
# Florida Board of Governors State University System

# University of West Florida
# Internal Management and Accounting Control and Business Process Assessment
# November 2019

Florida Board of Governors State University System
University of West Florida (UWF) Internal Management and Accounting Control and Business Process Assessment
November 2019

# I. Executive Summary

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

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

We have presented the results of our assessment of the University of West Florida (UWF) 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 UWF'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 UWF's control structure.

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

**UWF Observations Summary**

| Risk Category | Description | Risk Rating |
|---|---|---|
| Procurement | **1. Contract Management – Shared Services Contracts.** UWF has not established roles and responsibilities for managing shared service contracts. As a result, it was unclear how UWF established contract ownership and vendor performance monitoring, as well as how it verified that appropriate insurance, data privacy, and intellectual property protections were in place. | Moderate |
| Procurement | **2. Policies and Procedures – Vendor Setup and Monitoring.** UWF did not have documented standards or processes for vendor performance monitoring, as stipulated in BOG regulations 18.001, subsection (f). Therefore, it was unclear what standard practices, roles, and responsibilities had been implemented. | Moderate |
| Information Security | **3. Business Continuity Management – Incident Classification.** UWF does not have documented procedures or a classification schema to prioritize and respond to cybersecurity incidents. This increases the risk that UWF may not be able to appropriately and effectively respond to threats. | Moderate |
| Information Security | **4. Data Protection – Employee Removable Media.** UWF has not established a policy or 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 Security | **5. Employee Management – Employee Security Awareness Training.** UWF does not provide security training to employees on a reoccurring basis. If employees are not be prepared to identify emerging and evolving threats and tactics, it increases the likelihood of a successful breach. | Low |
| Information Security | **6. Data Protection – Employee Mobile Device Management Policy.** UWF 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 UWF information may be compromised if a malicious actor gains access to the phone | Low |

# II. Assessment Overview

The Board of Governors (the "Board" or "BOG") of the Florida State University System (SUS) engaged Crowe LLP to perform a system-wide "Internal Management and Accounting Control and Business Process Assessment". The purpose of this assessment was to evaluate the existing internal controls and review business processes to identify any areas of risk for the SUS. We performed these consulting services in accordance with the Standards for Consulting Services established by the American Institute of Certified Public Accountants. These services do not constitute an audit, review, or examination in accordance with standards established by the American Institute of Certified Public Accountants, and therefore, Crowe did not express an opinion on the accuracy or efficacy of the material assessed during the performance of these services.

The scope of our assessment was focused primarily on financial and operational risks, and secondarily on regulatory compliance risks. It included the twelve universities within the SUS as follows:

- Florida Agricultural and Mechanical University (FAMU)
- Florida Atlantic University (FAU)
- Florida Gulf Coast University (FGCU)
- Florida International University (FIU)
- Florida Polytechnic University (FPU)
- Florida State University (FSU)
- New College of Florida (NCF)
- University of Central Florida (UCF)
- University of Florida (UF)
- University of North Florida (UNF)
- University of South Florida (USF)
- **University of West Florida (UWF)**

This report represents the results of our assessment of the University of West Florida (UWF). 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 UWF 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 UWF’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 nine categories to have a minor level of residual risk and three categories to have a low level of residual risk. UWF's three highest categories of residual risk were Governance, Procurement, and Information Technology. 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: UWF Inherent vs. Residual Risk by Category**

