

**SEMINOLE COUNTY DISTRICT SCHOOL
BOARD**

Oracle PeopleSoft Applications and Skyward
Student Information System



Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the 2022-23 fiscal year, Serita D. Beamon served as Superintendent of the Seminole County Schools and the following individuals served as School Board Members:

	<u>District No.</u>
Kristine Kraus, Chair from 11-22-22	1
Kelley Davis from 11-22-22	2
Karen Almond through 11-21-22	2
Abby Sanchez, Vice Chair	3
Amy Pennock, Chair through 11-21-22	4
Autumn Garick from 11-22-22	5
Dr. Tina Calderone through 11-21-22	5

The team leader was Ellen Henley, 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 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

SEMINOLE COUNTY DISTRICT SCHOOL BOARD

Oracle PeopleSoft Applications and Skyward Student Information System

SUMMARY

This operational audit of Seminole County School District (District) focused on evaluating selected information technology (IT) controls applicable to Oracle PeopleSoft Applications, the Skyward Student Information System (Skyward), and District IT infrastructure, and included a follow-up on findings noted in our report No. 2020-039. Our audit disclosed the following:

Finding 1: District security awareness training needed improvement to reduce the risk of compromise to District data.

Finding 2: District controls over granting access privileges to Skyward could be improved.

Finding 3: District IT security controls related to user authentication, account management, monitoring, vulnerability management, and configuration management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The Seminole County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education and is governed by State law and State Board of Education rules. Geographic boundaries of the District correspond with those of Seminole County. The governing body of the District is the Seminole County District School Board (Board), which is comprised of five elected members. The appointed Superintendent of Schools is the Executive Officer of the Board. During the 2022-23 fiscal year, the District operated 65 elementary, middle, high, and specialized schools; sponsored 6 charter schools; and reported 68,198 unweighted full-time equivalent students.

The District uses Oracle PeopleSoft Applications (PeopleSoft) to process and report financial and human resources information and the Skyward Student Information System (Skyward) to process and report student information. In addition, the District maintains and manages the network domain, application and database servers, and database management systems supporting PeopleSoft and Skyward.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Awareness Training

A comprehensive security awareness training program instructing all employees on the importance of preserving the confidentiality, integrity, and availability of data and information technology (IT) resources entrusted to them is a foundational control for security vigilance and preventing and mitigating cybersecurity risks. An effective security awareness program includes identification of the specific knowledge, skills, and abilities needed to support District security and educates all employees about how to interact with data and IT resources in a secure manner.

As part of our audit, we examined District procedures, management directives, and related records supporting employee security awareness and skills training during the 2022-23 fiscal year. We found that the District provided training on various security topics, including social engineering, authentication, and data handling, and that security incident response was available to employees through District and vendor-provided solutions. However, the training was not mandatory or monitored for completion and, consequently, a comprehensive, mandatory security awareness training program had not been established. Subsequent to our inquiry, District management established a comprehensive, mandatory security awareness training course through the District learning management system and, according to District management, all staff had completed training by October 2023.

A comprehensive security awareness training program educates employees about data security and reduces the risk that the confidentiality, availability, and integrity of District data and IT resources will be compromised.

Recommendation: To help mitigate cybersecurity risks, District management should continue to implement a comprehensive, mandatory security awareness training program that educates District employees about their responsibilities and the importance of securing District data and IT resources.

Finding 2: Application Security Management

Effective application security management controls ensure that resource owners authorize the nature and extent to which employees access resources under their functional responsibility. Granting access to IT resources based on a demonstrated need to view, change, or delete data and restricting employees from performing incompatible functions or functions beyond their areas of responsibility is necessary to protect data and IT resources from unauthorized disclosure, modification, or destruction. In addition, periodic evaluations of access privileges associated with security groups help ensure that access privileges provided to each security group remain appropriate and necessary.

