STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-024
October 2017

LAKE COUNTY
DISTRICT SCHOOL BOARD

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period February 2017 through May 2017, Dr. Susan E. Moxley served as Superintendent to March 10, 2017, Diane Kornegay served as Superintendent from March 11, 2017, and the following individuals served as Board members:

	District No.
Bill Mathias	1
Kristi Burns, Ph.D.	2
Marc Dodd, Chairman	3
Sandy Gamble	4
Stephanie Luke, Vice Chairperson	5

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 Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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

LAKE COUNTY DISTRICT SCHOOL BOARD

SUMMARY

This operational audit of the Lake County School District (District) focused on evaluating selected information technology (IT) controls applicable to the Skyward school business suite software (Skyward business) and student management suite software (Skyward student). As summarized below, the audit disclosed areas in which improvements in District controls and operational processes were needed.

Finding 1: Skyward business and Skyward student applications change management controls need improvement to ensure that changes are appropriately tested and accepted.

Finding 2: Some inappropriate access privileges to Skyward business and Skyward student applications existed within the District.

Finding 3: Certain District security controls related to user authentication, user account management, and data change control needed improvement to ensure the confidentiality, integrity, and availability of District data and related IT resources.

BACKGROUND

The Lake County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education. The governing body of the District is the Lake County District School Board (Board), which is composed of five elected members. The Superintendent of Schools is the executive officer of the Board.

The District uses the Skyward school business suite software (Skyward business) and student management suite software (Skyward student) to process and report its finance, human resources, and student transactions. In addition, the District maintains and manages the supporting infrastructure (i.e., network domains, operating systems, and database management systems) for the Skyward business and Skyward student installations.

FINDINGS AND RECOMMENDATIONS

Finding 1: Change Management

Effective change management controls over vendor-provided application changes ensure that changes are appropriately tested and function as intended prior to being implemented into the production environment. Further, the effectiveness of change management controls is enhanced through user acceptance of vendor-provided application changes (i.e., user acknowledgement and understanding of the changes).

The Skyward vendor periodically provided the District addendums and Required Maintenance Addendums (RMAs) to apply to the District's Skyward business or Skyward student applications. Addendums are application changes initiated by Skyward and RMAs are corrections to issues identified by either Skyward or Skyward clients. Although the District's Manager of Information and Operations

Services and Database Administrator were responsible for implementing the addendums and RMAs, District management had not established procedures for testing the changes prior to implementation. In addition, although information related to the Skyward business application changes was made available to users, information related to the Skyward student application changes was not made available to users. Consequently, the District did not obtain user acceptance of the Skyward student application changes.

Effective change management controls reduce the risk that vendor-provided application changes may be implemented into the production environment without appropriate testing and user acknowledgement and understanding of the changes.

Recommendation: We recommend that District management establish procedures for testing application changes provided by Skyward and for user acceptance of Skyward student application changes.

Finding 2: Access Privileges

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls include granting employees access to IT resources based on a demonstrated need to view, change, or delete data and restricting employees from performing incompatible functions or functions outside of their areas of responsibility.

Our review of selected access privileges to the Skyward business and Skyward student applications disclosed that the District's Manager of Information and Operations Services, Database Administrator, Digital Content Systems Architect, and a Student Information Systems Specialist had systemwide access privileges to the Skyward business application. Additionally, the Manager of Information and Operations Services, Database Administrator, and Digital Content Systems Architect had systemwide access privileges to the Skyward student application. Systemwide access privileges allow update access to all functions within the business and student applications, including transaction origination, correction, and changes to finance, payroll, and student data and security tables.

In response to our inquiry, District management indicated that systemwide access is used for administration and support, including installing updates and running certain utilities, of the Skyward business and Skyward student applications. Nevertheless, complete update access privileges to the applications were not necessary for each of these employees' day-to-day responsibilities and were contrary to an appropriate separation of end-user and technical support functions. Appropriately restricted access privileges help protect District data and IT resources from unauthorized modification, loss, or disclosure.

Recommendation: We recommend that District management restrict systemwide access privileges to one designated account for each Skyward application and that the account granted these privileges be used only as needed for its defined business purpose and be appropriately monitored.

