STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-147
March 2021

CLAY COUNTY DISTRICT SCHOOL BOARD

Network and Operational Controls

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period September 2019 through July 2020, Mr. David Broskie served as Superintendent of the Clay County Schools and the following individuals served as School Board Members:

	District No.
Janice A. Kerekes, Vice Chair through 11-6-19	1
Carol Y. Studdard, Chair	2
Tina Bullock	3
Mary Bolla, Vice Chair from 11-7-19	4
Ashley Gilhousen	5

The team leader was Joseph D. Garcia, 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

CLAY COUNTY DISTRICT SCHOOL BOARD

Network and Operational Controls

SUMMARY

This operational audit of the Clay County School District (District) focused on evaluating selected information technology (IT) controls applicable to the District network and related operations. Our audit disclosed the following:

Finding 1: The District did not maintain a comprehensive inventory of IT resources, increasing the risk that unauthorized devices may connect to the District network without timely detection and security and other critical updates may not be timely implemented.

Finding 2: The District had not established a comprehensive, mandatory security awareness training program, increasing the risk for District data to be compromised.

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

BACKGROUND

The Clay 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 Clay County. The governing body of the District is the Clay County District School Board (Board), which is composed of five elected members. The elected Superintendent of Schools is the Executive Officer of the Board. During the 2019-20 fiscal year, the District operated 50 schools and centers, sponsored 3 charter schools, and reported 43,677 unweighted full-time equivalent students.

The District depends on the reliable function and security of critical network infrastructure for the storage and transmission of data in support of District operations. Network and operational controls serve to mitigate risks from known and emerging Internet security threats to the confidentiality, integrity, and availability of District data and IT resources.

FINDINGS AND RECOMMENDATIONS

Finding 1: Inventory of IT Resources

Effective inventory controls include the maintenance of a complete, accurate, and up-to-date inventory of information technology (IT) resources (e.g., computers, servers, network devices) to ensure that management is knowledgeable of all IT systems for which they are responsible and that the IT systems are secured and configured as intended by management. Further, a complete, accurate, and up-to-date inventory is necessary for the identification and remediation of unauthorized devices connected to the

network and for effective monitoring, testing, and evaluation of IT resources to ensure the timely implementation of security and other critical updates (e.g., anti-malware software).

According to District personnel, the District did not maintain a comprehensive inventory of all IT resources able and authorized to store and process information on the District network. As of July 2020, the District utilized Apple, Google, and Windows computers and network devices such as switches and routers in their operations. Although District management used software to scan the network for connected computers, only active Windows computers assigned to the District network were inventoried. Additional software was similarly used to scan other network devices that were active on the District network. However, an inventory of those devices had not been compiled as a baseline of authorized network devices.

In response to our inquiry, District management indicated that the District did not establish and maintain a comprehensive inventory of all IT resources because of the impact of the COVID-19 pandemic, insufficient time and staff resources, and changes in IT management. Maintenance of a comprehensive inventory of all IT resources is necessary to properly account for IT resources, facilitates the identification and remediation of unauthorized devices connected to the network, and ensures the timely implementation of security and other critical updates.

Recommendation: District management should establish and maintain a comprehensive inventory of all District-authorized IT resources.

Finding 2: Security Awareness Training

A comprehensive security awareness training program apprises new employees of, and reemphasizes to other employees, the importance of preserving the confidentiality, integrity, and availability of data and IT resources entrusted to them. An effective security awareness program includes the identification of the specific knowledge, skills, and abilities needed to support the security of District data and IT resources.

In July 2019, District management implemented a third-party training solution related to school safety and security measures. Courses available through the online delivery platform included IT security related topics such as cybersecurity, e-mail, passwords, and malware, in addition to other specialized non-IT security related topics such as transportation and classroom safety and stress management. However, our audit procedures disclosed that the available courses did not include training for safeguarding confidential and sensitive data and IT resources and, as of June 2020, only 3 of the District's 5,000 employees had completed one or more of the IT security related training courses.

In response to our inquiry, District management indicated that, until courses are approved by the District Professional Development Committee, all courses are optional for employees and, because of the impact of the COVID-19 pandemic, no determination had been made regarding mandatory training. The lack of a comprehensive, mandatory security awareness training program increases the risk that employees may compromise the confidentiality, availability, and integrity of District data and IT resources.

Recommendation: District management should establish a comprehensive, mandatory security awareness training program to ensure that employees are aware of their responsibilities and the importance of securing District data and IT resources.

Finding 3: Security Controls – Data Protection, User Authentication, Account Management, 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 data protection, user authentication, account management, 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 District data and related IT resources. However, we have notified appropriate District management of the specific issues.