IT access privileges within the Skyward Student Information System (Skyward) are controlled by assigning groups to employees. District personnel create groups and include menus with defined permissions to view or edit specific screens and fields. Groups are defined at the District level and at the school level allowing employees assigned access privileges across the District or at one or more school levels. Security groups are further assigned access values that determine the type of access allowed such as view, add, and change.

Our inquiries of District management, school administrators, and other District personnel, along with our evaluation of Skyward access records and procedures, disclosed that District controls over Skyward access privileges need improvement. Specifically:

- Generally, at the request of a teacher and approval from a school principal or assistant principal, designated school staff (e.g., the full-time equivalent clerk) make historical student grade changes.¹ As part of our audit, we selected 11 of the 65 District schools and evaluated the access privileges, as of June 29, 2023, assigned at those schools to one or more of the security groups allowing changes to historical student grades. We found that:

¹ A teacher requested grade change may be based on a student's submittal of a late assignment. District administrative staff may change historical grades based on end-of-course assessment grades.

- Security groups were not defined to disclose what a user had the ability to do or to enable principals to understand the access they granted.
- District procedures had not been established for requesting and approving access removal for staff who no longer needed the access.
- District personnel did not perform periodic evaluations of access privileges because a report identifying assigned security groups and the access privileges granted through the assigned groups was not readily available.

As a result, access authorization forms did not identify the access privileges that were granted and several personnel, including administrators, counselors, secretaries, and an audiologist, had unnecessary access privileges to update historical student grades.

- As of June 29, 2023, 15 District administrative employees had Districtwide access to change historical student grades and 1 administrative employee had access to change historical student grades for several schools. Our examination of District records supporting the access privileges of 8 selected employees disclosed that 7 employees² had unnecessary access to change historical student grades. One employee had retained the security group allowing the access to change grades from a previous position and another employee retained the security group allowing access after assisting with end-of-course assessment grade updates. Although the other employees had responsibilities over certain District or student record information, including staffing and course enrollment, scheduling, transcripts, and immunization and injury records, the security groups assigned provided the ability to change historical student grades, which was unnecessary for their responsibilities.
- We selected 48 employees from the 666 employees with access to a selected group,³ as of July 12, 2023, and found that 29 of the 48 employees had unnecessary access to view some or all of the District-defined confidential and critical student information granted through the group. District management stated that, although some access was unnecessary, the additional access privileges granted by the group supported the employees' job duties and that the District intends to explore the availability of additional restrictions for accessing attendance, discipline, health, and grade information.

In response to our inquiry, District management indicated that the security groups were initially created using vendor-provided employee roles that were no longer applicable to District operations and the ability to create more granular access according to employee responsibilities would be evaluated. Additionally, District management will evaluate solutions for completion of periodic access evaluations.

Appropriately restricted access privileges help protect District data and IT resources from unauthorized modification, loss, and disclosure. A similar finding was noted in our audit report No. 2020-039.

Recommendation: District management should appropriately define security groups to disclose what a user has the ability to do and enable principals to understand the access they grant. In addition, the District should establish procedures for requesting and approving access removal for staff who no longer need the access. The District should also establish procedures requiring periodic evaluation of access privileges granted within Skyward and ensure that the access privileges granted are necessary and appropriate for the employee's assigned responsibilities.

² Employees with unnecessary access to update student grades included the Director of Staffing and State Reporting, Administrator of Data Quality and Compliance, Information Services Project Manager, and a lead payroll specialist, accounts payable specialist, records specialist, and risk management specialist.

³ The group selected was assigned to employees at the District level or at 1 or more of 3 selected schools and allowed view access to student attendance, discipline, health, and grade information.

Finding 3: Security Controls - User Authentication, Account Management, Monitoring, Vulnerability Management, and Configuration Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain security controls related to user authentication, account management, monitoring, vulnerability management, and configuration management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of District data and related IT resources. However, we have notified appropriate District management of the five findings in the areas needing improvement. Similar findings related to user authentication, account management, and monitoring were noted in our report No. 2020-039.

