
# Florida Board of Governors State University System

# University of Central Florida
# Internal Management and Accounting Control and Business Process Review

November 2019

Florida Board of Governors State University System
University of Central Florida (UCF) Internal Management and Accounting Control and Business Process Review
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 Review". The purpose of this review 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 does not express an opinion on the accuracy or efficacy of the material reviewed during the performance of these services.

The scope of our review 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 review of the University of Central Florida (UCF) 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 review. Residual risk refers to the level of risk after considering the effectiveness of controls and other activities implemented to mitigate that risk. An in-depth discussion of our approach and rating methodology can be found in the *Assessment Overview* section of this report.

**Conclusion**

While the scope of our review precludes us from issuing an opinion on UCF'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 UCF'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 UCF 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, but we do not provide an opinion on the system of internal controls. 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 UCF management's responses can be found in the *Observations and Recommendations* section of this report.

**UCF Observations Summary**

| Risk Category | Description | Risk Rating |
|---|---|---|
| Financial Reporting | **1. Restricted Funds – Interfund Transfers.** UCF has not implemented controls to prevent or detect transfers in or out of restricted funds. Reports may be run on an ad-hoc basis to detect such transfers. This increases the risk that inappropriate transfers and use of restricted funds will go undetected. | Moderate |
| Information Technology | **2. Configuration Management – Configuration Management Program.** UCF 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 UCF to vulnerabilities. | Moderate |
| Information Technology | **3. Information Security Governance – Cybersecurity Risk Management Program.** UCF has not implemented an IT and Cybersecurity risk assessment program that defines cybersecurity risks, inherent risk (impact, threats, likelihood), and residual risk. This increases the risk that the university may not identify areas of high inherent risk and take the appropriate steps to prioritize and implement the appropriate mitigating controls. | Low |
| Information Technology | **4. Employee Management – Employee Security Awareness Training.** UCF 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 Technology | **5. Data Protection – Clean Desk Policy.** UCF 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 | **6. Data Protection – Employee Removable Media.** UCF 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 |

# 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 Review". The purpose of this review 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 does not express an opinion on the accuracy or efficacy of the material reviewed during the performance of these services.

The scope of our review 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 review of the University of Central Florida (UCF). As part of our review, 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 UCF 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 Effectiveness Ratings

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

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

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

### Residual Risk Assessment

We assigned a control effectiveness rating to each control to arrive at a residual risk rating in a consistent manner. The residual risk assessment was intended to provide an overview of the university’s risk management and control effectiveness. We recognized that each control and its related risk had unique components that would not be fully represented by the control effectiveness or residual risk rating. Therefore, we developed an observation and recommendation for controls rated as “Needs Improvement” or “Inadequate” in order to provide additional insight into that specific matter.

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 review. 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. UCF's three highest categories of residual risk were Procurement, Information Technology, and Grant Management. 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: UCF Inherent vs. Residual Risk by Category**