Finding 3: Security Controls – User Authentication, User Account Management, and Data Change Control

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

Without adequate security controls related to user authentication, user account management, and data change control, the confidentiality, integrity, and availability of District data and IT resources may be compromised, increasing the risk that District data and IT resources may be subject to improper disclosure, modification, and destruction.

Recommendation: We recommend that District management improve IT security controls related to user authentication, user account management, and data change control to ensure the continued confidentiality, integrity, and availability of District 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 2017 through May 2017 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 operational audit focused on evaluating selected IT controls applicable to the Skyward school business suite software (Skyward business) and student management suite software (Skyward student) during the period February 2017 through May 2017. 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 District management and staff and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed District personnel and reviewed operational documentation to obtain an understanding of:
    - The District's IT infrastructure and network architecture for Skyward business and Skyward student.
    - Authentication to the District's IT infrastructure, including selected hardware, operating systems, and database management systems related to Skyward business and Skyward student.
    - Logical design, administration, and periodic review procedures for logical access privileges granted to selected District IT resources and data.
    - Systems software and network infrastructure component change control procedures and processes.
    - Change management controls related to Skyward business and Skyward student and supporting databases.
    - Circumstances that necessitate the granting and use of systemwide access to Skyward business and Skyward student.
- Examined and evaluated the appropriateness of administrative access privileges granted as of February 10, 2017, for one of the District's three network domains and granted as of March 3, 2017, for another one of the District's three network domains.
- Examined and evaluated the appropriateness of administrative access privileges to the two Web servers and two database servers that support Skyward business and Skyward student as of March 3, 2017.

- Evaluated the effectiveness of logical access controls, including periodic reviews of access privileges assigned for the servers, network domains, and databases that support Skyward business and Skyward student.
- Evaluated authentication controls implemented to protect IT resources and data, including servers, network domains, databases, and remote log-on services that support Skyward business and Skyward student.
- Evaluated District controls in place for the use of systemwide access privileges.
- Evaluated the effectiveness of District change management controls related to the authorization, testing, and approval of Skyward application data changes prior to implementation into the production environment. Specifically, we examined three of the five data changes for Skyward business logged between July 1, 2016, and February 9, 2017, and all four data changes logged for Skyward student between November 2, 2016, and February 9, 2017.
- Evaluated the logging and monitoring controls, including actions performed by privileged users, for the servers, network domains, and databases that support Skyward business and Skyward student.
- 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

LAKE COUNTY SCHOOLS

201 West Burleigh Boulevard · Tavares · FL 32778-2496
(352) 253-6500 · Fax: (352) 253-6503 · www.lake.k12.fl.us

Superintendent:
Diane S. Kornegay, M.Ed.

School Board Members:
District 1
Bill Mathias
District 2
Kristi Burns, Ph.D.
District 3
Marc Dodd
District 4
Sandy Gamble
District 5
Stephanie Luke

October 5, 2017

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

Dear Ms. Norman,
We are pleased to respond to the preliminary and tentative audit finding and recommendations concerning the Office of Auditor General's information technology operational audit of the Lake County District School Board dated July 31, 2017. Our response to the findings are listed below:
Finding Number 1: Change Management
Recommendation: We recommend that the District management establish procedures for testing application changes provided by Skyward and for user acceptance of Skyward student application changes.
Response: Lake County District School Board agrees and has taken corrective action to improve change management controls and processes.
Finding Number 2: Access Privileges
Recommendation: We recommend that District management restrict system wide access privileges to one designated account for each Skyward application and that the account granted these privileges be used only as needed for its defined business purposes and be appropriately monitored.
Response: Lake County District School Board agrees. The support level we currently provide Skyward Business and Student users requires certain individuals to utilize system access privileges on a daily or weekly basis. We do understand the need to minimize system-wide access and will work toward minimizing the need for system-wide access.
Finding Number 3: Security Controls – User Authentication, User Account Management, and Data Change Control
Recommendation: We recommend that the District management improve IT security controls related to user authentication, user account management, and data change control to ensure continued confidentiality, integrity, and availability of District data and IT resources.
Response: Lake County District School board agrees and has taken corrective action to improve IT security controls related to user authentication, user account management, and data change control.
If you have any questions regarding this information, Please feel free to contact us at (352) 253-6500.

Sincerely,

Diane S. Kornegay
Superintendent
Lake County District School Board