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

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

PRIOR AUDIT FOLLOW-UP

The District had taken corrective action for the findings included in our report No. 2020-039 except that Findings 2 and 3 also were noted as Findings 1 and 3 in that report.

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 April 2023 through September 2023 in accordance with generally accepted government auditing standards. Those standards require 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 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 IT controls applicable to the Oracle PeopleSoft Applications (PeopleSoft), Skyward Student Information System (Skyward), and District IT infrastructure during the period July 2022 through June 2023 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 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 determine whether management has corrected, or is in the process of correcting, all deficiencies disclosed in our report No. 2020-039.
- 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; 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 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, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, and other guidelines to obtain an understanding of District organizational structure and regulatory requirements; reviewed District procedures, interviewed District personnel, and examined District records to obtain an understanding of District operations related to PeopleSoft, Skyward, and IT infrastructure and to evaluate whether District operations were designed properly and operating effectively.
- Evaluated the sufficiency of District controls; observed, documented, and tested key processes, procedures, and controls related to PeopleSoft and Skyward and the District IT infrastructure, including authentication, backup and recovery, configuration of systems, logical controls, and inventory and vulnerability management.
- Examined selected security settings related to the District network infrastructure, externally facing applications, remote access systems, and other critical servers and devices to determine whether

authentication controls were configured and enforced in accordance with IT best practices, including the use of multi-factor authentication.

- Evaluated the effectiveness of District logical access controls assigned to the District network and selected network devices, including the periodic evaluation of assigned accounts.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of April 10, 2023, within the four default network administrator system groups for the District network domains.
- Examined and evaluated the appropriateness of administrative access privileges, as of June 14, 2023, to the 2 critical servers supporting PeopleSoft and 7 of the 11 critical servers supporting Skyward.
- Examined and evaluated, as of July 28, 2023, the 90 accounts on 1 child domain not required to have a password change.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of April 10, 2023, for the four District high-risk network devices.
- Examined and evaluated selected District patch management controls for operating systems and network devices to ensure secure configurations are maintained. Specifically, we examined and evaluated the patch management controls for:
 - The 16 critical servers supporting the District network, PeopleSoft, and Skyward as of May 30, 2023.
 - The 4 high-risk network devices as of April 12, 2023.
- Examined and evaluated Board policies and District procedures for mobile device management, including maintaining an inventory, enforcing security requirements, and responding to loss of devices.
- Examined and evaluated the appropriateness of accounts assigned, as of April 7, 2023, on the finance and human resources (HR) databases supporting PeopleSoft for management and administration of the databases. Specifically, we examined and evaluated:
 - 13 accounts assigned selected administrative privileges on the finance database.
 - 13 accounts assigned selected administrative privileges on the HR database.
- Evaluated the effectiveness of logical controls assigned within Skyward, including periodic evaluations of access privileges.
- Examined and evaluated the appropriateness for 8 of 16 District administrative employees having the ability to update historical student grades as of June 29, 2023.
- Examined and evaluated the appropriateness of access privileges, as of July 12, 2023, granted within Skyward for 48 employees.
- Evaluated District controls in place for the use of systemwide access privileges.
- Evaluated the effectiveness of the District's logging and monitoring controls, including actions performed by privileged users for the databases supporting PeopleSoft.
- Evaluated the effectiveness of District logging and monitoring controls related to student information within Skyward.
- Evaluated District procedures and examined selected records to determine the adequacy of District procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.

