is not as high of a priority for protection via Mobile Device Management technologies.

No additional actions planned.

This report is furnished solely for the information and use of Florida Atlantic 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 4	Process Area	Priority Rating
Physical Security - Clean Desk Policy	Information Technology	Low

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

Criteria: We relied on the ISO 27001 A11.2.9 as the criteria upon which to evaluate these controls.

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

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

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

- Locking screens when employees leave their workstation
- Not writing down passwords
- Locking sensitive paper documents when not physically present
- Storing electronic information in designated areas (i.e. not on the local disk)

This policy should be implemented across all departments at FAU. IT should implement a process to periodically perform an inspection of workstation areas to verify departments are compliant with the policy.

Management Response:

FAU agrees with this finding. However, a clean desk policy is not a part of the Information Technology process area as indicated. A Clean Desk policy falls within general department operations. FAU has drafted a clean desk policy for consideration over the next year by University Executive Leadership.

Planned for implementation by December 2020.

Observation 5	Process Area	Priority Rating
Logging and Monitoring - Logging and Monitoring Policy	Information Technology	Low

Condition: Although FAU does have centralized log managed and performs regular reviews of logs, a formalized program has not been documented around logging and monitoring to ensure consistent standards are applied.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 AU-1 as the criteria upon which to evaluate these controls.

Root Cause: FAU has not yet prioritized resources to develop a formalized logging and monitoring policy.

Implication: Security incidents may go undetected and may not be stopped or prevented from causing damage to the company's computer systems, network, data, or business.

Recommendation: FAU should document a formal logging and monitoring program. This program should document the organization's logging and monitoring requirements. Suggested requirements include but are not limited to:

- System types to be logged
- Procedures for log review
- Alerting thresholds
- Log retention requirements
- Personnel to be alerted.

Management Response:

FAU Partially Agrees with this finding. NIST 800-53 is not applicable to the University as that standard specifically details recommendations for Federally operated systems which are not present at FAU. In addition, the version of NIST 800-53 cited is not finalized and is still in a draft form for seeking comments.

Applying NIST 800-171 to FAU, which is the standard recommendations for non-Federal systems, FAU is currently performing the activities recommended in section 3.3 which includes review and updating of logged events, supporting report generation to support on-demand analysis and reporting, providing systems to synchronize system times, retention of audit logs, and ensuring accountability for individual users.

Though we perform the activities, we do not have a formal policy governing them. FAU will create the policy and implement in the next 3 months.

Planned for implementation by February 2020.

Observation 6	**Process Area**	**Priority Rating**
IT Operations - Asset Tracking	Information Technology	Low

Condition: FAU has not compiled a complete listing of all IT assets held by the organization.

Criteria: We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 PM-5 as the criteria upon which to evaluate these controls

Root Cause: FAU has not prioritized the resources to compile an IT asset listing.

Implication: Without a fully centralized asset management solution, it is difficult to track the status of organization IT assets, creating a risk of sensitive data and equipment falling into unauthorized hands. Further, many IT security operations functions rely on an accurate asset inventory such as patch management, vulnerability management, replacement of unsupported systems, and processing of terminated employees.

Recommendation: FAU should establish an asset life cycle management process to manage the purchase, use, and decommissioning of assets, such as servers and workstations. The IT asset lifecycle is the sequence of stages that an organization's information technology asset goes through during the time span of its ownership. An IT asset is any company-owned information, software or hardware that is used in the course of business.

The stages of an IT asset's life-cycle are planning, procurement, deployment, usage, upgrade, decommission, disposition and salvage. IT asset management must incorporate effective procedures for each stage to promote the most effective use and maintenance of assets throughout the lifecycle and ensure their proper upgrading, replacement and disposal.

The three major stages are:

1. Acquisition – this begins the life-cycle of the asset. Once the asset is designed, procured, and installed according to specifications, it is placed in the RPI (Real Property Inventory). Here, it is tracked through its useful life.
2. Useful life – this stage encompasses the vast majority of the life-cycle. All operations and maintenance (O&M) activities are performed and tracked during the useful life stage in the life-cycle. When the asset has reached the end of its useful life, it is disposed.
3. Disposal – at the end of the asset's useful life, it is removed from service and sold, re-purposed, thrown away, or recycled. If there is still an operational need for the disposed asset's purpose, the life-cycle begins again with acquisition of a replacement.

Once a comprehensive asset lifecycle process has been established, a thorough review should be conducted for all assets in use by the organization. While conducting the review, all devices connected to the internal network should be logged including virtual servers, networking devices, and all software in use by the organization. These assets should be imported into the ServiceNow tool after the review is finished.

Management Response:

FAU agrees with this finding. FAU will develop a plan over this fiscal year to implement the tracking of IT assets and control avenues of procurement.

Planned for implementation by July 2020.

Observation 7	Process Area	Priority Rating
Employee Management – Employee Security Awareness Training	Information Technology	Low

Condition: Although FAU provides training upon hire and does provide ongoing security awareness activities, annual training is not currently 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: FAU has not prioritized resources to provide annual security training to all employees.

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

Recommendation: FAU should develop a program to provide annual training to users. This training should be updated at least annually to cover current and emerging cybersecurity risks and threats. Users should be required to sign an acknowledgement of this training and these acknowledgements should be tracked to ensure compliance.

Management Response:

FAU agrees with this finding. FAU is working to implement focused refresher training for all employees annually. We expect implementation in 3 to 6 months.

Planned for implementation by June 2020.

VI. Appendix - List of Interviewees at FAU

The following individuals were interviewed during our onsite visit to FAU the week of August 26, 2019. The name, title, and interview subject are included below.

1. Accounts Payable & Procurement:
   a. Jessica Cohen, University Controller
   b. Aaron Tramp, Assistant Director of Procurement
   c. Ed Schiff, Associate Director of Procurement
2. Budget and Financial Reporting:
   a. Stacey Bell, Associate Vice President for Finance, Planning and Analysis
   b. Jessica Cohen, University Controller
   c. Amy Cavasos, Director of Finance and Human Resource Information Systems
3. Capital Asset Management:
   a. Jessica Cohen, University Controller
   b. Stacy Volnick, Vice President for Administrative Affairs
   c. Azita Dashtaki, Associate Vice President for Facilities Management
4. Cash Management:
   a. Jessica Cohen, University Controller
   b. Elise Morgenstern, Associate Controller for Treasury Services and Financial Reporting
   c. Diana Zaia – Associate Controller over Cash and Investment Management
5. Compliance and Ethics: Elizabeth Rubin, Chief Compliance Officer
6. Grants Management:
   a. Lynn Asseff, Director of Financial Management
   b. Heather Saunders, Director of Research Accounting
7. Information Technology: Jason Ball, Chief Information Officer
8. Payroll: Rosa Naujoks, Tax Services Director, Payroll
9. Student Billing:
   a. Jessica Cohen, University Controller
   b. Desi Angelova, Assistant Controller
10. Governance: FAU Board of Trustees Chair, Anthony K. G. Barbar