STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2023-002
July 2022

VOLUSIA COUNTY
DISTRICT SCHOOL BOARD

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the 2020-21 fiscal year, Dr. Ronald “Scott” Fritz served as Superintendent of the Volusia County Schools from January 30, 2021; Dr. Carmen J. Balgobin served as Superintendent through January 29, 2021; and the following individuals served as School Board Members:

	District No.
Jamie M. Haynes, Vice Chair from 11-17-20	1
Anita Burnette from 11-17-20	2
Ida D. Wright through 11-16-20, Chair	2
Linda Cuthbert, Chair from 11-17-20, Vice Chair through 11-16-20	3
Carl Persis	4
Ruben Colón	5

The team leader was Nicole E. Ryals, CPA, and the audit was supervised by Keith A. Wolfe, CPA.

Please address inquiries regarding this report to Edward A. Waller, CPA, Audit Manager, by e-mail at tedwaller@aud.state.fl.us or by telephone at (850) 412-2887.

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

VOLUSIA COUNTY DISTRICT SCHOOL BOARD

SUMMARY

This operational audit of the Volusia County School District (District) focused on selected District processes and administrative activities and included a follow-up on findings noted in our report No. 2019-211 and the management letter comment in the 2019-20 fiscal year financial audit report. Our operational audit disclosed the following:

Finding 1: District personnel did not always verify vendor bank accounts before electronic payments were made to those accounts and, as a result, electronic payments totaling $359,566 for vendor services were made to a wrong bank account.

Finding 2: Required background screenings were not always timely performed.

Finding 3: District procedures for monitoring implementation of the District enterprise resource planning (ERP) system did not include use of the Board-established steering committee or other effective procedures to ensure the timely and successful implementation of the system.

Finding 4: During the 2019-20 and 2020-21 fiscal years, the District did not conduct required annual tangible personal property (TPP) inventories or obtain Board approval for disposed TPP items with a net value of $200,000.

Finding 5: As similarly noted in our report No. 2019-211, some unnecessary information technology (IT) user access privileges existed that increased the risk that unauthorized disclosure of sensitive personal information of students may occur.

Finding 6: District records did not clearly identify the access privileges of the 58 users with access to the District finance ERP system, increasing the risk that unauthorized disclosure, modification, or destruction of District data and IT resources could occur.

Finding 7: District security management needs improvement.

Finding 8: District personnel did not receive security awareness training for the 2020-21 fiscal year.

Finding 9: District IT security controls related to user authentication continue to need improvement.

BACKGROUND

The Volusia 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 Volusia County. The governing body of the District is the Volusia 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 2020-21 fiscal year, the District operated 69 elementary, middle, high, and specialized schools; sponsored 7 charter schools; and reported 57,759 unweighted full-time equivalent students.

FINDINGS AND RECOMMENDATIONS

Finding 1: Vendor Payments

State law[1] requires each school district to establish and maintain internal controls designed to, among other things, detect fraud, promote and encourage compliance with applicable contracts and best practices, and safeguard assets. For example, to ensure that vendor payments are appropriate, and to reduce the likelihood of fraud or errors associated with those payments, it is essential for vendor information (e.g., address and bank account) changes to be properly authorized, documented, and independently verified before payments are made.

Responses to audit inquiries and our examination of District records disclosed that, during the 2020-21 fiscal year, vendor payments were made by District check or Automated Clearing House (ACH) electronic payments. The District Purchasing Department was responsible for approving vendors and entering vendor information into the District finance enterprise resource planning (ERP) system and District personnel documented satisfactory receipt of goods and services before payments were made. Pursuant to the District *Purchasing Manual,* District departments and schools were required to e-mail vendor address changes to the Purchasing Department for approval.

Although the *Purchasing Manual* required the Purchasing Department to approve vendor address changes, District procedures did not require documented independent verification as to the accuracy of the change and to confirm that the vendor authorized the changes. Similarly, the *Purchasing Manual* did not require verification that the vendor authorized changes to bank account information for ACH electronic payments or that the changes were accurate. Moreover, Finance Department procedures, as of November 2020, allowed District vendors to request and receive electronic payments by submitting an *ACH Payment Authorization* form and a voided check to a Finance Department e-mail account. According to District personnel, vendor information changes were not verified of record before payment because District procedures had not been established to require that verification.

As part of our audit, we inquired of District personnel and examined District records for any known or suspicious transactions or activities. Through these procedures, we were made aware of the following sequence of events associated with District payments to a vendor for information technology (IT) resources and other payment-related activities.

- In September 2020, Finance Department personnel received a scanned voided check identifying the vendor's appropriate address, along with a completed *ACH Payment Authorization* form, to change the vendor payment method from District check to ACH electronic payment to the requester's bank account. After the change, the District attempted to make a $181.30 ACH electronic payment to the requester's account; however, the payment was refused and Finance Department personnel notified the requester using the requester's e-mail address. Subsequent to the notification, the requester submitted another completed *ACH Payment Authorization* form with a voided check showing the vendor's appropriate address but identifying a different bank and bank account number. Finance Department personnel used that to update the vendor payment information in the finance ERP system.

[1] Section 1010.01(5), Florida Statutes.