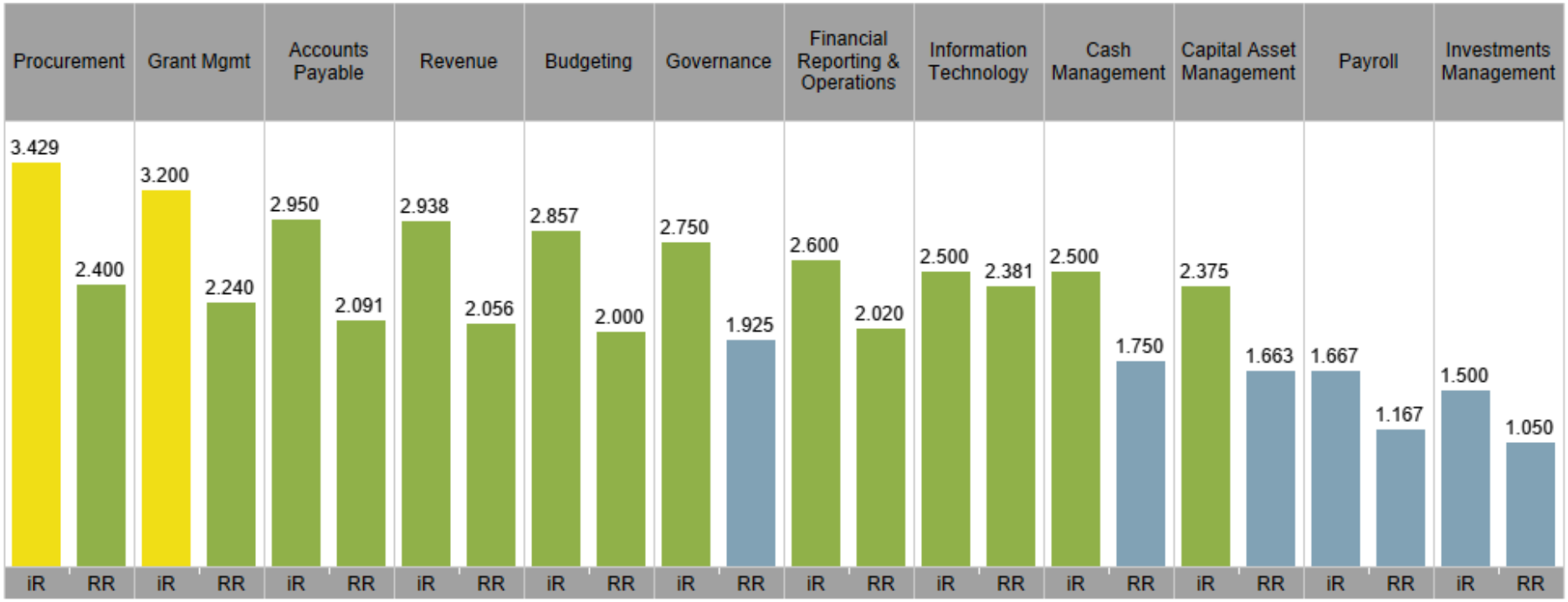

**Exhibit 2** highlights similar information but uses different visualizations to illustrate how the control effectiveness rating reduced the level of inherent risk (i.e. resulting in the residual risk score). The inherent risk represents the baseline score in each category prior to considering the effectiveness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

| Risk Factor Category | iR | Control Mitigation Effectiveness | RR |
|---|---|---|---|
| Accounts Payable | 2.950 | 0.293 | 2.091 |
| Budgeting | 2.857 | 0.300 | 2.000 |
| Capital Asset Management | 2.375 | 0.300 | 1.663 |
| Cash Management | 2.500 | 0.300 | 1.750 |
| Financial Reporting & Operations | 2.600 | 0.250 | 2.020 |
| Governance | 2.750 | 0.300 | 1.925 |
| Grant Mgmt | 3.200 | 0.300 | 2.240 |
| Information Technology | 2.500 | 0.064 | 2.381 |
| Investments Management | 1.500 | 0.300 | 1.050 |
| Payroll | 1.667 | 0.300 | 1.167 |
| Procurement | 3.429 | 0.300 | 2.400 |
| Revenue | 2.938 | 0.300 | 2.056 |

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

We believe that UCF would benefit from several high-value enhancements such as automating controls over fund transfers within their existing financial reporting ERP modules or when the university begins implementing its new ERP system, which is currently in the planning stages. Additionally, the university could strengthen its control structure over Information Technology risks with several process and procedural enhancements over mobile computing and workspace security.

Finally, we conclude that with continuous advances in technology, universities can exponentially improve the level and reach of services to its students and increase administrative efficiencies. However, 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. UCF should consider strengthening their risk management practices through its developing enterprise risk management program 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 while pursuing its mission.

