STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2022-197
May 2022

ST. PETERSBURG COLLEGE

Oracle PeopleSoft Applications

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period November 2020 through October 2021, Dr. Tonjua Williams served as President of St. Petersburg College and the following individuals served as Members of the Board of Trustees:

Thomas Kidwell, Chair from 8-17-21, Vice Chair through 8-16-21
Jason Butts, Vice-Chair from 8-17-21
Katherine E. Cole, Chair through 8-16-21
Deveron M. Gibbons
Nathan M. Stonecipher

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

ST. PETERSBURG COLLEGE

Oracle PeopleSoft Applications

SUMMARY

This operational audit of St. Petersburg (College) focused on selected information technology (IT) controls applicable to St. Petersburg College Oracle PeopleSoft Applications (PeopleSoft Applications) system for maintaining and processing student account information and the infrastructure supporting College PeopleSoft Applications. Our operational audit disclosed the following:

Finding 1: College controls over application security management need improvement to ensure that access privileges to student information granted within PeopleSoft Applications are necessary and appropriate.

Finding 2: College IT security controls over user authentication, account management, logging and monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources.

BACKGROUND

St. Petersburg College (College) is under the general direction and control of the Florida Department of Education, Division of Florida Colleges, and is governed by State law and State Board of Education rules. A board of trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of five members appointed by the Governor and confirmed by the Senate. The College President serves as the Executive Officer and the Corporate Secretary of the Board and is responsible for the operation and administration of the College.

The College uses Oracle PeopleSoft Applications (PeopleSoft Applications) to record, process, and report finance and human resources transactions and student information. In addition, the College maintains and manages the network domain, application and database servers, and database management systems supporting PeopleSoft Applications.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Security Management

Effective application security management controls include resource owners identifying specific employees and authorizing the nature and extent to which those employees may access the resources where the owner has functional responsibility. Granting access to information technology (IT) resources based on a demonstrated need to view, change, or delete data and restricting individuals from performing incompatible functions or functions outside of their areas of responsibility is necessary to protect data and IT resources from unauthorized disclosure, modification, or destruction. In addition, documented periodic evaluations of access privileges associated with security groups help ensure that access privileges provided to each security group remain appropriate and necessary.

PeopleSoft Applications security is implemented through role assignment to an employee's user profile. Permission lists are created and assigned to each role and define the user's access privileges to a defined set of functions, pages, or fields that enable them to perform assigned job responsibilities. Security within the PeopleSoft Applications Campus Solutions module controls user access to view or modify system information related to student information such as student records, recruiting and admissions, and academic advising. Securing student records includes defining access privileges for functions including enrollment, student program and information, degrees and graduation, credit transfers, and transcripts. Enrollment functions are secured additionally through assignment of an access identification (ID) to the user. An enrollment access ID determines the time period when a user can perform certain enrollment functions and the type of overrides to which a user has access, including enrollment holds, requisite checking, class limits, drop period, and grade changes.

As part of our audit, we examined College records, inquired of College personnel, and found that documented periodic evaluations of application access privileges were made to financial aid roles, including roles with access to social security numbers. However, a comprehensive evaluation of all critical roles and access IDs assigned to employees, including the permission lists defined to the roles and the enrollment functions secured through the access IDs, had not been performed as of September 2021. In addition, we noted that the Manager of PeopleSoft Student Systems Development assigns roles to new and transferred employees based on information identified and approved as necessary for assigned job responsibilities. Notwithstanding, the Manager did not have the ability to view the defined permission lists for the roles assigned to employees or to view the defined enrollment functions for the access IDs assigned to employees to ensure that the access privileges granted within PeopleSoft Applications to view or modify student information aligned with employees' approved job responsibilities. Consequently, the Manager did not have an effective means to evaluate the appropriateness of access privileges prior to granting new roles or continuing existing roles and assigning access IDs to new or transferred employees.

