STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-027
November 2017

LEON COUNTY
DISTRICT SCHOOL BOARD

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period May 2017 through August 2017, Rocky Hanna served as Superintendent and the following individuals served as Board members:

	District No.
Alva Striplin, Vice Chair	1
Rosanne Wood	2
Maggie Lewis-Butler	3
DeeDee Rasmussen	4
Georgia "Joy" Bowen, Chair	5

The team leader was Sudeshna Aich, 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

LEON COUNTY DISTRICT SCHOOL BOARD

SUMMARY

This operational audit of the Leon County School District (District) focused on evaluating selected District information technology (IT) controls applicable to the Skyward school business suite software (Skyward), including the contractual relationship with Integrated Systems Corporation as the application service provider for the District's Skyward installation. As summarized below, the audit disclosed areas in which improvements in District controls and operational processes were needed.

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

BACKGROUND

The Leon County School District (District) is part of the State system of public education under the general direction of the Department of Education. The governing body of the District is the Leon 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) for its finance and human resources transactions. Skyward is the District's Enterprise Resource Planning system for financial and human resources management. The District signed a Hosted Software License Agreement (Agreement) with Integrated Systems Corporation (ISCorp) on March 22, 2011, for server and application hosting, management, and operations services related to Skyward. The Agreement's term includes the initial effective period of 3 years and additional renewal periods. The Agreement was last renewed on April 25, 2017, for a period of 3 years.

FINDING AND RECOMMENDATION

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

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, logging, and security management 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, logging, and security management 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, logging, and security management 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 May 2017 through August 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, during the period May 2017 through August 2017, selected District IT controls applicable to Skyward, including the contractual relationship with ISCorp as the application service provider for the District's Skyward installation. 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 documentation applicable to District and ISCorp operations to obtain an understanding of:
  - The delineation of responsibilities between the District and ISCorp for the administration, support, and maintenance of Skyward and the supporting IT infrastructure.
  - IT infrastructure supporting the District's Skyward installation, including the network, operating systems, and database management system.
  - Authentication to Skyward and the database management system.
  - Circumstances which necessitate the granting and use of Systemwide access to Skyward.
  - Active Directory architecture and the domains supporting authentication to Skyward.
  - Change management controls related to the District's network operating system and network infrastructure devices.
- Evaluated the effectiveness of logical access controls, including periodic reviews for the network domains, servers, and database management system that support Skyward.
- Examined and evaluated the appropriateness of administrative access privileges for the District's network domains which include the user accounts as of May 4, 2017, for District staff accessing Skyward.
- Examined and evaluated the appropriateness of user accounts granted administrative access privileges to the database as of June 26, 2017.
- Evaluated the effectiveness of District security management controls for ensuring the adequacy of activities performed by ISCorp related to data management and security.
- Evaluated the effectiveness of District change management controls related to the authorization, testing, and approval of Skyward application data changes prior to implementation into production environment. Specifically, we examined two of the four data changes for Skyward logged between July 1, 2016, and June 27, 2017.
- Evaluated user authentication controls implemented for authentication to the District's network domains, Skyward, and the database management system.
- Evaluated logging and monitoring controls over system activity, including network security events and actions performed by privileged users.
- Evaluated District vulnerability management controls for network system software and infrastructure devices.
- 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

October 24, 2017

Ms. Sherill F. Norman
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Attached is the official written response to the preliminary and tentative audit findings resulting from the operational audit of the Leon County School District information technology (IT) controls applicable to the Skyward school business suite software (Skyward) including the contractual relationship with Integrated Systems Corporation.

We value the information provided during the audit process. District staff has thoroughly reviewed each of the findings and has either fully implemented corrective action or developed a plan to fully implemented appropriate corrective actions in the near future.

We thank you for the opportunity to respond to the audit finding. If additional information is required, please feel free to contact us.

Sincerely,

Rocky Hanna

Rocky Hanna

Enclosure
cc: Livetra Paul, Director of Internal Audit
Bill Nimmons, Executive Director, Technology and Information Services
Gillian Gregory, Assistant Superintendent Academic Services

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

User Authentication - The District has a plan in place to ensure that all users meet the requirements stated in the finding by December 31, 2017

Logging – The District implemented the recommended changes and will continue to monitor the logs as indicated in the finding.

Security Management – The District received an updated Data Security Agreement from the hosting vendor. Additionally, the District has requested a copy of the AICPA SOC 2 audit upon completion. District staff will review that audit to determine future contract negotiation points with the vendor. Further, the District has purchased data breach insurance which became effective this year.