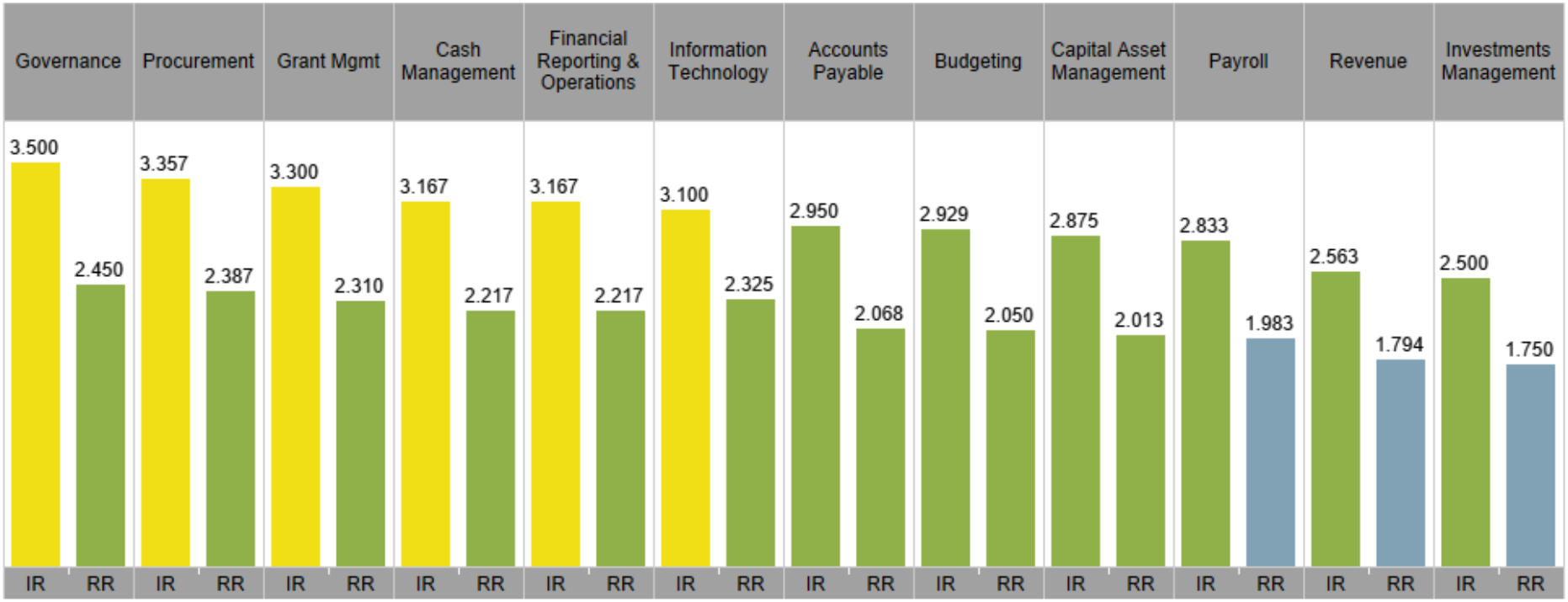

**Exhibit 2** highlights similar information but uses different visualizations to illustrate how the control rating reduced the level of inherent risk (i.e. resulting in the residual risk score). The inherent risk represents the baseline score in each category prior to considering internal controls.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

**Exhibit 2: UWF Inherent vs. Residual Risk with Control Rating**

| Risk Factor Category | IR | Control Mitigation Effectiveness | RR |
|---|---|---|---|
| Accounts Payable | 2.950 | 0.299 | 2.068 |
| Budgeting | 2.929 | 0.300 | 2.050 |
| Capital Asset Management | 2.875 | 0.300 | 2.013 |
| Cash Management | 3.167 | 0.300 | 2.217 |
| Financial Reporting & Operations | 3.167 | 0.300 | 2.217 |
| Governance | 3.500 | 0.300 | 2.450 |
| Grant Mgmt | 3.300 | 0.300 | 2.310 |
| Information Technology | 3.100 | 0.250 | 2.325 |
| Investments Management | 2.500 | 0.300 | 1.750 |
| Payroll | 2.833 | 0.300 | 1.983 |
| Procurement | 3.357 | 0.289 | 2.387 |
| Revenue | 2.563 | 0.300 | 1.794 |

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

We also noted a common theme throughout our assessment that the university would likely benefit from an enhanced focus in the areas where third-party risk management and data protection intersect. While we have addressed specific risks in our observations and recommendations, we understand that this is an area in which UWF and many other higher education institutions are expanding or will be planning to expand their operational activities. For example, the number of providers and types of services in this area is rapidly expanding, and consequently, so are the associated risks. For example, university student support, call centers, or collection agencies are commonly granted access to student account information. Payroll service providers receive and transmit data electronically, and cloud-based storage services are becoming an increasingly efficient and inexpensive way in which to manage large amounts of data, including personally identifiable and sensitive data.

