STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-075
December 2020

FLORIDA ATLANTIC UNIVERSITY

Workday® Enterprise Cloud Applications

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period February 2020 through May 2020, Dr. John W. Kelly served as President of Florida Atlantic University and the following individuals served as Members of the Board of Trustees:

Abdol Moabery, Chair	Brad Levine
Shaun Davis, Vice Chair	Mary Beth McDonald
Kevin Buchanan through 5-8-20 [a]	Elycia Morris
Brent Burns	Celine Persaud from 5-9-20 [a]
Dr. Michael Dennis through 5-6-20	Robert S. Rubin
Dr. Malcolm Dorman	Robert J. Stilley
Dr. Jeffrey P. Feingold	Dr. Kevin Wagner [b]

[a] Student Body President.
[b] Faculty Senate Chair.

The team leader was Sue Graham, CPA, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us or by telephone at (850) 412-2926.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

FLORIDA ATLANTIC UNIVERSITY

Workday® Enterprise Cloud Applications

SUMMARY

This operational audit of Florida Atlantic University (University) focused on selected information technology (IT) controls applicable to the Workday® Enterprise Cloud Applications (Workday®), and the contractual relationship with Workday, Inc. as the provider for the University's Workday® Software as a Service subscription. As summarized below, our audit disclosed an area in which improvements in University controls and operational processes are needed.

Finding 1: The University did not timely deactivate the IT user access privileges of certain former University employees.

Finding 2: University IT security controls related to account management and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of University data and IT resources.

BACKGROUND

The Florida Atlantic University (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) normally consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate Chair and Student Body President also serve as members.

While the BOG establishes the powers and duties of the Trustees, the Trustees are responsible for setting University policies, which are to provide governance in accordance with State law and BOG regulations. The Trustees select the University President, who is subject to confirmation by the BOG. The University President serves as the executive officer and the corporate secretary of the Trustees and is responsible for administering the University policies prescribed by the Trustees.

The University uses the Workday® Enterprise Cloud Applications (Workday®) for recording, processing, and reporting finance and human resources transactions. The University executed a Master Subscription Agreement (MSA) with Workday, Inc. on October 31, 2013, with an extended order effective April 30, 2018, for the subscription to Workday® using Software as a Service. Under the terms of the MSA, Workday, Inc. hosts the Workday® applications and maintains and manages the supporting information technology (IT) infrastructure.

FINDINGS AND RECOMMENDATIONS

Finding 1: Timely Deactivation of Information Technology User Access Privileges

Effective management of IT user access privileges includes the timely deactivation of employee IT access privileges when an employee separates from employment. Prompt action is necessary to ensure that the access privileges are not misused by former employees or others to compromise data or IT resources.

Business processes or a collection of tasks that are completed in a specific order are a core functionality within Workday® enabling changes to data through the configuration and maintenance of process flows. Initiation of a business process and routing of tasks through completion of the business process is dictated by an end-user's security role in the system. Each University department has the responsibility for notifying the Human Resources Department of employment separations by initiating the termination business process. The business process included the employee's effective date of separation, which was input as the employee's last working day or final pay date. Workday® accounts and assigned security groups were automatically deactivated through a business process task with the employee's effective date of separation recorded as the date of deactivation regardless of the actual date the task was completed. Notification to the applicable security administrators for deactivation of access privileges specific to other University applications occurred through additional tasks routed through the business process. In addition, a task notifying the security administrator within the Office of Information Technology occurred for the deactivation of access to the University's virtual private network, as applicable, and subsequent deactivation of assigned groups enabling user access to network resources and application platforms through an overnight batch job process.

Our evaluation of University procedures disclosed that the use of the termination business process did not always result in the timely communication of employee separations for processing and timely deactivation of employee access privileges. Specifically, our examination of University records supporting the termination business process for 727 employees during the period September 1, 2019, through March 27, 2020, disclosed that the access privileges for 337 employees, including 284 Other Personal Services (OPS) employees,[1] were not timely deactivated upon the employees' separation from University employment. Specifically, the termination business process was completed from 2 to 164 days, an average of 38 days, after the effective date of separation for the 284 OPS employees and from 2 to 54 days, an average of 8 days, after the effective date of separation for the 53 non-OPS employees.

According to University management, the termination business process for OPS employees and adjunct professors may be delayed up to a year to avoid repeating the onboarding process should the employee be rehired or reassigned to another department. However, the University had not established effective employment separation procedures to timely deactivate access privileges of OPS employees and adjunct professors who separate from University employment. Our examination of University records supporting 12 of the 53 non-OPS employees disclosed that initiation of the termination business process was delayed, for example, because staff untimely notified the responsible authority for the business process,

[1] The 284 OPS employees included 226 students.

misunderstood how to use the termination business process, were negotiating to keep the resigning employee, or were awaiting notification for the resigning employee's potential reassignment to another department.

Timely employment separation processing and deactivation of employee access privileges to University applications and network resources upon separation from employment reduces the risk that access privileges may be misused by the former employee or others.