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

Recommendation: District management should improve the IT security controls related to data protection, user authentication, account management, and vulnerability management to ensure the 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 September 2019 through September 2020 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 District network and related operations during the period September 2019 through July 2020, and selected actions subsequent thereto. The overall objectives of the audit were:

- 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.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)[1] and adapted for a government environment within the *Standards for Internal*

[1] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

Control in the Federal Government issued by the United States Government Accountability Office. That framework is illustrated in the following table.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the Board and District Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that all internal control components were significant to our audit objectives. The associated underlying principles significant to our objectives included:

- Board and management commitment to integrity and ethical values.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the District's goals and objectives.
- Management design of control activities to achieve the District's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management use of relevant and quality information to achieve the District's objectives.
- Management communication of information internally necessary to achieve the District's objectives.
- Management communication of information externally necessary to achieve the District's objectives.
- Management activities to monitor the District's internal control system and evaluate the results.
- Management remediation of identified internal control deficiencies on a timely basis.

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, regulations, 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 our 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 our 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 our audit findings and 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 vendors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting our audit, we:

- Reviewed applicable laws, rules, Board policies, District procedures, and other guidelines; interviewed District personnel; and examined District records to obtain an understanding of the District network and related operations 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 District IT processes for network and operational controls, including authentication, logical controls, vulnerability management, data protection, security awareness training, incident response, inventory management, and logging and monitoring of the network.
- Evaluated the effectiveness of inventory management controls for District IT resources, including a process for regular discovery and remediation of unauthorized devices.
- Evaluated the effectiveness of District logical access controls assigned to the District network and selected network devices and software, including periodic evaluations of assigned user access privileges.
- Examined and evaluated security settings related to the District network and selected network devices and software to determine whether authentication controls were configured and enforced in accordance with IT best practices.

- Examined selected logs and reports to determine the adequacy of District logging and monitoring controls designed for the network and selected network devices, including monitoring, analysis, and remediation.
- Evaluated the effectiveness of District configuration management controls of selected network devices, including establishing, modifying, and monitoring standard secure configurations; implementing software updates; and managing device end-of-life.
- Evaluated the effectiveness of District data protection controls, including procedures and tools used to prevent unauthorized data disclosure.
- Evaluated the effectiveness of District vulnerability management controls, including policies and procedures for scanning, analysis, and remediation of identified vulnerabilities; appropriate tools for identification of malicious software; and malware defense.
- Evaluated the effectiveness of the District security awareness training program and examined District records as of June 8, 2020, to determine the number of employees that attended IT security related training courses.
- Evaluated the effectiveness of District incident response procedures, including a comprehensive plan with defined roles, training, and communication.
- Examined and evaluated the appropriateness of administrative privileges for the District network domain as of May 12, 2020.
- Examined and evaluated six user accounts with access to request changes to the District firewall as of June 16, 2020.
- Evaluated the adequacy of 7,423 District computers' malware protection as of August 6, 2020.
- Examined and evaluated 930 domain accounts not required to have a password change as of May 26, 2020.
- 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

CLAY COUNTY DISTRICT SCHOOLS

900 WALNUT STREET, GREEN COVE SPRINGS, FL 32043
P (904) 336-6500 **F** (904) 336-6536 **W** oneclay.net

SUPERINTENDENT OF SCHOOLS
David S. Broskie

BOARD MEMBERS:
Janice Kerekes, District 1
Beth Clark, District 2
Tina Bullock, District 3
Mary Bolla, District 4
Ashley Gilhousen, District 5

March 5, 2021
Sherrill F. Norman, CPA
Auditor General
State of Florida

Re: Response to Information Technology Operational Audit Findings

Finding 1: *The District did not maintain a comprehensive inventory of IT resources, increasing the risk that unauthorized devices may connect to the District network without timely detection and security and other critical updates may not be timely implemented.*

District Response 1:
The District is implementing new controls with the hosted firewall to identify unauthorized devices in order to meet the requirements of the finding, creating a more comprehensive inventory of IT resources.

Finding 2: *The District had not established a comprehensive, mandatory security awareness training program, increasing the risk for District data to be compromised.*

District Response 2:
The District will be implementing mandatory security awareness training for new hires in the onboarding process. Security training for existing administrators and staff will be implemented on designated Professional Learning Days and during school staff meetings.

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

District Response 3:
The District is working to improve IT security controls related to data protection, user authentication, account management, and vulnerability management. In addition, the district is investigating tools for improved data protection and vulnerability management to ensure the confidentiality, integrity, and availability of district data and IT resources.

Respectfully,

David S. Broskie, Superintendent
Clay County District Schools