- On October 1, 2020, the requester e-mailed the Finance Department to cancel ACH electronic payments and to revert to District check payments.
- On October 15, 2020, the requester again e-mailed the Finance Department another *ACH Authorization* form with a scanned voided check with the vendor's appropriate address but another bank and bank account number, and Finance Department personnel updated the payment information in the finance ERP system.
- On October 20, 2020, the District IT Department received an e-mail from the authorized vendor regarding past due invoices that were unpaid by the District.
- During the period October 21, 2020, through November 12, 2020, the District made four ACH electronic payments totaling $359,566 for vendor services to the requester's bank account.
- On November 18, 2020, the District IT Department responded to the October 20, 2020, authorized vendor e-mail and indicated that payments had been made by ACH electronic payments.
- On November 20, 2020, the authorized vendor notified the District that the ACH payment bank account was not an authorized vendor bank account and District personnel notified the DeLand Police Department about the theft and filed a police report.
- On November 25, 2020, the District recovered proceeds relating to the theft totaling $193,869 from the District's bank and $140,697 from the District's cyber insurance company. Ultimately, the District was responsible for the $25,000 deductible portion of the District's insurance policy.

In response to these events, in December 2020 District procedures were revised to discontinue vendor-initiated payment method changes from District checks to electronic payments. However, through August 2021, Finance Department personnel were allowed to continue inputting other vendor information changes, such as address changes to reroute vendor checks, without independent verification.

To evaluate the authorization and propriety of vendor information changes, we requested for examination District records identifying changes during the 2020-21 fiscal year. However, according to District personnel, the finance ERP system could not generate a report of the changes and other records were not readily available to identify vendor information changes. In response to our inquiry, District personnel indicated that, as of September 2021, the Purchasing Department assumed responsibility for all vendor information changes and that, by June 2022, District procedures will be established to require independent verification of vendor bank account information in the finance ERP system. In June 2022, the DeLand Police Department indicated that the theft investigation was in progress, no charges had been filed, and the theft appeared to be the result of an overseas fraud scheme.

Without effective procedures to document independent verification of vendor information changes before payments are made, there is an increased risk for fraud or errors to occur without timely detection and recovery of losses. In addition, absent records identifying all vendor information changes, the District's ability to monitor those changes and the propriety of vendor payments is limited.

The District internal auditor included the fraudulent transactions in an audit of Finance Department activities and reported the results to the Audit Committee in September 2021. The results included recommendations that the District implement a comprehensive verification process for vendor file changes, maintain a list of authorized vendor representatives to make changes, and confirm the changes with those representatives through a formal vendor change application form, as well as a secondary review of all vendor file changes. The internal auditor also recommended that the Finance Department collaborate with the IT Department to maintain an audit trail or log of vendor information changes that identifies the changes, who made them, and when they were made.

Recommendation: The District should continue efforts to enhance the vendor payment process. Such efforts should include effective procedures requiring documented independent verification of vendor information changes, such as changes to vendor addresses and bank accounts, to ensure the proper authorization and accuracy of the changes before payments are made. To provide for appropriate verification, the District should also modify the finance ERP system so the system can generate an audit trail or log that identifies the changes and who and when the changes were made.

Finding 2: Background Screenings

Pursuant to State law,[2] instructional and noninstructional personnel who fill positions that require direct contact with students must undergo a level 2 background screening[3] at least once every 5 years. As of June 30, 2021, the District employed 8,199 (5,195 instructional and 3,004 noninstructional) personnel requiring background screenings and, according to District personnel, the Human Resource (HR) Department is responsible for ensuring timely screenings. District personnel manually input the date of the background screening into the District HR ERP system to track the date of the most recent screening.

As part of our audit, we scanned District records as of August 2021 supporting the most recent background screening dates for the 8,199 employees and found that 386 (5 percent) of those employees did not undergo a background screening in the past 5 years. Subsequent to our inquiry, District personnel indicated that background screenings for the 386 employees were completed by November 2021. We requested for examination District records supporting the screenings of 28 of the 386 employees and found that 3 employees had separated from District employment and the screenings for the other 25 were completed but ranged from 3 months to 5 years, or an average of 9 months, late.

In response to our inquiries, District personnel indicated that employee turnover, the lack of sufficient personnel, and increasing demands placed on the HR Department caused the untimely screenings. Although the subsequent background screenings disclosed no unsuitable backgrounds, our procedures cannot substitute for management's responsibility to ensure and document that background screenings are performed timely. Absent effective controls to ensure the timely screenings, there is an increased risk that individuals with unsuitable backgrounds may be allowed access to students.

Recommendation: The District should enhance procedures to appropriately monitor background screening due dates and ensure that applicable employees obtain the required background screenings at least once every 5 years.

Finding 3: Enterprise Resource Planning

State Board of Education (SBE) rules[4] and Board policies[5] provide that the District may acquire IT systems, such as an ERP system and related services, by direct negotiation and contract with a provider as best fits the District's needs. Appropriately written ERP system project contracts establish reasonable time lines for testing the system, before the system is fully implemented, to disclose unanticipated

[2] Sections 1012.32, 1012.465, and 1012.56(10), Florida Statutes.
[3] A level 2 background screening includes fingerprinting for Statewide criminal history records checks through the FDLE and national criminal history records checks through the Federal Bureau of Investigation.
[4] SBE Rule 6A-1.012(14), Florida Administrative Code (FAC).
[5] Board Policy 702, *Purchasing*.

problems and to verify that the system will function as intended. In addition, it is important for the District to establish procedures for effectively monitoring project progression during the system implementation process.