Recommendation: University management should ensure that department use of the termination business process results in the prompt deactivation of employee access privileges when employees separate from University employment.

Finding 2: Security Controls – Account Management and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to account management and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of University data and related IT resources. However, we have notified appropriate University management of the specific issues.

Without appropriate security controls related to account management and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of University data and related IT resources may be compromised.

Recommendation: University management should improve IT security controls related to account management and logging and monitoring to ensure the confidentiality, integrity, and availability of University data and IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from February 2020 through May 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on selected significant University IT controls applicable to the Workday® Enterprise Cloud Applications (Workday®), and the contractual relationship with Workday, Inc. as the provider for the University's Workday® Software as a Service (SaaS) subscription during the period September 2019 through May 2020, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)[2] and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the Board and University Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that the internal control components significant to our audit objectives included control environment, control activities, and monitoring. The associated underlying principles significant to our objectives included:

- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the University's goals and objectives.

[2] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

- Management evaluation of employee performance and holding individuals accountable for their internal control responsibilities.
- Management design of control activities to achieve the University's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management activities to monitor the University's internal control system and evaluate the results.
- Management remediation of identified internal control deficiencies on a timely basis.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, University policies and procedures, and other guidelines, interviewed University personnel, and examined University records to obtain an understanding of University operations related to Workday® and to evaluate whether University operations were designed properly and operating effectively.
- To evaluate the sufficiency of University controls, observed, documented, and tested key processes, procedures, and controls related to the University's IT processes for Workday®, including authentication, logical controls, security management; the supporting University network infrastructure, including authentication, logical controls, logging and monitoring, and vulnerability management; and the SaaS subscription with Workday, Inc., including ensuring provision for

security, administration, and maintenance controls for Workday® and the supporting IT infrastructure.

- Examined the Master Subscription Agreement and Service Level Agreement between the University and Workday, Inc., effective October 31, 2013; extension agreement effective April 30, 2018; Service Organization Controls 1 Report for the period October 1, 2018, to March 31, 2019; Service Organization Controls 1 Report for the period April 1, 2019, to September 30, 2019; and Service Organization Controls 2 Report for the period October 1, 2018, to September 30, 2019, to determine the sufficiency of the University's assurance related to Workday, Inc.'s security and data management controls for the IT infrastructure supporting Workday®.
- Evaluated the effectiveness of logical access controls, including the periodic reviews of accounts assigned to the University root network domain and three child domains.
- Examined and evaluated the appropriateness of administrative access privileges for the University's network domains as of February 19, 2020.
- Evaluated selected security settings related to Workday® and the University's supporting network infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Examined selected scan reports, audit policies, logs, and documents to evaluate the adequacy of the University's controls for vulnerability management related to the network infrastructure supporting Workday®, including secure configurations, vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs.
- Examined selected business processes to evaluate the adequacy of the University's system documentation relating to Workday® to promote efficient and effective operations.
- Examined business processes, security groups and definitions, procedures for reviewing assigned security groups and changing business processes, and selected business process and security group assignment changes to determine the adequacy of University security management controls related to Workday®.
- Evaluated the membership assigned to the security administrator security group to determine the adequacy of University controls over the security administration function for Workday®.
- Examined and evaluated 11 of the 191 business processes defined by the University as of February 19, 2020, to determine whether the business process rules promote an appropriate separation of duties.
- Examined and evaluated the termination business process for 727 employees during the period September 1, 2019, through March 27, 2020, to determine whether the process was timely initiated and completed and employee access privileges were promptly deactivated upon each employee's separation from University employment.
- Evaluated the adequacy of the University's logging and monitoring controls over changes to the security and configuration of Workday®.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

FLORIDA ATLANTIC UNIVERSITY

Office of Information Technology
777 Glades Road
Boca Raton, FL 33431
Tel: 561.297.3440
Fax: 561.297.3945
http://www.fau.edu/oit

December 9, 2020

Sherrill F. Norman, CPA
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman,

Please see Florida Atlantic University's response to the State IT Audit results provided to us in November of 2020.

Finding #1

The University recognizes the challenges identified by this finding. In particular, the complexity of managing temporary employees, such as adjuncts and student employees (e.g., graduate assistants) who have regular gap periods in their employment, makes this a unique challenge for all universities. In response, FAU has established a working group to develop and recommend both technological and procedural changes to identify when a temporary employee is in a gap period or should be properly terminated. For employees in a gap period, a process to reduce access privileges will be developed. The working group will provide recommendations to the Assistant Vice President of Human Resources with a targeted implementation by the end of the current fiscal year. For all employees, we will create validations in Workday to prevent mistakes and maintain data integrity, conduct trainings for supervisors and HR business partners, monitor for late submissions through biweekly reports, and follow up with refresher trainings. These additional actions will also be completed by the end of the current fiscal year.

Finding #2

We concur with the finding. The Office of Information Technology has already completed the necessary corrective actions, and procedures have been altered to ensure centralized monitoring and management of all University domains.

Please feel free to reach out to us with any further clarifications to our responses.

Sincerely,

Jason Ball