STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-138
March 2019

UNIVERSITY OF FLORIDA

Oracle PeopleSoft Applications

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period April 2018 through September 2018, Dr. W. Kent Fuchs served as President of the University of Florida and the following individuals served as Members of the Board of Trustees:

Morteza “Mori” Hosseini, Chair	Rahul Patel
Thomas G. Kuntz, Vice Chair	Marsha D. Powers
James W. Heavener	Dr. Jason J. Rosenberg
David L. Brandon	Robert G. Stern
Ian M. Green [a]	Katherine Vogel Anderson [b] from 6-1-2018
Leonard H. Johnson	Anita G. Zucker
Daniel T. O’Keefe	David M. Quillen, MD [b] through 5-31-2018

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

The team leader was Vikki Mathews, 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

UNIVERSITY OF FLORIDA

Oracle PeopleSoft Applications

SUMMARY

This operational audit of the University of Florida (University) focused on evaluating selected information technology (IT) controls applicable to the Oracle PeopleSoft Applications (PeopleSoft Applications). As summarized below, our audit disclosed areas in which improvements in University controls and operational processes are needed.

Finding 1: University IT security controls related to user authentication, account management, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of University data and IT resources.

BACKGROUND

The University of Florida (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) 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 Faulty Senate Chair and Student Body President are also 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 polices prescribed by the Trustees.

The University uses Oracle PeopleSoft Applications (PeopleSoft Applications) for the University's finance, human resources, portal, and student financials applications. In addition, the University maintains and manages the IT infrastructure supporting PeopleSoft Applications, including application, Web, Integration Broker, batch and process scheduler, and database servers, and the database management systems.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Controls – User Authentication, 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 user authentication, 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 user authentication, 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: We recommend that University management improve certain security controls related to user authentication, 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 educational 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 April 2018 through September 2018 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 evaluating selected IT controls applicable to the University's PeopleSoft applications during the period April 2018 through August 2018 and selected actions subsequent thereto. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control 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.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; 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 and controls 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 the IT systems and 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 University 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:

- Interviewed University staff and reviewed University records to obtain an understanding of and evaluate University operations for the PeopleSoft Applications system architecture, including authentication, logical access controls, logging and monitoring, and vulnerability management for the supporting servers and database management systems infrastructure.
- Evaluated the effectiveness of logical access controls, including periodic review of accounts assigned to servers and databases supporting PeopleSoft Applications.
- Examined and evaluated the appropriateness of access privileges granted to:
    - 299 accounts assigned to each of the 6 virtual application servers as of April 20, 2018.
    - 296 accounts assigned to each of the 2 virtual application Integration Broker servers and 299 accounts assigned to each of the other 2 virtual application Integration Broker servers as of April 20, 2018.
    - 299 accounts assigned to each of the 2 virtual batch and process scheduler servers as of April 20, 2018.
    - 296 accounts assigned to each of the 2 virtual Web Integration Broker servers as of April 20, 2018.
    - 299 accounts assigned to each of the 4 virtual Web servers as of April 20, 2018.
    - 297 accounts assigned to each of the 6 virtual database servers as of May 14, 2018.
    - 5 accounts assigned to 11 physical servers as of May 16, 2018.
- Examined and evaluated the appropriateness of services enabled on the 24 virtual servers supporting PeopleSoft Applications. Specifically, we examined and evaluated:
    - 4 services on each of the 6 virtual application servers as of April 20, 2018.
    - 4 services on each of the 4 virtual application Integration Broker servers as of April 20, 2018.
    - 4 services on each of the 2 virtual batch and process scheduler servers as of April 20, 2018.
    - 4 services on each of the 2 virtual Web Integration Broker servers as of April 20, 2018.
    - 4 services on each of the 4 virtual Web servers as of April 20, 2018.
    - 4 services on each of the 6 virtual database servers as of May 14, 2018.

- Examined and evaluated the appropriateness of accounts and privileges granted to the finance, human resources (HR), portal, and student financials databases as of April 17, 2018. Specifically, we examined and evaluated:
  - 51 accounts assigned selected administrative privileges to the finance database.
  - 51 accounts assigned selected administrative privileges to the HR database.
  - 51 accounts assigned selected administrative privileges to the portal database.
  - 57 accounts assigned selected administrative privileges to the student financials database.
- Evaluated user authentication controls related to the University's IT infrastructure supporting PeopleSoft Applications.
- Evaluated the effectiveness of the University's logging and monitoring controls related to the IT infrastructure supporting PeopleSoft Applications.
- Evaluated controls for vulnerability management as it relates to the IT infrastructure supporting PeopleSoft Applications, including secure configurations, vulnerability assessment and remediation, maintenance, monitoring and analysis of audit logs, and malware defense.
- 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

UF UNIVERSITY of FLORIDA

Senior Vice President and Chief Operating Officer
Charles E. Lane

204 Tigert Hall
PO Box 113100
Gainesville, FL 32611-3100
352-392-9122
352-392-6278 Fax

February 19, 2019

Ms. Sherrill F. Norman, CPA
Auditor General, State of Florida
Suite G74, Claude Pepper
Building I 1 1 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Please find enclosed the University of Florida responses for the audit findings that are included in the University of Florida Oracle PeopleSoft Applications prepared by your office.

If you have any questions or require additional information, please contact Elias G. Eldayrie, Vice President and Chief Information Officer, at (352) 273-1788.

Sincerely,

Charlie Lane
Senior Vice President and COO

Copy to: Elias Eldayrie, Vice President and CIO
Joe Cannella, Interim Chief Audit Executive

Finding 1: Security Controls – User Authentication, Account Management, and Logging and Monitoring:

Recommendation: We recommend that University management improve certain security controls related to user authentication, account management, and logging and monitoring to ensure the confidentiality, integrity, and availability of University data and IT resources.

Management's Response: As recommended, the University will review and implement certain security controls related to user authentication, account management, and logging and monitoring.

Expected Implementation: October 15, 2019

Responsible Party: University of Florida Information Technology