# III. Objectives and Scope

The purpose of this review 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 UCF, and to provide observations and recommendations to the UCF Board of Trustees, UCF 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 UCF:

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

We performed these consulting services in accordance with the Standards for Consulting Services established by the American Institute of Certified Public Accountants. These services do not constitute an audit, review, or examination in accordance with standards established by the American Institute of Certified Public Accountants, and therefore, Crowe does not express an opinion on the accuracy or efficacy of the material reviewed during the performance of these services. 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 review of UCF 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 review 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 UCF'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 UCF 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 |
|---|---|---|
| Financial Reporting | **1. Restricted Funds – Interfund Transfers** | Moderate |
| Information Technology | **2. Configuration Management – Configuration Management Program** | Moderate |
| Information Technology | **3. Information Security Governance – Cybersecurity Risk Management Program** | Low |
| Information Technology | **4. Employee Management – Employee Security Awareness Training** | Low |
| Information Technology | **5. Data Protection – Clean Desk Policy** | Low |
| Information Technology | **6. Data Protection – Employee Removable Media** | Low |

**Observations and Recommendations**

| Observation 1 | Process Area | Priority Rating |
|---|---|---|
| **Restricted Funds – Interfund Transfers** | Financial Reporting | Moderate |

**Condition:** UCF has not implemented controls to prevent or detect transfers in or out of restricted funds. While reports may be run on an ad-hoc basis to detect such transfers, a process has not been established to review these transactions.

**Criteria:** Interfund transfers should be prohibited, unless extraordinary circumstances prevail, to prevent unauthorized or inappropriate use of restricted funds.

**Root Cause:** UCF has not yet prioritized resources to implement controls over fund transfers.

**Implication:** In the absence of preventive or detective control mechanisms, the risk increases that an inappropriate transfer and/or use of funds will go undetected.

**Recommendation:** We recommend that UCF configure and implement automated controls within their financial accounting system to restrict interfund transfers. In the short-term UCF should establish a review process to identify and validate all interfund transfers.

**Management Response:**

The university is establishing an additional automated ERP financial system workflow control at the executive management level to review and approve construction general ledger journals of $2 million or more prior to posting the journal. Ongoing training will be provided to key personnel to ensure that these controls are effectively and consistently implemented.

Planned for implementation by December 31, 2019.

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

**Condition:** Although UCF has documented IT configuration standards, templates, and system baselines for information systems (server, networking device, workstation, mobile devices, etc.), a Configuration Management Program, which includes security configurations (hardening guides) has not been documented. As an example, the configuration standards and templates do not include:

- **Security Impact Statements** – Prior to being placed into production use, each new, or significantly modified, or enhanced information system must include a brief security impact statement that has been prepared according to standard procedures.
- **Acceptance Criteria** – The acceptance criteria for new information systems, upgrades, and the implementation of new versions must include performance and capacity management requirements
- **Security Requirements Identification** – Before an information system undergoes configuration activities, Management must have clearly specified and documented the relevant security requirements.
- **Production Systems Documentation** – Every software or hardware system to be used for production business activities must be clearly documented and approved in advance of its deployment.
- **Security Hardening Standards** – All information systems placed into product must conform to minimum security configurations standards defined by the Information Security Department, which may include but not limited to:
    - **Default Passwords** – All vendor-supplied default passwords must be changed before any computer or communications system is used for business.
    - **User ID Review** – Before any production multi-user computer operating system is installed, all privileged user IDs that are not assigned to a specific employee or partner must be renamed or disabled.
    - **Unnecessary Software** – Software features that could be used to compromise security, and that are clearly unnecessary in the computing environment, must be disabled at the time when software is installed on multi-user systems.
    - **Unnecessary Functionality** – All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed from the computer and communication infrastructure.
    - **System Security Status Tools** – Every multi-user system must include sufficient automated tools to assist the Security Administrator in verifying the security status of the computer and must include mechanisms for the correction of security problems.

- **Certified Organization** – A procedure document should be obtained describing the organization manages configuration compliance. Document any tools used to support this process.
- **System Integrity Checking Software** – Based on risk, information systems must run integrity checking software that detects changes in configuration files system software files, application software files, and other system resources.

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

**Root Cause:** UCF has not prioritized the standardization of forming a Configuration Management Program.

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

**Recommendation:** UCF should formally document a Configuration Management Program, which is based on industry IT and Security best practices and should reference all currently documented standards / templates. Additionally, security configuration standards (hardening guides) should be referenced when developing system baselines.