Also, our examination of College records supporting the assigned access IDs as of September 2021 disclosed that 212 employees were assigned one of three access IDs that provided the ability to override or modify all or select enrollment functions, including the ability to make grade changes. To evaluate those ID assignments, we examined College records supporting 24 selected employees with ID assignments allowing grade changes and found that the ability to modify historical grades was inappropriate or unnecessary for 16 employees.[1]

In response to our inquiry, College management indicated that the Manager of PeopleSoft Student Systems Development would be provided additional security access related to permission lists and that a review of the enrollment function security was underway as of March 2022. Appropriately restricted access privileges help protect College data and IT resources from unauthorized modification, loss, and disclosure.

Recommendation: College management should enhance procedures to ensure that individuals are restricted from performing incompatible functions or functions outside their areas of responsibility. Such enhancements should include the performance of periodic comprehensive

[1] Employees with inappropriate or unnecessary access privileges included, for example, athletic coaches, a grants management coordinator, and a research specialist.

evaluations, on at least an annual basis, of access privileges granted to student information within PeopleSoft Applications, including evaluating access privileges granted to critical roles and access IDs, to verify that the privileges are necessary and appropriate for each user's assigned responsibilities.

Finding 2: Security Controls – User Authentication, Account Management, Logging and Monitoring, and Vulnerability Management

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, logging and monitoring, and vulnerability management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of College data and related IT resources. However, we have notified appropriate College management of the four findings in the areas needing improvement.

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

Recommendation: We recommend that College management improve IT security controls related to user authentication, account management, logging and monitoring, and vulnerability management to ensure the confidentiality, integrity, and availability of College 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 information technology (IT) operational audit from July 2021 through January 2022 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 significant St. Petersburg College (College) IT controls applicable to Oracle PeopleSoft Applications (PeopleSoft Applications) used for maintaining and processing student account information and the PeopleSoft Applications supporting infrastructure during the period November 2020 through October 2021, 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.

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, College procedures, and other guidelines; interviewed College personnel; and examined College records to obtain an understanding of College operations related to PeopleSoft Applications and to evaluate whether College operations were designed properly and operating effectively.
- Evaluated the sufficiency of College controls; observed, documented, and tested key processes, procedures, and controls related to the College's IT processes for PeopleSoft Applications infrastructure, including authentication, logical controls, vulnerability management, logging and monitoring of the network, application and database servers (servers), and the database management systems (databases), and PeopleSoft Applications Campus Solutions module, supporting server, database, and network device change management.
- Evaluated the effectiveness of College logical access controls assigned to the College network, servers, and databases supporting PeopleSoft Applications, including the periodic evaluation of assigned accounts.
- Evaluated the effectiveness of logical controls assigned within the PeopleSoft Applications Campus Solutions module, including College procedures related to the periodic evaluation of assigned user access privileges.