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

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 UWF 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 UWF'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 UWF 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 |
|---|---|---|
| Procurement | **1. Contract Management – Shared Service Contracts** | Moderate |
| Procurement | **2. Policies and Procedures – Vendor Setup and Monitoring** | Moderate |
| Information Security | **3. Business Continuity Management – Incident Classification** | Moderate |
| Information Security | **4. Data Protection – Employee Removable Media** | Low |
| Information Security | **5. Employee Management – Employee Security Awareness Training** | Low |
| Information Security | **6. Data Protection – Employee Mobile Device Management Policy** | Low |

**Observations and Recommendations**

| Observation 1 | Process Area | Priority Rating |
|---|---|---|
| Contract Management – Shared Services Contracts | Procurement | Moderate |

**Condition:** UWF has not established roles and responsibilities for managing shared services contracts with other entities. For example, UWF did not provide copies of executed contracts to demonstrate that service level expectations, insurance requirements, data privacy and intellectual property protections, and other significant areas of risk had been identified, adequately addressed, and monitored for compliance. Additionally, the ownership for monitoring performance under the terms and conditions of those agreements had not been clearly established.

**Criteria:** BOG Regulation 18.001 (1) Each university Board of Trustees shall adopt regulations establishing basic criteria related to procurement, including procedures and practices to be used in acquiring commodities and contractual services, as follows: (c) Evaluating, approving, and utilizing contracts let by any State of Florida agency or department, the Federal Government, other states, political subdivisions, not-for-profit cooperatives or consortia, or any independent college or university for the procurement of commodities and contractual services, when it is determined to be cost-effective and in the best interest of the University, to make purchases under contracts let by such other entities.

**Root Cause:** UWF stated that they primarily rely on the entity who negotiated the agreement to manage the contract (e.g. the BOG, other universities in the SUS, or other third parties). As a result, UWF has not prioritized the standardization of forming these types of agreements or assigning ownership to monitor performance.

**Implication:** The lack of standard practices for establishing shared service contracts increases UWF's exposure to a wide-range of risks, which include loss of intellectual property or personally identifiable information, financial liability, excessive costs or delays, subpar quality of goods and services, and the inability to achieve expected outcomes.

**Recommendation:** Crowe recommends that UWF document the process for executing shared service contracts. The process should include but is not limited to 1) Identifying roles and responsibilities for initiating, reviewing, and executing the agreement. 2) Clarifying scope of services, period of performance, performance metrics, and other technical matters.3) Establishing standard terms and conditions that address issues of data privacy, intellectual property, and insurance requirements. 4) Identifying ownership, roles, and responsibilities for monitoring performance throughout the length of the agreement.

**Management Response:**
Management agrees. For shared services we will create Participation Agreements with the other institutions. We will ensure the following information is covered:

- Roles and responsibilities for initiating, reviewing and executing the agreement,
- Scope of services, period of performance, technical matters and performance metrics,
- Standard terms and conditions addressing data privacy, intellectual property and insurance requirements, and
- Ownership, roles and responsibilities for monitoring performance.

Planned for implementation by April 30, 2020

| Observation 2 | Process Area | Priority Rating |
|---|---|---|
| Policies and Procedures – Vendor Setup and Monitoring | Procurement | Moderate |

**Condition:** The University did not have documented standards or a process for monitoring and tracking the performance of vendors as stipulated in BOG regulations. UWF had documented procedures for several components of the procurement function, such as for P-Cards and purchase requisitions; however, they did not have documented procedures for vendor setup or monitoring. UWF's Director of Procurement stated that UWF consistently performs a thorough vendor certification process to ensure new vendors are not on any disbarred list, will be able to provide the requested goods or services, and present no conflict of interest issues; however, these practices were not documented as standard operating procedures. It was also unclear what standard practices, roles, and responsibilities were established for monitoring vendor performance.