The Board decided to replace the District's existing ERP system and, to assist with the process, established a District Steering Committee in October 2016 to help develop the request for proposal (RFP), advertise the RFP, and select the ERP system provider. After direct negotiations with the selected provider, in July 2017 the Board approved an ERP system project contract for finance and human resources applications that included the project scope, deliverables, and vendor and District responsibilities during the system implementation process. Notwithstanding the contract-established dates for implementing the ERP system phases, the contract did not establish timelines for testing and modifying the system before the system was fully implemented. Although we requested, District personnel could not explain why such timelines were not established.

Under the contract terms for project governance, the District Steering Committee was responsible for ensuring project progression through system implementation. Contract-required tasks to ensure successful project progression included monthly quality assurance meetings to review reports on project status and overall progress prepared jointly by the vendor and District project managers. As part of our audit, we requested for examination District records evidencing the Committee meetings and related actions at those meetings. While agendas mentioning the ERP system RFP and vendor selection criteria were maintained for meetings during the period October 2016 through June 2017, District records did not include recorded minutes of those meetings and, when the contract was executed in July 2017, the Committee ceased to exist. In addition, the Board contracted with another service provider who tracked and reported project activities for the period March 11, 2020, through March 10, 2021. However, District records did not demonstrate any efforts to ensure that the project progressed through system implementation according to contract and District personnel could not explain why the Committee ceased to function after the contract was executed.

Table 1 outlines the ERP system contract costs and contract and actual implementation dates.

Table 1
ERP System Contract Costs
and Contract and Actual Implementation Dates

Component	Contract Costs	Contract Implementation Dates	Actual Implementation Dates
Project Management, Change Management, Quality Assurance	$ 543,050	Throughout the Project	Throughout the Project
Phase I – Finance	1,992,400	July 2018	July 2019
Phase IIa – Human Capital Management	1,902,800	January 2019	Not Applicable
Phase IIb – Planning and Budgeting	765,000	September 2018	September 2019
Travel	34,500	Throughout the Project	Throughout the Project
Total	$5,237,750		

Source: District records.

During the period December 2018 through November 2020, the Board approved four change orders, which increased the total District cost by $2.4 million for additional consultant hours and extended related delivery dates, while project deliverables either remained the same or were reduced. Although we requested, District records were not provided to demonstrate how the change orders benefited the District. Specifically:

- The first change order dated December 2018 extended the implementation date for both Phase I and Phase IIa, and District records were not maintained to justify the extension dates. Additionally, the change order removed, for each phase, the vendor's responsibility to correct the prototype until all requirements were identified and included, consequently limiting the District's ability to ensure that the ERP system ultimately met District expectations.
- For the three subsequent change orders dated May 2019, July 2019, and March 2020, the deliverable date for the HR/payroll module, included in Phase IIa for Human Capital Management, was further extended without District records justifying the extensions. While the change orders authorized additional vendor payroll testing, conversion procedures, and reconciliation reports mainly to ensure that the payroll calculation process was completed within the new application, District records were not maintained to show why the additional services were not part of the original contract or how the project progressed as a result of the change orders. Ultimately, as discussed below, the District decided against use of the ERP system Phase IIa component, resulting in unnecessary system costs totaling $1,340,210.

In response to our inquiries, District personnel indicated that several District personnel changes[6] occurred that contributed to the ERP system implementation delays as new personnel needed time to understand the status of the ERP system implementation process and determine actions necessary to help complete the process. Notwithstanding, had the Steering Committee functioned effectively, Committee members who continued to participate could have reduced or eliminated the delays by collaborating with new personnel and ensuring timely project progression through system implementation.

In August 2021, after expending $1,340,210 during the previous 4 years for the ERP Phase IIa, the District elected to continue use of the previous HR application because Phase IIa did not produce correct employee pay amounts. In May 2022, District personnel indicated they were negotiating with the vendor for cost reimbursements related to the nonfunctional Phase IIa component.

Absent contract provisions to establish timelines for testing and modifying an IT system through system implementation and continued oversight by a District Steering Committee or other District procedures to ensure timely project progression, there is an increased risk for the District to experience excessive costs, unacceptable deliverables, and avoidable deliverable due date extensions.

Recommendation: The District should establish effective procedures to ensure efficient and effective implementation of IT systems and related services. Such procedures should require and ensure that:

- **IT system contracts establish timelines for testing and modifying the system before the system is fully implemented.**

[6] Personnel changes included changes in the Superintendent, Chief Information Officer, Chief Human Resources Officer (Steering Committee Member), Chief Operations Officer (Steering Committee Member), and Chief Finance Officer (Steering Committee Member) positions as well as several District personnel in the IT, Human Resources, and Finance Departments.

