STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-212
May 2019

CHARLOTTE COUNTY
DISTRICT SCHOOL BOARD

Focus Student Information System

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period, July 2018 through October 2018, Steve Dionisio served as Superintendent of the Charlotte County Schools and the following individuals served as School Board Members:

	District No.
Lee Swift, Vice Chair	1
Kim Amontree	2
Robert Segur	3
Ian Vincent, Chair	4
Wendy Atkinson	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 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

CHARLOTTE COUNTY DISTRICT SCHOOL BOARD

Focus Student Information System

SUMMARY

This operational audit of the Charlotte County District School Board (District) focused on evaluating selected information technology (IT) controls applicable to the Focus Student Information System (Focus) for maintaining and processing student account information and the infrastructure supporting Focus. As summarized below, our audit disclosed areas in which improvements in District controls and operational processes are needed.

Finding 1: District controls related to application security management need improvement.

Finding 2: Change management controls related to application and systems software and network infrastructure changes need improvement to ensure that changes are appropriately documented, authorized, tested (where applicable), and approved prior to implementation into the production environment.

Finding 3: District controls related to periodic reviews of access to the servers and database and network administrator groups need improvement.

Finding 4: District IT security controls related to user authentication, user account management, and logging and monitoring of system activity need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The Charlotte 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 Charlotte County District School Board (Board), which is composed of five elected members. The appointed Superintendent of Schools is the executive officer of the Board. During the 2017-18 fiscal year, the District had 21 centers and schools other than charter schools, 3 charter schools, and reported 15,422 unweighted full-time equivalent students.

The District uses the Focus Student Information System (Focus) to process and report student information. In addition, the District maintains and manages the IT infrastructure supporting Focus, including the network domain, application servers, database server, and database management system.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Security Management

Effective application security management provides a framework for managing risk, developing policies, and monitoring the adequacy of application-related controls. As part of application security management, a comprehensive, documented security design ensures, through the identification of sensitive transactions and separation of duties, that security roles are defined appropriately so that users are not granted excessive or inappropriate access. In addition, periodic reviews of access privileges associated with security roles help ensure that access privileges provided to each security role remain appropriate and necessary.

IT access privileges within Focus are controlled by assigning profiles to users. Permissions to access certain modules and view or edit specific screens and fields are defined to each profile. Although the District established 49 separate profiles, because Focus is unable to produce reports detailing user access capabilities, the District could not, upon audit request, provide a listing of the capabilities granted to each user through the assigned profiles. Consequently, District records did not demonstrate the appropriateness of user IT access privileges assigned within Focus or that District management had an effective process in place for maintaining and reviewing user access privileges.

In response to our audit inquiry, District management indicated that a project was initiated in June 2018 to review the access privileges assigned to each of the District's profiles using an online review of each screen defined to a specific profile to determine the associated view and edit capabilities and assess the appropriateness of those capabilities for a given District user role. The review had not been completed as of February 2019. However, District management further indicated that the District anticipates upgrading in April 2019 to the next version of Focus which provides for reporting of user access capabilities.

Absent the ability to effectively review access privileges, there is an increased risk that the District may not timely detect and address inappropriate or unnecessary access privileges, should they exist.

Recommendation: We recommend that District management improve application security management by implementing an effective process for the periodic review of access privileges assigned within Focus and the timely removal of any inappropriate or unnecessary access privileges detected.

Finding 2: Change Management

Effective change management controls over modifications to application systems and hardware and systems software ensure that only authorized, tested (where applicable), and approved changes are implemented into the production environment. Further, the effectiveness of change management controls is enhanced through controls that ensure documented change control procedures.

Our audit inquiries and review of available documentation related to Focus application changes disclosed that, although Focus School Software staff (Focus staff) made changes to the Focus student system, the District had not established procedures to require documentation of the authorization, testing (where applicable), and approval for all changes. Specifically, some changes to the Focus application were documented in a ticketing system or by an e-mail communication, while other changes may have been verbally discussed between District and Focus staff, for example, during meetings held monthly at the District. To further corroborate our understanding of the District's current process for making changes to the Focus application, we reviewed the eight changes implemented during the period July 1, 2018, through September 30, 2018. Of the eight changes, three were recorded in the ticketing system which documented the appropriate authorization and approval for each change. Of the remaining five changes, three did not have any supporting documentation and the other two were documented through e-mail communication; however, neither e-mail communication was complete with regard to authorization and approval.

In addition, our audit procedures disclosed that although the District documented major changes such as server upgrades and replacement of switches using a Web-based documentation service, management had not established procedures for managing changes to system software and the network infrastructure, including network devices, servers, and operating systems, to ensure that changes are documented to evidence appropriate authorization, testing (where applicable), and approval prior to implementation into the production environment.