The Configuration Management Program and each standard / guideline should include, but not limited to, the purpose, scope, roles and responsibilities, violations, approval and ownership, and references (if applicable). At a minimum, Management should perform a yearly review, update, and approval of each procedure, standard, and guideline to verify they meet or exceed current industry security standards and practices.

**Management Response:**

UCF management agrees with the need to document the organization's configuration requirements and procedures, and accordingly has previously established a comprehensive set of such standards, copies of which have been previously provided. As an element of UCF's ongoing efforts to increase the efficacy of its cybersecurity posture, we are implementing NIST 800-53 standards more broadly, while pursuing NIST 800-171 controls where appropriate.

Planned for implementation by August 2020.

| Observation 3 | Process Area | Priority Rating |
|---|---|---|
| Information Security Governance – Cybersecurity Risk Management Program | Information Technology | Low |

**Condition:** UCF has not implemented an IT and Cybersecurity Risk Assessment Program that defines cybersecurity risks, inherent risk (impact, threats, likelihood), and residual risk.

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

**Root Cause:** UCF has not prioritized resources to develop an IT and Cybersecurity Risk Assessment Program as recommended by the referenced security standards.

**Implication:** The organization may not be able to identify areas of high inherent risk and take the appropriate steps to prioritize and implement the appropriate mitigating controls.

**Recommendation:** UCF should institute a cybersecurity risk assessment process to determine compliance with the university's security requirements and controls. The risk assessment program should include requirements for determining risk, performing assessments to measure control effectiveness, and establishing a risk tolerance threshold.

The program should document the methodology for performing risk assessments, including a "top-down" or "bottom-up" approach.

A "top-down" risk assessment identifies cybersecurity risk(s) at the business or organizational level (i.e. risk scenarios). A "bottom-up" risk assessment assigns risks to organizational asset(s) or software. Each approach should develop and use impact categories to determine how each risk may affect the organization, if realized. The process should include employee surveys and an evaluation of controls, with applicable departments, to determine the impact, likelihood (threat assessment), and residual risk in order to determine inherent cybersecurity risks. UCF should use the outcome of this assessment to prioritize information security initiatives to reduce the overall risk profile. Management should also investigate solutions for developing and implementing a risk management framework.

The "bottom-up" risk assessment can also be utilized during the planning stage of the system development life cycle (SDLC), during the evaluation stage of a vendor product review, and\or annually for critical high-risk systems and when critical changes are made. The chosen risk assessment methodology and process should be evaluated on an annual basis.

The cybersecurity risk assessment process should consider:

1. The criticality of the system;
2. The sensitivity of the information processed;
3. The value of the system or application;
4. The threats associated with the system or application;

5. The likelihood of the threats occurring, and the potential damage of an incident derived from the threat;
6. The system's exposure to the threat;
7. The system's or application's vulnerabilities; and
8. The system interfaces and extent of system interconnections, including internal and external dependencies.

The result(s) of the risk assessment should conclude:

1. Residual risk and risk level (i.e., high, moderate, or low, for each risk).
2. Findings identified based on lack of controls or non-compliance with required controls to reduce the inherent risk.
3. Finding Action Plan – The action taken to remediate, transfer, mitigate or accept the risk.

**Management Response:**

UCF Management agrees with the essence of the audit recommendation. The UCF Information Security Office strives to comply with the NIST Cybersecurity Framework (CSF) and has several elements of a risk management program in place; these have been previously provided.

Implementing an institution-wide Cybersecurity Risk Management Program will require considerable resources. UCF Information Security Office does not currently have the resources to establish a comprehensive risk management program for the entire organization. The UCF Information Security Office, in collaboration with the University's Compliance & Risk Management Office, will submit a fiscal year 2020-21 request for the resources required to develop a comprehensive internal program. Contingent on resources and applicable scope of IT risk management, the Information Security Office will aim to implement an appropriate Cybersecurity Risk Management Program by Fall 2023.