**Criteria:** BOG Regulations 18.001 requires universities to establish, "Basic criteria related to procurement, including procedures and practices to be used in acquiring commodities and contractual services." Subsection (f) of that regulation specifies that these criteria should include, "barring any vendor from doing business with the University for demonstrated cause, including previous unsatisfactory performance."

**Root Cause:** UWF has not prioritized documenting its practices for vendor setup and monitoring due to its reliance on experienced staff members with substantial institutional knowledge.

**Implication:** Without a formally documented procedure in place for third party vendor setup, there is an increased risk that new suppliers will not be properly vetted before being allowed to do business with UWF. Similarly, vendor monitoring practices are more likely to be overlooked or performed inconsistently without documented standard operating procedures. This risk would increase further in the event of turnover in positions currently responsible for vendor setup and monitoring.

**Recommendation:** We recommend that UWF document standard operating procedures for vendor setup, including requirements for conducting:

- Reference and background checks
- Verifying proper licensing and insurance coverage
- Validating tax identification information

We recommend that UWF document standard practices for vendor performance monitoring, including:

- Assigning of ownership for monitoring procedures
- Contract compliance checks
- Invoice review and approvals by technical or subject matter experts
- Mechanisms for reporting subpar performance and debarring vendors.

UWF should incorporate these standard procedures into routine employee training for those charged with procurement or vendor management responsibilities.

**Management Response:**

Management Agrees. UWF will identify 'critical' vendors and contracts to monitor performance and assign ownership of monitoring procedures, contract compliance checks, and mechanisms for reporting subpar performance and debarring of vendors. The invoice review and approval by technical or subject matter experts will be the responsibility of the department acquiring the goods or services. This will be included in the UWF Procurement Manual.

Planned for implementation by April 30, 2020.

| Observation 3 | Process Area | Priority Rating |
|---|---|---|
| Business Continuity Management – Incident Classification | Information Security | Moderate |

**Condition:** The organization has not documented a procedure for the classification and prioritization of cybersecurity incidents. Additionally, a classification schema has not been documented within policy that details criteria for detected cybersecurity incidents.

**Criteria:** We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 IR-1, IR-8 as the criteria upon which to evaluate these controls.

**Root Cause:** UWF has not prioritized resources to create a classification policy. UWF stated in their response to our control questionnaire that they do not deal with a significant number of cybersecurity incidents.

**Implication:** Without an implemented procedure to classify and prioritize incidents, UWF may not be able to effectively respond to threats, resulting in the misidentification of the severity of an incident and hampering the response effort.

**Recommendation:** UWF should update the incident response program to include requirements and procedures to classify and prioritize cybersecurity incidents. This should include an analysis of the systems affected and what data is stored on those systems. A classification schema should be created to rank the criticality of each incident. Each level of criticality should include detailed instructions on response time expectations, and communication plans.

**Management Response:**

Management agrees. We will develop a cybersecurity classification schema based on several factors including the category of the system, the level of data sensitivity and possible broader consequences to dependent systems. The schema will describe the kind of incident and expected response plans.

Planned for implementation by the close of Q1 2020.

| Observation 4 | Process Area | Priority Rating |
|---|---|---|
| Data Protection – Employee Removable Media Management | Information Security | Low |

**Condition:** UWF has not established a policy to manage employees' and contractors' use of removable media, (i.e. USB drives). Also, technical controls have not been implemented to restrict 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:** UWF has not prioritized resources to address the risk of employees using removable media.