Effective change management controls reduce the risk that erroneous or unauthorized application, hardware, or system software changes may be implemented into the production environment and ensure that documentation for all changes evidences appropriate authorization, testing, and approval.

Recommendation: We recommend that District management establish change control procedures to ensure and to document that application and systems software and network infrastructure changes are appropriately authorized, tested (where applicable), and approved prior to implementation into the production environment.

Finding 3: Periodic Review of Access Privileges

Effective access controls include periodic reviews of accounts and associated access privileges to data and IT resources to help ensure that only authorized accounts have access and that the access provided to each account remains appropriate and necessary.

Our audit procedures disclosed that District management had not established procedures for, and had not performed, periodic reviews of all accounts (i.e., staff, system, and service accounts) on the Windows server and database, and assigned to administrator groups for the network.

Periodic reviews of accounts and associated access privileges increase management's assurance that accounts continue to be authorized and appropriate and reduce the risk that unauthorized disclosure, modification, or destruction of District data and IT resources may occur.

Recommendation: We recommend that District management establish procedures for, and perform, periodic reviews of accounts and associated privileges on the Windows server and database and for administrator groups on the network.

Finding 4: Security Controls – User Authentication, User Account Management, and Logging and Monitoring

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, user account management, and logging and monitoring 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 user authentication, user account management, and logging and monitoring, 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, user account management, and logging and monitoring 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 July 2018 through October 2018 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 Focus Student Information System (Focus) during the period July 2018 through October 2018, and selected actions subsequent thereto. 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 staff and reviewed District documentation to obtain an understanding of and evaluate District operations for the Focus infrastructure, including authentication, logical controls, change management, and logging and monitoring of the network, application and database servers, and the database management system; Focus application logical controls, change management, and logging and monitoring; and the data and business process flows within Focus.
- Evaluated the effectiveness of logical access controls, including periodic reviews of access privileges assigned within Focus.
- Evaluated the effectiveness of logical access controls, including periodic reviews of accounts assigned to the network domain, application and database servers, and the database management system supporting Focus.
- Examined and evaluated the appropriateness of administrative privileges, as of July 10, 2018, for the District's network domain and, as of July 12, 2018, for the database server.
- Examined and evaluated 85 network domain accounts, as of July 10, 2018, not required to have a password change.
- Examined and evaluated the appropriateness of 87 accounts assigned to the database management system, as of July 3, 2018.
- Examined and evaluated the appropriateness of 37 accounts, as of September 10, 2018, assigned to each of the two application servers supporting Focus.
- Evaluated user authentication controls related to Focus and the IT infrastructure supporting Focus.
- Evaluated the effectiveness of the District's change management controls related to the authorization, testing, and approval of Focus application changes.
- Examined and evaluated the appropriateness of eight Focus changes implemented during the period July 2018 through September 2018.
- Evaluated the effectiveness of system software and network infrastructure component change control procedures related to the District's IT infrastructure applicable to Focus.
- Evaluated the effectiveness of the District's logging and monitoring controls, including actions performed by privileged users, for the network domain, application and database servers, and the database management system supporting Focus.
- Evaluated the effectiveness of the District's logging and monitoring controls related to student information in Focus.

- 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***.

