STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-095
January 2020

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource Subsystem (FLAIR)

Sherrill F. Norman, CPA
Auditor General

Chief Financial Officer

Pursuant to Article IV, Sections 4(c) and 5(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Jimmy Patronis served as Chief Financial Officer during the period of our audit.

The team leader was Arthur Wahl, CPA, CISA, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

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

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource Subsystem (FLAIR)

SUMMARY

This operational audit of the Department of Financial Services (Department) focused on evaluating selected information technology (IT) controls applicable to financial reporting and applicable to the Florida Accounting Information Resource Subsystem (FLAIR) and included a follow-up on selected findings included in our report No. 2019-068 applicable to the scope of our audit. Our audit disclosed the following:

Finding 1: The Department did not always timely deactivate the FLAIR user accounts with access privileges to the Central Accounting Component and Payroll Component when employees separated from Department employment. Similar findings were noted in our report No. 2019-068.

Finding 2: As similarly noted in our report No. 2019-068, the Department had not established a comprehensive policy for the performance of background screenings of employees and contracted consultants in positions of special trust. Additionally, background screening processes for contracted consultants need improvement to ensure all consultants are screened prior to the start of the contracted work.

Finding 3: Certain security controls related to physical security, user authentication, and logging and monitoring continue to need improvement to help ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.

BACKGROUND

The Florida Accounting Information Resource Subsystem (FLAIR) is the State of Florida's accounting system. State law[1] establishes FLAIR as a subsystem of the Florida Financial Management Information System and the Department of Financial Services (Department) as the functional owner of FLAIR. The functions of FLAIR, as stated in State law[2] include accounting and reporting, so as to provide timely data for producing financial statements for the State in accordance with generally accepted accounting principles, and auditing and settling claims against the State.

FLAIR and the Department play a major role in ensuring that State financial transactions are accurately and timely recorded and that the State's Comprehensive Annual Financial Report (CAFR) is presented in accordance with appropriate standards, statutes, rules, and regulations.

FLAIR is composed of four components:

- The Departmental Accounting Component (DAC), which maintains State agency accounting records and provides accounting details for general ledger transactions, accounts receivable, accounts payable, grants, projects, and assets. DAC provides State agency management with a budgetary check mechanism. The Statewide Financial Statements Subsystem of DAC and

[1] Sections 215.93(1)(b) and 215.94(2), Florida Statutes.

[2] Section 215.94(2)(a),(b), Florida Statutes.

Wdesk are used to assist and support the Department's Division of Accounting and Auditing in the preparation of the State's CAFR. State agencies are the primary users of DAC.

- The Central Accounting Component (CAC), which maintains the State of Florida's checkbook used by the Department to process payments for the State. CAC is a cash-basis system for the control of budget by line item of the General Appropriations Act. The primary user of CAC is the Division of Accounting and Auditing.
- The Payroll Component, which processes the State's payroll. The Division of Accounting and Auditing is the primary user of the Payroll Component. The Bureau of State Payrolls within the Division of Accounting and Auditing administers payroll processing.
- The Information Warehouse, which is a reporting system that allows users to access information extracted from DAC, CAC, the Payroll Component, and certain systems external to FLAIR. State agencies are the primary users of the Information Warehouse.

The Department is responsible for the operation and maintenance of FLAIR. Within the Department, the Office of Information Technology operates the Chief Financial Officer's Data Center that maintains FLAIR.

In 2014, the Department, as the functional owner of FLAIR, created the Florida Planning, Accounting, and Ledger Management (Florida PALM) project to replace FLAIR and most of the applications within the Cash Management Subsystem (CMS)[3] with an integrated, enterprise financial management solution to modernize the State's financial management processes and system. A Pre-Design, Development, Implementation (Pre-DDI) Closeout Report was issued on June 29, 2018, which concluded the Pre-DDI phase. On July 20, 2018, the project entered DDI Phase 1 by executing a contract with Accenture, LLP for Software and System Integrator Services. DDI Phase 1 implements the financial management software solution focusing on core functionality (at a minimum, functionality currently performed by the FLAIR DAC, CAC, Payroll Component, Information Warehouse, and selected CMS functions). DDI Phase 2 will implement expanded functionality beyond what is defined for DDI Phase 1 (e.g., transition from Grant Accounting to full Grant Management functionality) to meet the solution goals.