- **Steering committees effectively monitor IT system project progression through system implementation according to contract by conducting monthly quality assurance meetings and maintaining records to document actions taken at those meetings.**
- **District records are maintained to demonstrate how contract change orders benefit the District.**

Finding 4: Tangible Personal Property

At June 30, 2021, the District reported costs of $78.5 million for tangible personal property (TPP), including furniture, fixtures, and equipment and motor vehicles, and a total of $59.7 million for accumulated depreciation on that TPP. State law[7] and Florida Department of Financial Services (DFS) rules[8] require the District to maintain adequate records of TPP in its custody and to ensure that a complete physical inventory is taken annually. State law also requires the authority for TPP disposals be recorded in the minutes of Board meetings.

Similarly, Board policies[9] require that an inventory of all TPP be performed annually, all TPP items found during the inventory be included in the property records, and items not located be promptly reported to the property custodian to cause a thorough investigation to be made. If the investigation determines that the item was stolen, the District is required to file a report with the appropriate law enforcement agency describing the missing item and the circumstances surrounding the disappearance. The policies also require the Board to approve all TPP dispositions.

In response to our request for District records supporting the required 2019-20 and 2020-21 fiscal year annual TPP inventories, District personnel indicated that a physical inventory was last done during the 2018-19 fiscal year when the District's inventory tracking software was used and that the software had not been integrated into the new finance ERP system. Consequently, the finance ERP system could not generate property records by custodian or location to help facilitate the 2019-20 and 2020-21 fiscal year inventories.

In addition, although the District disposed of TPP items with acquisition costs totaling $11.9 million and accumulated depreciation totaling $11.7 million during the 2018-19 through 2020-21 fiscal years, District personnel did not present a list of obsolete TPP items to the Board to approve for disposal, contrary to State law and Board policies. In response to our inquiry, District personnel indicated that a list of obsolete TPP items is typically presented to the Board for approval after disposal of the obsolete TPP items. However, the Board never approved the TPP disposals during the 2018-19 through 2020-21 fiscal years since the finance ERP system did not have the ability to produce a report of obsolete TPP items.

Given the District's significant investment in TPP, it is important that TPP items be effectively safeguarded and managed. Absent the conduct of appropriate annual physical inventory procedures and Board authorization for TPP disposals, the District cannot demonstrate compliance with State law and DFS rules and there is an increased risk that any loss or theft of District property will not be timely detected, reported to the appropriate parties, or correctly reflected in District property and accounting records. In

[7] Chapter 274. Florida Statutes.
[8] DFS Rule 69I-73, Florida Administrative Code.
[9] Board Policy 712, *Tangible Personal Property.*

November 2021 District personnel informed us that, due to the finance ERP system's inability to provide TPP information and records, the District obtained another software application for use in the recording and monitoring of TPP acquisitions, deletions, and inventories.

Recommendation: The District should enhance procedures to provide for proper accountability for District TPP. Such procedures should include a complete and documented physical inventory of TPP each year with thorough investigation of items not located and notification to the appropriate law enforcement agency and the Board for items determined stolen. In addition, before TPP items are disposed of, the District should ensure that Board authorization is obtained.

Finding 5: Information Technology – User Access Privileges to Sensitive Personal Student Information

The Legislature has recognized in State law[10] that social security numbers (SSNs) can be used to acquire sensitive personal information, the release of which could result in fraud against individuals or cause other financial or personal harm. Therefore, public entities are required to provide extra care in maintaining the confidential status of such information. Effective controls restrict individuals from accessing information unnecessary for their assigned job duties and provide for documented, periodic evaluations of IT user access privileges to help prevent individuals from accessing sensitive personal information inconsistent with their responsibilities.

Student SSNs are included in the student records maintained within the District's student information system (SIS) to, for example, register newly enrolled students and transmit that information to the Florida Department of Education through a secure-file procedure and provide student transcripts to colleges, universities, and potential employers based on authorized requests. Board policies[11] authorize designated District school officials access to student records in the exercise of a legitimate educational interest.

Our examination of District records disclosed that, as of August 2021, the District SIS contained sensitive personal information for 162,619 former and 50,442 current students and 754 District users had continuous access to the former and current student information. According to District personnel, the District SIS included a mechanism to differentiate the access privileges to sensitive personal information of former and current students, but that mechanism had not been utilized.

As part of our audit, we inquired of District personnel and examined District records supporting the IT user access privileges for all 754 users with access privileges to the sensitive information of students. We found that District records did not demonstrate the need for 209 users, such as District SIS administrators, individuals who worked for the SIS provider, testing coordinators, and help desk personnel, to have access privileges to the sensitive information of former or current students. In response to our inquiries, District personnel indicated that periodic evaluations of access privileges had not been performed due to higher than usual workloads resulting from the COVID-19 pandemic.

Subsequent to our inquiry, District personnel indicated that the inappropriate access privileges were eliminated for the 209 users. The existence of unnecessary IT user access privileges increases the risk

[10] Section 119.07(5)(a), Florida Statutes.
[11] Board Policy 201, *Student Records*.

of unauthorized disclosure of sensitive personal information and the possibility that such information may be used to commit fraud against former or current District students. A similar finding was noted in our report No. 2019-211.

Recommendation: To ensure that sensitive personal information maintained by the District is properly safeguarded, the District should perform periodic evaluations of IT user access privileges and timely remove any inappropriate or unnecessary access privileges detected. In addition, if an employee only requires access privileges to either current or former student information, the District should utilize system capabilities to limit such access accordingly.