- Evaluated selected security settings related to PeopleSoft Applications and the supporting infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Evaluated College procedures and examined selected scan reports and policies to evaluate the adequacy of College vulnerability management controls related to the PeopleSoft Applications supporting IT infrastructure, including vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs and malware defense.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges within the four default network administrator system groups for the College root domain and one child domain as of August 17, 2021.
- Examined and evaluated the appropriateness of the five accounts assigned administrator access privileges for the selected College firewall as of September 21, 2021.
- Examined and evaluated, as of August 20, 2021, the 1,526 child domain accounts not required to have a password change.
- Examined and evaluated the appropriateness of access privileges granted on the 19 servers supporting PeopleSoft Applications. Specifically, as of September 29, 2021, we examined:
    - The 32 accounts on each of the 4 database servers supporting PeopleSoft Applications.
    - The 34 accounts on each of the 15 application servers supporting PeopleSoft Applications.
- Evaluated College procedures related to the recording, documenting, and reporting of changes to confidential and critical student record information within the PeopleSoft Applications Campus Solutions module to determine the adequacy of College logging and monitoring controls related to student information.
- Evaluated College procedures related to patches, upgrades, and changes to the PeopleSoft Applications supporting infrastructure, including system software and selected firewalls, to determine whether modifications required appropriate authorization, testing, and approval.
- Evaluated College procedures and selected College records related to PeopleSoft Applications Campus Solutions module upgrades and changes to determine whether modifications required appropriate authorization, testing, and approval.
- Evaluated College procedures and examined selected configuration settings for database and server logs to determine the adequacy of College logging and monitoring controls designed for the PeopleSoft Applications supporting infrastructure, including actions performed by privileged users.
- Evaluated College procedures and examined selected College records related to data recovery activities, prioritization, and security of backup data.
- Evaluated College procedures and examined selected College records related to managing the College's asset inventory and monitoring unauthorized network connections.
- Examined and evaluated the appropriateness of access privileges, as of September 27, 2021, granted within the PeopleSoft Applications Campus Solutions module for 24 of the 212 employees with access identification allowing the ability to modify historical grades.
- Examined and evaluated the appropriateness of the six accounts on each of the eight databases assigned selected administrative access privileges, as of August 18, 2021, to the database supporting PeopleSoft Applications.
- Examined and evaluated, as of August 18, 2021, the appropriateness of the 4 accounts with default passwords defined to one or more of the eight databases supporting PeopleSoft Applications.

- 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

St. Petersburg College
SPC

May 5, 2022

Sherrill F. Norman, CPA
Auditor General
State of Florida
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450
EMAIL: flaudgen_audrpt_ita@aud.state.fl.us

RE: St. Petersburg College Information Technology Operational Audit

Please see the following statement of explanation concerning all preliminary and tentative audit findings, including actual or proposed corrective actions.

Finding 1: College controls over application security management need improvement to ensure that access privileges to student information granted within PeopleSoft Applications are necessary and appropriate.

Upholding the security of student information and maintaining the integrity of our student-related data is of utmost importance to St. Petersburg College (SPC). SPC will evaluate all critical roles and access assigned to employees that utilize the PeopleSoft Student system, including the permission lists defined to the roles and enrollment functions secured through those access controls. At the time of the audit, the college used three distinct access IDs that control the ability to modify or select PeopleSoft enrollment functions. All three of these access IDs include the capacity to make historical grade changes. During the audit period the number of IDs were increased.

Corrective action regarding this finding has been taken. The number of access ID's have been increased from three to four access ID's. The new access ID does not include the capacity to make historical grade changes. This new access ID was assigned to the users who do not need to make historical grade changes and the users original access ID was deleted.

Additional proposed corrective actions include the following enhancements. St. Petersburg College will perform a more comprehensive review of the manager's access to roles and enhance and formalize the business process and procedures related to issues of performance of incompatible functions or functions outside employee's area of responsibility. The college will perform periodic evaluations, on at least an annual basis, of access privileges granted to student information within PeopleSoft Applications, including evaluating access privileges granted to critical roles and access IDs.

St. Petersburg College

SPC

Finding 2: College IT security controls over user authentication, account management, logging and monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of college data and IT resources.

St. Petersburg College recognizes the importance of continuous improvement to IT security controls related to user authentication, account management, logging and monitoring and vulnerability management as part of the colleges overall IT Security program. The college primarily uses National Institute of Standards and Technology (NIST) guidelines as the framework that governs these controls.

Corrective actions taken and proposed actions include establishing a detailed remediation plan to improve IT security controls related to user authentication, account management, logging and monitoring, and vulnerability management. The plan will include procurement and implementation of necessary tools or services to ensure success of the remediation plan and will enhance the confidentiality, integrity, and availability of college data and IT resources.

Respectfully,

Tonjua Williams

Tonjua Williams, Ph.D.
President
St. Petersburg College

Mailing Address: Post Office Box 13489, St. Petersburg, FL 33733-3489