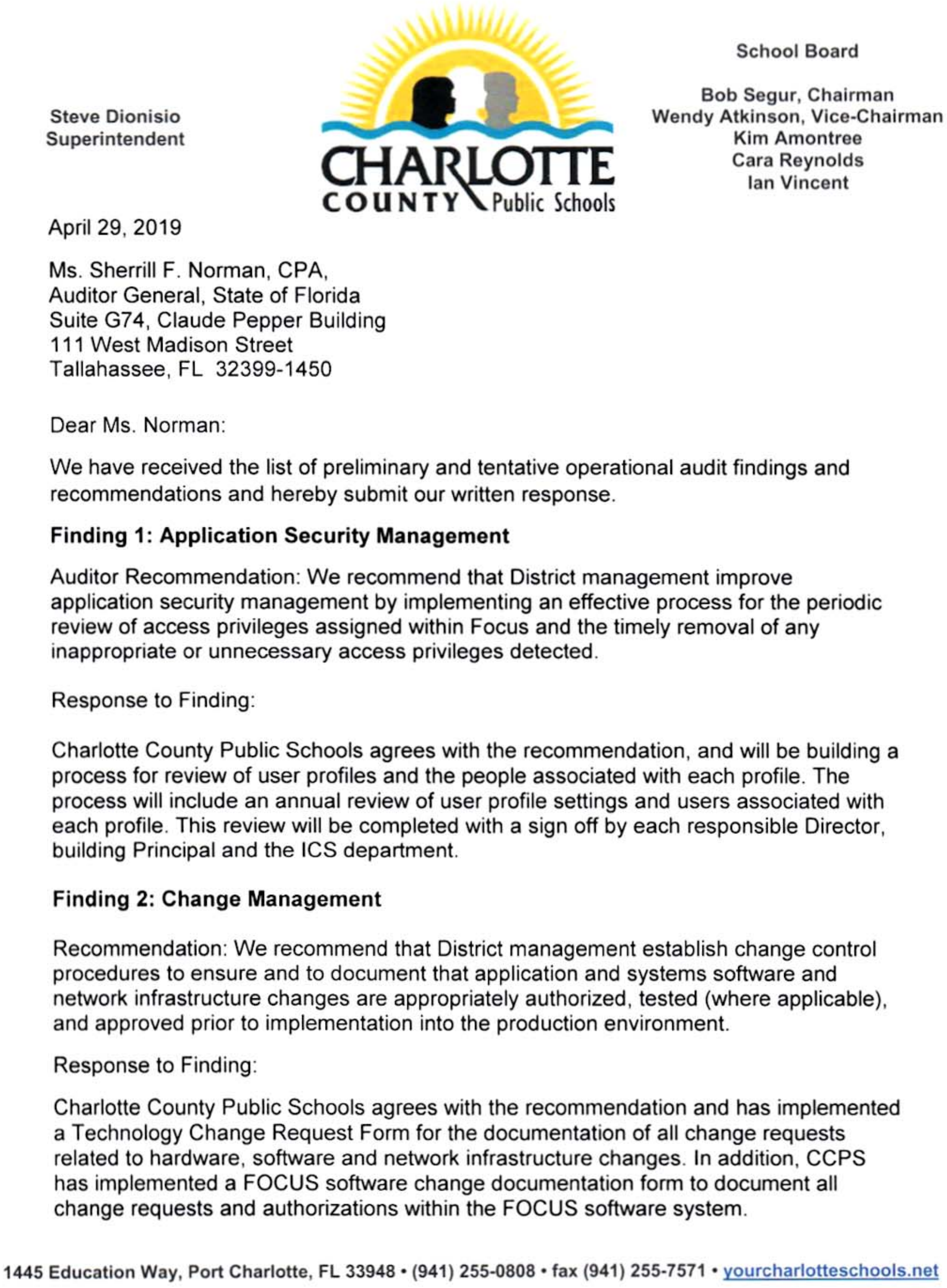
AUTHORITY

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

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



Steve Dionisio
Superintendent

CHARLOTTE
COUNTY Public Schools

April 29, 2019

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

Dear Ms. Norman:

We have received the list of preliminary and tentative operational audit findings and recommendations and hereby submit our written response.

Finding 1: Application Security Management

Auditor Recommendation: We recommend that District management improve application security management by implementing an effective process for the periodic review of access privileges assigned within Focus and the timely removal of any inappropriate or unnecessary access privileges detected.

Response to Finding:

Charlotte County Public Schools agrees with the recommendation, and will be building a process for review of user profiles and the people associated with each profile. The process will include an annual review of user profile settings and users associated with each profile. This review will be completed with a sign off by each responsible Director, building Principal and the ICS department.

Finding 2: Change Management

Recommendation: We recommend that District management establish change control procedures to ensure and to document that application and systems software and network infrastructure changes are appropriately authorized, tested (where applicable), and approved prior to implementation into the production environment.

Response to Finding:

Charlotte County Public Schools agrees with the recommendation and has implemented a Technology Change Request Form for the documentation of all change requests related to hardware, software and network infrastructure changes. In addition, CCPS has implemented a FOCUS software change documentation form to document all change requests and authorizations within the FOCUS software system.

Finding 3: Periodic Review of Access Privileges

Recommendation: We recommend that District management establish procedures for, and perform, periodic reviews of accounts and associated privileges on the Windows server and database and for administrator groups on the network.

Response to Finding:

Charlotte County Public Schools agrees with the need to establish a written procedure and periodic review of accounts and associated privileges in this area. Currently, CCPS does review these users periodically as personnel changes happen. CCPS recognizes the need for a more formal process and will work towards the implementation of such a procedure.

Finding 4: Security Controls – User Authentication, User Account Management, and Logging and Monitoring

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

Response to Finding:

CCPS will review the IT security controls related to the above referenced areas and will look to improve upon the settings currently in place.

Thank you for your time and insight while working with our district staff during this process, as it helps improve the operations of Charlotte County Public Schools.

Sincerely,

Steve Dionisio
Superintendent of Schools