The DDI Phase 1 includes transitioning FLAIR DAC, CAC, and Payroll Component functions and CMS functions to Florida PALM. In 2021, five State organizations will transition from DAC, CAC, and CMS to Florida PALM; and the remaining State organizations will transition from CAC and CMS functions. DDI Phase 1 also includes the remaining organizations transitioning from DAC to Florida PALM in two groups, the first half in July 2023, and the second half in July 2024. Finally, in 2025, DDI Phase 1 includes all State organizations transitioning from the FLAIR Payroll Component to Florida PALM. DDI Phase 2 includes all State organizations implementing additional functionality in 2026. An Executive Steering Committee, together with the Florida PALM Project Director, is responsible for Florida PALM project governance. The Committee consists of 15 members and includes representatives from multiple State agencies.

[3] The CMS includes the CMS application, Fund Accounting, Dis-Investments, Consolidated Revolving Account, Bank Accounts, Warrant Processing, Investment Accounting, State Accounts, Archive, Special Purpose Investment Account (SPIA), and Certificates of Deposit (CD). Florida PALM replaces eight of these applications, excluding Archive, SPIA, and CD.

FINDINGS AND RECOMMENDATIONS

Finding 1: Timely Deactivation of Access Privileges

Effective management of information technology (IT) access privileges includes the timely deactivation of employee IT access privileges when an employee separates or is suspended from employment. Prompt action is necessary to ensure that the access privileges are not misused by former employees or others to compromise data or IT resources. Department policy[4] states that access shall be granted on the principles of least privilege and a need-to-know basis and requires access control administrators to deactivate, by the close of business on the separation date, access assigned to employees voluntarily separating from Department employment. For involuntary separations, Department policy requires the Information Security Manager to ensure access to the Department's network is deactivated at the designated time of the involuntary separation.

Our audit procedures disclosed that the Florida Accounting Information Resource Subsystem (FLAIR) user accounts were not always timely deactivated upon an employee's separation from Department employment. Specifically, we evaluated the user accounts for 19 employees with CAC access privileges and 10 employees with Statewide access privileges to the Payroll Component who separated from Department employment during the period July 1, 2018, through June 30, 2019, and found that:

- The user accounts for 3 of the 19 former employees with CAC access privileges were not timely deactivated and remained active from 1 to 5 days after the employees separated from Department employment.
- The user accounts for 4 of the 10 former employees with Statewide access privileges to the Payroll Component were not timely deactivated and remained active from 1 to 111 days after the employees separated from Department employment.

Timely deactivation of FLAIR user accounts upon an employee's separation from Department employment reduces the risk that CAC and Payroll Component access privileges may be misused by the former employee or others. Similar findings were noted in prior audits of the Department, most recently in our report No. 2019-068.

Recommendation: We recommend that Department management ensure that FLAIR user accounts with CAC and Payroll Component access privileges are timely deactivated upon the employee's separation from Department employment.

Finding 2: Background Screenings

Effective security controls include the performance of security background screenings upon hire and periodically thereafter for personnel in sensitive or special trust positions. Such positions typically include IT personnel with elevated access privileges or responsibilities for the custody of sensitive IT resources. Additionally, State law[5] requires each State agency to designate positions that, because of the special trust, responsibility, or sensitive location, require security investigations (i.e., background screenings).

[4] Administrative Policies and Procedures, *Application Access Control Policy*, 4-05.

[5] Section 110.1127(2)(a), Florida Statutes.

All persons and employees in such positions must undergo background screenings, including fingerprinting, as a condition of employment and continued employment.

In prior audits of the Department, most recently in our report No. 2019-068, we noted that the Department had not established a comprehensive Departmentwide policy for background screenings that required the periodic performance of background screenings for personnel and contracted consultants in positions of special trust. In response to our prior audits, Department management indicated that a Departmentwide background screening policy was in development and would include the requirement for timely performance of background screenings of employees and contracted consultants in positions of special trust. The draft policy requires contracted consultants to be screened prior to hire and every 2 years. As part of our follow-up audit procedures, we examined the Department's policies and procedures and noted that, as of November 4, 2019, the Departmentwide background screening policy continued to be in development and remained uncompleted. While the Department only had a draft policy for background screenings, the Department had a process that required new employees and contracted consultants hired into positions of special trust to be screened as a condition of employment and employees transferring to a position of special trust be screened if it had been more than 6 months since their last screening.