- Evaluated the effectiveness of District configuration management controls, including establishing and maintaining secure configurations; disabling insecure protocols; implementing firewalls or port filtering to protect network resources; and timely applying software updates and managing device end-of-life.
- Evaluated District procedures and examined selected scan reports and policies to evaluate the adequacy of District vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- Evaluated District procedures and examined selected backup reports to determine the adequacy of the District data recovery procedures to restore District IT assets to a pre-incident trusted state.
- Evaluated the effectiveness of the District security awareness training program.
- 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 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 this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



SERITA BEAMON
Superintendent

Educational Support Center
400 E. Lake Mary Boulevard
Sanford, Florida 32773-7127
Phone: (407) 320-0000
Fax: (407) 320-0281

Visit Our Web Site
www.scps.us

December 18, 2023

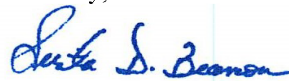
Sherrill F. Norman, CPA
Auditor General
State of Florida
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Re: Response to Information Technology Operational Audit Findings

Dear Ms. Norman:

Attached are our responses to the findings in the I.T. operational audit completed by your office. Although audits bring about additional requirements in an already thinly resourced organization, they do provide an opportunity for us to examine our I.T. practices and protocol for opportunities to improve how we manage our vast technology systems. I want to compliment your staff for their thorough work and professional demeanor.

Sincerely,



Serita Beamon

cc: Kristine Kraus, Board Chair at the time of the Audit

Ulysses Vazquez, Chief Technology Officer
Thomas Condo, Supervisor Information Services Operations

IT Operational Controls Audit

SBSC Response to PNT Findings

Finding 1:

District security awareness training needed improvement to reduce the risk of compromise to District data.

Recommendation:

To help mitigate cybersecurity risks, District management should continue to implement a comprehensive, mandatory security awareness training program that educates District employees about their responsibilities and the importance of securing District data and IT resources.

Response:

SBSC (School Board of Seminole County) management implemented a comprehensive security awareness training program on **July 1, 2023**. A "Cybersecurity Basics" training is now mandated through the Canvas LMS (Learning Management System). The course covers the District's AUP (Acceptable Use Policy), password security, password safety, email security, phishing, smishing, internet safety, malware, and social media security. Participants are required to take a quiz at the end of the training and receive a passing grade. Once successful, participants receive one service-hour within the District's professional development system. Training is mandated by the Human Resources department for all staff as part of annual training coursework (Cybersecurity Awareness, Child Abuse, Title IX, and Student Mental Health Awareness), and has a deadline of **October 2**. Course participation is tracked via Microsoft Power-BI analytics. Staff receive bi-weekly email reminders about any unmet training. The frequency of reminders increases as the training deadline nears, and notifications are also sent to the employee's immediate supervisor. Evidence of Cybersecurity Basics course completion by SBSC staff for the 2023-24 school year was sent to the State AG audit team on **November 3, 2023**. SBSC will mandate a new Cybersecurity training course for District Leadership during the 2024-25 school year. This will reduce cybersecurity risks and satisfy **1012.585(3)(g) F.S.** renewal requirements for professional certificates containing *Educational Leadership or School Principal*, as established in **Rule 6A-5.080 F.A.C.**

Finding 2:

District controls over granting access privileges to Skyward could be improved.

Recommendation:

District management should appropriately define security groups to disclose what a user can do and enable principals to understand the access they grant. In addition, the District should establish procedures for requesting and approving access removal for staff who no longer need access. The District should also establish procedures requiring periodic evaluation of access privileges granted within Skyward and ensure that the access privileges granted are necessary and appropriate for the employee's assigned responsibilities.

IT Operational Controls Audit SBSC Response to PNT Findings

Response:

SBSC will implement an outward facing security group description document to better inform site supervisors (AKA School Principals) on security group functions. SBSC currently removes security access when employees change job sites. However, we will explore options for when employees change roles within their current site. SBSC will also explore options for site administrators, where feasible, to conduct periodic evaluation of employee Skyward access, notifying district personnel of any needed changes.

Finding 3:

District IT security controls related to user authentication, account management, monitoring, vulnerability management, and configuration management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

Recommendation:

We recommend that District management improve IT security controls related to user authentication, account management, monitoring, vulnerability management, and configuration management to ensure the confidentiality, integrity, and availability of District data and IT resources.

Response:

As recommended, SBSC has put measures in place to improve IT security controls related to monitoring, vulnerability management, and configuration management. SBSC is currently in the process of addressing concerns raised around user authentication and account management.