**Implication:** Without restrictions on the 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:** UWF 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:**

Management partially agrees. This observation as written is impractical and possibly detrimental to the academic mission of the University. A University by its very nature needs to allow for the use of removable media given there are innumerable reasons and needs for external devices (many which have storage capabilities) which serve teaching and learning purposes. The University is not a “company” with homogenous and strictly defined equipment. In addition, the solutions suggested in the table (a few of which no longer point to secure web pages) and the Technet article are not adequate to provide sufficient technical controls for the kind of environment we have. However, we do recognize that the use of USB drives can be a risk and UWF has already banned their use with respect to Protected information via our Information Security & Privacy Policy. In addition, we recognize that we can, in a limited fashion, apply technical controls to administrative endpoint workstations used by employees with elevated privileges who would pose the greatest risk to an information breach.

We will employ our existing endpoint protection product (Cylance) to place a technical control to prevent the use of USB devices on computers within certain areas of high risk due to the access to large stores of Protected information. We will determine this by grouping these endpoint workstations in a special ‘area’ within the management capabilities of the Cylance platform.

Implementation Plan: We will implement these controls in a pilot area by close of Q1 2020 and if the pilot is successful, we will implement to all other identified areas of risk by end of Q4 2020.

| Observation 5 | Process Area | Priority Rating |
|---|---|---|
| Employee Management – Employee Security Awareness Training | Information Security | Low |

**Condition:** Although UWF provides security training to new users upon hire, annual training is not required. Through discussion with UWF, they are evaluating an annual security awareness training program; however, one was not in place at the time of the assessment.

**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:** UWF has not prioritized resources to provide annual security training.

**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 breach.

**Recommendation:** UWF should continue with the plan to 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:**

Management agrees. We are reviewing cybersecurity awareness material we have already developed and additionally compiled from other sources. We will create a ‘certification’ that will be tracked electronically and will track the yearly completion of cybersecurity awareness for all employees classified as “knowledge workers”. We will review and update the material yearly as appropriate to highlight new threats. Additionally, we will amend the University Information Security & Privacy policy to compel employees to complete this yearly awareness training.

Implementation Plan: The training and certification will become available by the end of Q2 2020.

| Observation 6 | Process Area | Priority Rating |
|---|---|---|
| Data Protection – Employee Mobile Device Management Policy | Information Security | Low |

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

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

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

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

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

**Management Response:**

Management partially agrees. The University does not provide mobile phones to its employees nor does it have the budget for an enterprise-wide MDM. However, we recognize that policy and guidelines for the safe use of personal mobile devices are an important addition to our security posture. We will also include a training module to inform employees of the proper safety best practices.

Implementation Plan: We have drafted a mobile and personal device policy and will be submitting this policy through the policy process by the start of Q1 2020.

# VI. Appendix

**List of Interviewees at UWF**

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

1. Budgeting and Financial Management: Betsy Bowers, Vice President Finance & Administration
2. Capital Budget Management: Melinda Bowers, Associate Vice President Facilities Management
3. Capital and Operating Budget Preparation and Management: Michelle Randu, Budget Manager
4. Business Continuity & Disaster Recovery: Peter Robinson, Director of Environmental Health & Safety
5. Business Continuity & Disaster Recovery: Nicole McDonald, Assistant Director of Environmental Health & Safety
6. Business Continuity & Disaster Recovery: Pennie Sparks, Risk Manager
7. Financial Accounting and Operations: Colleen Asmus, Controller
8. Financial Accounting and Operations: Billy Pollard, Senior Associate Controller
9. Financial Accounting and Operations: Jeffrey Djerlick, Associate Controller
10. Student Billing: Lisa Griswold Student Accounts
11. Student Billing: Audrey Liss, Student Accounts
12. Grants Management, Dr. Matthew Schwartz, Associate Vice President of Research Administration
13. Information Security and Data Privacy: Geissler Golding, Director of Infrastructure & Chief IT Security Officer
14. Procurement: Angie Jones, Director, Procurement & Contracts
15. Regulatory Compliance: Matt Packard, Chief Compliance Officer
16. UWF Board of Trustee Chair, J. Mort O'Sullivan