Finding 6: Information Technology – Other User Access Privileges

Access controls are intended to protect data and IT resources from unauthorized disclosure, modification, or destruction. Effective access controls provide employees access to IT resources based on a demonstrated need to view, add, change, or delete data and restrict employees from performing incompatible functions or functions outside their areas of responsibilities. As part of these controls, a security administrator is responsible for granting employee IT access privileges and limiting such IT privileges based on the employee's job responsibilities. Periodic evaluations of assigned IT access privileges are necessary to ensure that employees can only access those IT resources that are necessary to perform their assigned job responsibilities.

As noted in Table 1 in Finding 3, the District transitioned to the ERP system finance component in July 2019. The District finance component includes, for example, the ability to create and edit vendor information, create and post journal entries, and process payment transactions. In addition, the District ERP system HR/payroll module includes, for example, the ability to add new employees, adjust pay rates, and process payroll transactions. The District security administrator is responsible for granting IT access privileges by assigning roles to employees; however, District records supporting the finance component access privileges only identify role names in general and did not specify the access privileges associated with each role or the propriety of the privileges assigned based on assigned job responsibilities.

For example, one role name is "buyer" and District personnel assume that the role is related to the finance component purchasing function; however, District personnel were unaware whether access privileges established by this role may also grant incompatible privileges in the ERP System finance component to create vendors, post journal entries, and process payment transactions. A user with such incompatible privileges could create a fictious vendor, submit a requisition order, issue a purchase order, and approve an invoice for payment.

Our examination of District records disclosed that 33 users were assigned and had appropriate update access privileges to the ERP System HR/payroll module. However, since District records did not demonstrate the specific access granted to the ERP system finance component, the propriety of the access for the 58 finance component users was uncertain, increasing the risk that the users' access privileges may have been unnecessary or incompatible with their job responsibilities. Also, because District records did not specify the access privileges associated with each role, periodic evaluations of assigned IT access privileges have not been conducted. In addition, the District internal auditor included user access to the finance component in the scope of an audit of Finance Department activities and

reported[12] that "…roles do not contain detailed descriptions of access or edit rights, thus we were unable to complete our audit procedures to determine if user access roles were appropriate."

Subsequent to our inquiries, District personnel indicated that they are aware of the need to limit access to critical functions, and in February 2022, the District entered into a contract with a vendor to develop customized roles for the ERP system finance component based on purchasing and finance staff job responsibilities to assign roles that will maintain an appropriate separation of duties. While other District controls such as documented Board review and approval of monthly financial reports mitigate some of the risk associated with these access control deficiencies, absent documented access privileges and appropriate monitoring of those privileges, management has limited assurance that District data and resources are adequately protected against unauthorized disclosure, modification, or destruction and that any unauthorized actions that may occur will be timely detected.

Recommendation: The District should continue efforts to identify access privileges assigned to roles within the ERP system finance component to ensure that such privileges are limited to those necessary for employees to perform their assigned duties. Such efforts should also include periodic evaluations of IT user access privileges to ensure that the privileges restrict employees from performing incompatible functions or functions outside their areas of responsibilities.

Finding 7: Information Technology – Security Management

Effective security management outlines the duties of those responsible for overseeing security and those who own, use, or rely on District IT resources. Such management should include policies and procedures to ensure risk reduction and compliance with applicable standards and guidance and with District-determined system configuration requirements.

In January 2022, the District Chief Information Officer (CIO) began drafting an *Information and Technology Services Directives, Standards, Guidelines, and Procedures Manual* to address network, server, and endpoint security, access, and other cybersecurity controls. The intent of the manual was to underscore the CIO's responsibility for operating a security program to effectively manage risk and ensure the protection of District IT systems through a set of directives documenting expectations for achieving the underlying Board-approved policies over IT areas. Implementation of certain directives relied on detailing requirements or procedures within a standard. However, as of May 2022, standards had not been developed for directives, including encryption, configuration management, electronic data disposal, endpoint, network, and server security, information classification and protection, and logging. In addition, a cyber security incident response plan had not been developed to address the directive for computer security incident response to mitigate cybersecurity incidents affecting District information and technology assets and following the best practice recommendations from the National Institute of Standards and Technology.

In response to our inquiries, District personnel indicated that security management procedures had not been developed because implementation of the new ERP system was not completed. Notwithstanding, without effective security management, including defined requirements and procedures for implementing security directives, the risk is increased that controls designed to ensure the confidentiality, integrity, and

[12] Internal Audit Report: Year End Tax Reporting and Disbursements.

availability of District data and IT resources will not be followed consistently or in accordance with management's expectations.

Recommendation: District management should continue to develop the *Information and Technology Services Directives, Standards, Guidelines, and Procedures Manual*, including the completion of all corresponding standards.

Finding 8: Information Technology – 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.

During May 2021, the District began using a Web-based provider to provide security awareness training that included topics such as student data privacy, the proper use of District technology, phishing prevention, and cybersecurity awareness. Subsequently, in July 2021, the District began using a bundled security training application. However, we found that, as of January 2022, only staff in the District's IT Department had completed the IT security-related training courses and District personnel indicated that staff in all other departments would complete the training at the beginning of the 2022-23 fiscal year.

The lack of a comprehensive security awareness training program increases the risk that employees may compromise the confidentiality, availability, and integrity of District data and IT resources.