Planned for Implementation by Fall 2023 (contingent upon funding).

| Observation 4 | Process Area | Priority Rating |
|---|---|---|
| Employee Management – Employee Security Awareness Training | Information Technology | Low |

**Condition:** Although UCF provides security training to new users upon hire, annual training is not required.

**Criteria:** We relied on the National Institute of Standards and Technology (NIST) SP 800-53 r5 AT-3 as the criteria upon which to evaluate these controls.

**Root Cause:** UCF has not prioritized resources to provide annual security training to all employees.

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

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

**Management Response:**

UCF Management agrees with the audit recommendation. The UCF Information Security Office is in the process of creating a security awareness policy that will require all employees to complete annual security awareness training. We anticipate the policy will be approved in Spring 2020 and by Fall 2020 every employee will be assigned to an online security awareness training course delivered through the University's learning management system. This meets NIST 800-53 r4 AT-1 and AT-2 requirements. However, to meet the NIST requirement SP 800-53 r5 AT-3, as suggested by the audit, will require additional staff resources and content development. The UCF Information Security Office will submit a fiscal year 2020-21 request for resources to establish a Security Awareness Program Manager position, which will further develop the security awareness program, implement initiatives to increase the reach of awareness efforts, and establish partnerships with other UCF departments.

Planned for implementation by Fall 2020.

| Observation 5 | Process Area | Priority Rating |
|---|---|---|
| Data Protection – Clean Desk Policy | Information Technology | Low |

**Condition:** Although some departments have clean desk programs, UCF 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:** UCF 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:** UCF 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 UCF. IT should implement a process to periodically perform an inspection of workstation areas to verify departments are compliant with policy.

**Management Response:**

UCF Management agrees with the audit recommendation. The UCF Information Security Office, in concert with the General Counsel's Office and University Compliance, Ethics, and Risk, will centralize existing policies and training materials into a specific Clean Desk policy and deliver it to the University Policy Committee for approval by Fall 2020.

Planned for Implementation by Fall 2020.

| Observation 6 | Process Area | Priority Rating |
|---|---|---|
| Data Protection – Employee Removable Media | Information Technology | Low |

**Condition:** Although UCF 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:** UCF 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:** UCF 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 university 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:**

UCF Management agrees with the audit recommendation and will work on an implementation plan that balances effective controls while avoiding excessive disruption. The UCF IT Endpoint Engineering Team will conduct research during summer of 2020 and determine the feasibility of implementing technical controls in the fall 2020 timeframe.

Planned for Implementation by Fall 2020.

# VI. Appendix - List of Interviewees at UCF

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

1. Information Technology – David Canova, Director Enterprise Applications, Mike Sink, Assoc VP & COO, Aaron Stremish, Sr. Director IT Strategy & Planning
2. Grant Management – Michelle Greco, Grant & Regulatory Assoc. Controller, Dorothy Yates, Assoc. VP, Research Admin, Doug Backman, Dir. Sponsored Programs
3. Governance – Liz Klonoff, VP of Research
4. Payroll – Jeremy Armstrong, Payroll Manager
5. Capital Projects – Misty Shepherd, Interim VP for Admin and Finance
6. Compliance, Ethics and Risk Management – Andrea Gandy, Risk Management Director, Christina Serra, Interim Chief Compliance Ethics and Risk
7. Accounts Payable & Procurement – Joel Levenson, Executive Director of Tax, Payables and Procurement
8. Accounting – Brad Hodum, Accounting Operations Interim Controller, Meghan Nelson, Assistant Controller
9. Budgeting – Dennis Crudele, Financial Statement Preparation Interim CFO, Donna DuBuc, University Budgeting Director
10. Information Security – Chris Vakhordjian, Assoc. VP & Chief Security Officer
11. Student Billing – Kelly D'Agostino, Bursar
12. Revenue – Alicia Keaton, Director of Financial Aid
13. Internal Audit – Robert Taft, Internal Audit
14. Board of Trustee – Robert Garvy, Representative