We evaluated background screening reports as of June 24, 2019, for 17 of the 53 Office of Information Technology (OIT) contracted consultants requiring background screening as a condition of providing services to the OIT. We included in the 17 OIT contracted consultants selected for evaluation the 5 contracted consultants identified in our report No. 2019-068 as missing a current background screening to determine whether the Department had taken corrective action. Our audit procedures disclosed that, as of June 24, 2019:

- Corrective action had not been taken for 4 of the 5 contracted consultants identified in our audit report No. 2019-068 as lacking a current background screening, and the 4 contracted consultants continued to lack a background screening for the current contracts that began in 2017.
- For 2 of the contracted consultants, while background screenings were performed in December 2013 and March 2015, respectively, a background screening had not been performed for the current contracts that began in July 2018.
- For 1 contracted consultant, a background screening for the current contract beginning in March 2017 was not completed.

Without a comprehensive Departmentwide background screening policy and effective procedures, the risk is increased that people with inappropriate backgrounds may be employed in positions of special trust and may gain access to confidential or sensitive data and IT resources.

Recommendation: We again recommend that Department management finalize the comprehensive Departmentwide background screening policy and related procedures and ensure the timely performance of background screenings of contracted consultants in positions of special trust.

Finding 3: Security Controls – Physical Security, User Authentication, 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 physical security, user authentication, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FLAIR data and other Department IT resources. However, we have notified appropriate management of the specific issues. Similar findings were communicated to Department management in connection with prior audits of the Department, most recently with our report No. 2019-068.

Without adequate security controls related to physical security, user authentication, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of FLAIR data and other Department IT resources may be compromised.

Recommendation: We recommend that Department management improve certain security controls related to physical security, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2019-068 that are applicable to the scope of this audit.

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 information technology (IT) operational audit from May 2019 through September 2019 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 Department of Financial Services (Department) IT business process application controls and general controls applicable to financial reporting during the period July 2018 through June 2019 and subsequent actions thereto. The overall objectives of the audit were:

- To evaluate the effectiveness of selected IT business process application controls and IT general controls applicable to the Florida Accounting Information Resource Subsystem (FLAIR) 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 determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2019-068 that are applicable to the scope of the audit.
- 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 agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel and reviewed related documentation to obtain an understanding of:
  - The strategic IT planning process and status of the Florida Planning, Accounting, and Ledger Management (Florida PALM) project, including system architecture, funding, and project timelines.
  - The processes used and data flows for synchronizing data between FLAIR and Wdesk, the application used to assist in the preparation of the State's Comprehensive Annual Financial Report, and the procedures for restricting access to Wdesk.
  - Background screening processes for Department employees and contracted consultants in positions of special trust.
  - Processes for deactivation of access to the Central Accounting Component (CAC) and the Payroll Component functions.

- Processes for granting, discontinuing, and periodically reviewing physical access to the Department's Data Center and other Office of Information Technology (OIT) secured areas and the physical security measures in place.

- Evaluated logical access controls for CAC, Payroll Component, and Wdesk user accounts. Specifically, we evaluated:
  - Department procedures and examined Department records to determine whether periodic reviews were performed to evaluate the appropriateness of user access privileges for Wdesk.
  - The appropriateness of access for the 17 users with update access privileges to Wdesk as of June 27, 2019.
  - The adequacy of the process to restrict update access in Wdesk for prior year financial data after the reports are finalized.
  - The 19 user accounts that were assigned to CAC users who separated from Department employment during the period July 1, 2018, through June 30, 2019, to determine whether access privileges were timely removed.
  - The 10 user accounts that were assigned to Payroll Component users who separated from Department employment during the period July 1, 2018, through June 30, 2019, to determine whether access privileges were timely removed.
  - The 2,191 active CAC user accounts throughout the period July 1, 2018, through June 30, 2019, to determine whether any active accounts were assigned to vacant positions.
- Evaluated the adequacy of selected logging and monitoring controls for the Department's network, the Payroll Component, and Wdesk.
- Evaluated user identification and authentication controls, for the Departmental Accounting Component, CAC, the Payroll Component, Wdesk, and the Department's network.
- Evaluated the adequacy of controls over the synchronization of data between FLAIR and Wdesk, including the process to ensure that manual updates in Wdesk are included FLAIR.
- Examined and evaluated the Departmentwide and OIT background screening policies and procedures providing for the performance of background screenings for employees and contracted consultants in positions of special trust.
- Evaluated the timeliness of background screenings for 17 of the 53 contracted consultants providing services to the OIT as of June 24, 2019.
- Evaluated the appropriateness of physical access controls implemented at the Department's Data Center to protect its IT resources and data. Specifically, we evaluated:
  - The adequacy of policies and procedures related to restricting physical access.
  - The appropriateness of physical access privileges to the Data Center and OIT-secured areas for the 84 active key cards as of June 5, 2019.
  - The adequacy of quarterly access reviews of physical access privileges to the Data Center and OIT-secured areas for the period July 1, 2018, through June 30, 2019.
- Observed on June 12, 2019, the Department's physical security control processes implemented for OIT-secured areas to determine whether access to sensitive areas and IT resources was appropriately restricted.
- 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

CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

January 10, 2020

Sherrill F. Norman
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's information technology operational audit of the *Florida Accounting Information Resource Subsystem (FLAIR).*

If you have any questions concerning this response, please contact David Harper, Inspector General, at (850) 413-3112.

Sincerely,

Jimmy Patronis
Chief Financial Officer

JP/swm
Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 FAX (850) 413-2950

Florida Accounting Information Resource Subsystem (FLAIR)
Information Technology Operational Audit

DEPARTMENT OF FINANCIAL SERVICES
RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Timely Deactivation of Access Privileges

The Department did not always timely deactivate the FLAIR user accounts with access privileges to the Central Accounting Component and Payroll Component when employees separated from Department employment. Similar findings were noted in our report No. 2019-068.

Recommendation: We recommend that Department management ensure that FLAIR user accounts with CAC and Payroll Component access privileges are timely deactivated upon the employee's separation from Department employment.

Response: The Department concurs. The Division of Accounting & Auditing (A&A) has revised desktop procedures and provided training to additional staff on the administrative team to assist in prevention of untimely access deactivation. A&A will continue to monitor access control reports as well as work with Agency personnel to ensure timely deactivation of access. On December 13, 2019, A&A met with Agency Admin Directors and discussed the importance of monitoring agency access and timely deactivation. A&A will continue outreach to agencies in an effort to improve this process.:

Office of Information Technology (OIT) response: Although this is a manual process, due to our defense in depth strategy the risk is low, as the users must have an active "Active Directory" account to gain access to FLAIR. OIT's FLAIR team is researching potential methods of identifying potentially separated or role/duty changes by DFS users. If this type of report can be generated, this will minimize the risk of user privileges not being deactivated timely. Additional funding through an LBR would be necessary for automation to occur for this process.

Expected Completion Date for Corrective Action: February 28, 2020

Finding No. 2: Background Screenings

As similarly noted in our report No. 2019-068, the Department had not established a comprehensive policy for the performance of background screenings of employees and contracted consultants in positions of special trust. Additionally, background screening processes for contracted consultants need improvement to ensure all consultants are screened prior to the start of the contracted work.

Recommendation: We again recommend that Department management finalize the comprehensive Departmentwide background screening policy and related procedures and ensure the timely performance of background screenings of contracted consultants in positions of special trust.

Response: The Department concurs. The Division of Administration will continue its efforts to establish a comprehensive Departmentwide background screening policy and related procedures, both of which will be designed to ensure the timely performance of background screenings of employees and contracted consultants, being designated into positions of special trust.

Office of Information Technology (OIT) response: This is a moderate risk. OIT is actively working to assure all OIT workers are screened timely prior to onboarding and rescreened as recommended in the DFS draft policy. OIT will make the necessary changes to follow the approved DFS policy once completed and approved in June 2020. OIT is also having the identified consultants during the 2019 Audit rescreened and to be completed no later than February 21, 2020.

Expected Completion Date for Corrective Action: June 30, 2020

Finding No. 3: Security Controls – Physical Security, User Authentication, and Logging and Monitoring

Certain security controls related to physical security, user authentication, and logging and monitoring continue to need improvement to help ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.

Recommendation: We recommend that Department management improve certain security controls related to physical security, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.

Response: The Department concurs. The risk involved with this finding is low, as we have defense in depth; and we are continuing to improve overall processes and timeliness on our physical security and user authentication processes. ISO is defining the current operational guides for logging and monitoring controls and reports.

The Division of Accounting and Auditing is currently working with the Department's Office of Information Technology to strengthen authentication controls.

Expected Completion Date for Corrective Action: October 31, 2020