Recommendation: The District should continue efforts to establish a comprehensive security awareness training program to inform employees about their responsibilities and the importance of securing District data and IT resources.

Finding 9: Information Technology – Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain District controls related to user authentication needed improvement. We are not disclosing 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, the risk is increased that the confidentiality, integrity, and availability of District data and IT resources may be compromised. A similar finding was noted in our report Nos. 2019-211 and 2016-075.

Recommendation: The District should improve security controls related to user authentication to ensure the continued confidentiality, integrity, and availability of District data and IT resources.

PRIOR AUDIT FOLLOW-UP

The District had taken corrective actions for findings included in our report No. 2019-211 and the management letter comment in the 2019-20 financial audit report, except as noted in Findings 5 and 9 and shown in Table 2.

Table 2
Findings Also Noted in Previous Audit Reports

Finding	2017-18 Fiscal Year Operational Audit Report No. 2019-211, Finding	2014-15 Fiscal Year Operational Audit Report No. 2016-075, Finding
5	4	Not Applicable
9	5	7

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 operational audit from May 2021 through June 2022 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This operational audit focused on selected District processes and administrative activities, including, but not limited to, District information technology resources and related controls, public meetings and communications, school safety, fiscal transparency, compensation, construction, and other expenses. For those areas, our audit objectives were to:

- Evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, and safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2019-211 and the management letter comment in the 2019-20 financial audit report.
- 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 those areas included within the scope of the audit, weaknesses in management's internal controls significant to our audit objectives; instances of noncompliance with

applicable laws, rules, regulations, contracts, grant agreements, and other guidelines; 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 transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions 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 the program, activity, or function; identifying and evaluating internal controls significant to our audit objectives; 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.

Our audit included transactions, as well as events and conditions, occurring during the 2020-21 fiscal year audit period, and selected District actions taken prior and subsequent thereto. Unless otherwise indicated in this report, these records and transactions 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 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 and District procedures, and other guidelines, and interviewed District personnel to obtain an understanding of applicable processes and administrative activities.
- Reviewed Board information technology (IT) policies and District procedures to determine whether the policies and procedures addressed certain important IT control functions, such as security, configuration management, electronic data disposal, logging and monitoring, patch management, and vulnerability assessment.
- Evaluated District procedures for maintaining and reviewing employee access to IT data and resources. We examined selected access privileges to the District enterprise resource planning (ERP) system Human Capital Management component to determine the appropriateness and necessity of the access based on employee job duties and user account functions and whether the access prevented the performance of incompatible duties. Specifically, we tested all 33 users with update access privileges to critical human resource (HR) functions. We also identified 58 users with update access privileges to the District ERP system financial component to determine the appropriateness and necessity of access to the finance component. In addition, we examined the administrator account access privileges granted and procedures for oversight of administrative accounts for the applications to determine whether these accounts had been appropriately assigned and managed.

- Examined District records supporting the acquisition of an ERP system and related services to determine whether the District evaluated the effectiveness and suitability of the ERP system prior to purchase, contract change orders were evaluated for reasonableness and supported by District records, and deliverables met the contract terms and conditions.
- Evaluated District procedures for protecting the sensitive personal information of students, including social security numbers. Specifically, we examined the access privileges of all 754 individuals who had access to sensitive personal student information to evaluate the appropriateness and necessity of the access privileges based on the employee's assigned job responsibilities.
- Evaluated District procedures to prohibit former employee access to electronic data files. We also determined whether all 33 users with update access privileges to the ERP system HR/payroll module and all 58 users with update access to the ERP system finance component were active employees.
- Determined whether Board security policies or District procedures governing the classification, management, and protection of sensitive and confidential information were developed.
- Examined network and application security settings to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Determined whether an adequate, comprehensive IT security awareness and training program was in place.
- Evaluated District IT procedures for requesting, testing, approving, and implementing changes to the District finance and HR ERP system.
- Evaluated Board policies and District procedures and examined supporting documentation to determine whether audit logging and monitoring controls for applications data changes; security table changes; sensitive or privileged accounts, such as database administrators and system administrators; and key systems activity and security events were configured in accordance with IT best practices.
- Evaluated the adequacy of District procedures related to security incident response and reporting.
- Analyzed the District's General Fund total unassigned and assigned fund balances at June 30, 2021, to determine whether the total was less than 3 percent of the fund's revenues, as specified in Section 1011.051, Florida Statutes. We also performed analytical procedures to evaluate the District's ability to make future debt service payments.
- Examined the District Web site to determine whether the 2020-21 fiscal year proposed, tentative, and official budgets were prominently posted pursuant to Section 1011.035(2), Florida Statutes. In addition, we determined whether the Web site contained the required graphical representations, for each public school within the District and for the District, of summary financial efficiency data and fiscal trend information for the previous 3 years, and a link to the Web-based fiscal transparency tool developed by the Florida Department of Education (FDOE).
- Examined Board policies and procedures and District records related to public records requests during the period January 2021 through August 2021 to determine whether the District granted those requests in compliance with Chapter 119, Florida Statutes.
- Reviewed audit plans and audit agendas to determine whether the District-contracted internal auditor during the audit period reported directly to the Board or its designee as required by Section 1001.42(12)(l), Florida Statutes, and performed the duties specified in that section. We also determined whether the internal auditor developed audit work plans based on annual risk assessments considering input from other finance and administrative management.
- From the population of expenditures totaling $56.4 million and transfers totaling $8.6 million during the period July 2020 through March 2021, from nonvoted capital outlay tax levy proceeds,

discretionary sales tax proceeds, impact fees, and other restricted capital project funds, examined documentation supporting selected expenditures and transfers totaling $1.9 million and $5.1 million, respectively, to determine District compliance with the restrictions imposed on the use of these resources, such as compliance with Section 1011.71(2), Florida Statutes.

- Examined Board minutes identifying surplus property deletions and disposals during the audit period, interviewed District personnel, and reviewed District records to evaluate the District's surplus property control procedures.
- Requested for examination documentation supporting the District's annual tangible personal property (TPP) physical inventory process to determine whether the inventory was completed and the results were reconciled to the property records, appropriate follow-up was made for any missing items, and law enforcement was timely notified for any items that could not be located and considered stolen. In addition, we requested for examination District records supporting the propriety of TPP disposals.
- Evaluated severance pay provisions in the Superintendent's employment contract to determine whether the provisions complied with Section 215.425(4), Florida Statutes.
- From the compensation payments totaling $224.7 million to 9,525 employees during the period July 2020 through March 2021, examined District records supporting compensation payments totaling $59,246 to 31 selected employees to determine the accuracy of the rate of pay and whether supervisory personnel reviewed and approved employee reports of time worked.
- Determined whether the appointed Superintendent's compensation for the audit period was in accordance with State law, rules, and Board policies.
- From the population of 4,319 instructional personnel and 215 school administrators compensated a total of $132 million for the period July 2020 through March 2021, examined documentation for 30 selected employees to determine whether the District had developed adequate performance assessment procedures for instructional personnel and school administrators based on student performance and other criteria in accordance with Section 1012.34(3), Florida Statutes, and whether a portion of each selected instructional employee's compensation was based on performance in accordance with Section 1012.22(1)(c)4. and 5., Florida Statutes.
- Examined District records supporting teacher salary increase allocation payments totaling $10 million for the audit period to 4,421 instructional personnel to determine whether the District submitted required reports (salary distribution plan and expenditure reports) to the FDOE and used the funds in compliance with Section 1011.62(18), Florida Statues.
- Examined District records for the audit period for 28 employees, 30 contractor workers, and 21 volunteers selected from the population of 8,199 employees, 4,155 contractor workers, and 63 volunteers to assess whether individuals who had direct contact with students were subjected to the required fingerprinting and background screenings.
- Evaluated the effectiveness of Board policies and District procedures addressing the ethical conduct of instructional personnel and school administrators, including reporting responsibilities related to employee misconduct which affects the health, safety, or welfare of a student, to determine the sufficiency of those policies and procedures to ensure compliance with Section 1001.42(6), Florida Statutes.
- Evaluated Board policies and District procedures to ensure that health insurance was provided only to eligible employees, retirees, and dependents and that, upon an employee's separation from District employment, insurance benefits were timely canceled as appropriate based on the Board policies.
- Evaluated District procedures for acquiring health insurance for officers and employees and examined related records to determine whether the District complied with Section 112.08, Florida Statutes. We also reviewed the reasonableness of procedures for acquiring other types of

commercial insurance to determine whether the basis for selecting insurance carriers was documented in District records and conformed to good business practices.

- From the four significant construction projects with expenditures totaling $28.4 million for the period July 2020 through March 2021, selected two construction management contract projects with guaranteed maximum price contracts totaling $27.4 million and examined documentation supporting selected project expenditures totaling $2.4 million to determine compliance with Board policies, District procedures, and applicable provisions of State law and rules. Specifically, we examined District records to determine whether:
  - The construction manager was properly selected pursuant to Section 255.103, Florida Statues.
  - District personnel properly monitored subcontractor selection and licensures.
  - Architects were properly selected pursuant to Section 287.055, Florida Statutes, and adequately insured.
  - Appropriate Board policies and District procedures addressing the negotiation and monitoring of general conditions costs had been established.
  - 6 selected payments totaling $2.4 million were adequate and sufficiently supported.
  - Projects progressed as planned consistent with established benchmarks and were cost effective, and contractors performed as expected.
  - The District made use of its sales tax exemption to make direct purchases of materials or documented justification for not doing so.
- Examined District records to determine whether the Board had adopted appropriate school safety policies and the District implemented procedures to ensure the health, safety, and welfare of students and compliance with Sections 1006.07, 1006.12, 1006.13, 1011.62(15), and 1012.584, Florida Statutes.
- Examined District records to determine whether the Board had adopted appropriate mental health awareness policies and the District had implemented procedures to promote the health, safety, and welfare of students and ensure compliance with Sections 1011.62(16), and 1012.584, Florida Statutes, and State Board of Education (SBE) Rule 6A-1.094124, Florida Administrative Code.
- Determined whether vendor payments were reasonable, correctly recorded, adequately documented, for a valid District purpose, properly authorized and approved, and in compliance with applicable State laws, SBE rules, contract terms and Board policies; and applicable vendors were properly selected. Specifically, from the population of vendor payments totaling $204.9 million for the period July 2020 through March 2021, we examined District records supporting 31 selected payments totaling $674,974.
- Through responses to audit inquiries and examination of District records, evaluated the propriety of vendor payment methods, including District check and Automated Clearing House electronic payments and vendor authorization for those payments.
- From the population of expenditures totaling $20.5 million related to 156 vendors for contracted services during the period July 2020 through March 2021, examined supporting documentation, including the contract documents, for 17 selected payments totaling $1.9 million related to 13 contracts to determine whether:
  - The District complied with applicable competitive selection requirements (e.g., SBE Rule 6A-1.012, Florida Administrative Code).
  - The contracts clearly specified deliverables, time frames, documentation requirements, and compensation.

- District records evidenced that services were satisfactorily received and conformed to contract terms before payment.
- The payments complied with contract provisions.

- 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, requires that the Auditor General conduct an operational audit of each school district on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

VOLUSIA COUNTY SCHOOLS

Dr. Carmen J. Balgobin
Superintendent of Schools

School Board of Volusia County

Mr. Ruben Colón, Chairman
Ms. Jamie M Haynes, Vice Chairman
Mrs. Linda Cuthbert
Mrs. Anita Burnette
Mr. Carl Persis

July 21, 2022

Ms. Sherrill F. Norman, CPA
Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

This letter is in response to the preliminary and tentative audit findings and recommendations as outlined in your letter dated June 23, 2022.

As requested, enclosed you will find a written statement in response to the preliminary and tentative findings, along with the corrective action plans as warranted.

Sincerely,

Dr. Carmen J. Balgobin
Superintendent of Schools

Enclosure
Copy to: School Board Members

P.O. BOX 2118 · 200 NORTH CLARA AVE
DELAND, FL 32720
(386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

Finding 1: Vendor Payments
The vendor payment process has been enhanced. Verification of vendor bank accounts is a function of the Purchasing Department effective September 2021. Procedures include independent verification of vendor information changes.

Finding 2: Background Screenings
This duty was assigned to an HR Analyst. At the end of each month, they log in to FLDLE and review any employee who is due for the 5-year review. Each person is looked up individually in our HR system. If they are still employed with us, their fingerprints are re-submitted. If they are no longer working for us, they are deleted from FLDLE. A spreadsheet is now kept of those who are deleted each month.

Finding 3: Enterprise Resource Planning
VCS acknowledges that our ERP implementation has not been fully successful. We have established a new steering committee to establish effective procedures to ensure efficient and effective implementation of our ERP. We are reviewing the current ERP and possible new solutions. The committee is establishing timelines for testing and modifying the system as we determine the full scope of functionality the district needs in its ERP and if our current systems meet those requirements. The district has moved to direct licensing of its current system and canceled any further consultation contracting for the past implementation of phase II.

Finding 4: Tangible Personal Property
Upon go-live with Oracle on July 1, 2019, we no longer had the ability to utilize our physical inventory software. The Oracle software did not have the capabilities to conduct physical inventory. We had researched and met with 3rd party vendors over time to acquire a new more sophisticated physical inventory taking software. We had begun implementing a new software called Destiny but ran into many roadblocks with its ability to communicate with Oracle. That implementation was cancelled, and the search began again for a software. On June 24, 2021, we contacted FOCUS School Software and began the process of acquiring their services for a physical inventory software. We went 'live' with the FOCUS inventory system on May 2, 2022. Our schools and departments conducted their FY22 physical inventory through June 30th, using the Fixed Assets module in FOCUS. Their findings and signed reports have been submitted to the inventory office for final review. We plan to start the FY23 physical inventory in September/October timeframe.
On June 14, 2022, a list of disposed assets from July 2019 to February 2022 went before the Board and was approved for retirement. Those assets were updated with the Board Approved date and 'retired' from the FOCUS Fixed Assets system.

Finding 5: Information Technology – User Access Privileges to Sensitive Personal Student Information
VCS acknowledges the existence of some accounts with unnecessary elevated privileges. We have conducted an evaluation of user access privileges and removed any inappropriate or unnecessary access privileges found. We are also working with our SIS vendor (Focus) to better configure our access privileges to ensure that staff only have the level needed.

Finding 6: Information Technology – Other User Access Privileges
The District developed customized roles for the ERP system finance component based on purchasing and finance staff job responsibilities to assign roles that will maintain an appropriate separation of duties and identify access privileges assigned to ERP roles in the finance system to ensure that such privileges are limited to those necessary for employees to perform their assigned duties. We are reviewing the current ERP and possible new solutions.

P.O. BOX 2118 · 200 NORTH CLARA AVE
DELAND, FL 32720
(386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

Finding 7: Information Technology – Security Management
The District has developed a cyber security improvement plan and has begun implementing it including multi-factor authentication and improvements in our firewall and DNS filtering systems.

Finding 8: Information Technology – Security Awareness Training
The District is developing an online training for student data privacy and security awareness for all staff.

Finding 9: Information Technology – Security Controls – User Authentication
The District has developed a cyber security improvement plan that will help us better protect the confidentiality, integrity, and availability of data and IT resources.

P.O. BOX 2118 · 200 NORTH CLARA AVE
DELAND, FL 32720
(386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer