STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2022-128
February 2022

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource Subsystem (FLAIR) and Selected Information Technology General Controls

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 Suzanne B. Varick, CPA.

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) and Selected Information Technology General Controls

SUMMARY

This operational audit of the Department of Financial Services (Department) focused on the Florida Accounting Information Resource Subsystem (FLAIR) and selected information technology (IT) general controls. The audit also included a follow-up on the findings included in our report No. 2021-131. Our audit disclosed the following:

Finding 1: FLAIR program change controls need improvement to ensure that all program changes are appropriately authorized, tested, and implemented into the production environment.

Finding 2: Certain security controls related to logical access, configuration management, user authentication, and logging and monitoring continue to need improvement to 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. As provided in State law,[2] the functions of FLAIR include accounting and reporting 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 Annual Comprehensive Financial Report (ACFR) is presented in accordance with appropriate standards, rules, regulations, and statutes.

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 the Wdesk application are used to assist and support the Department, Division of Accounting and Auditing, in publishing the State's ACFR. State agencies are the primary users of DAC.
- The Central Accounting Component (CAC), which maintains the State'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.

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

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

- 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 (BOSP) 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. The primary users of the Information Warehouse are State agencies, the Division of Accounting and Auditing, and the Department's Office of Information Technology (OIT).

The Department is responsible for the design, implementation, and operation of FLAIR. Within the Department, the OIT operates the Chief Financial Officer's Data Center and maintains FLAIR.

In 2014, the Department created the Florida Planning, Accounting, and Ledger Management (Florida PALM) project to replace FLAIR and the cash management and accounting management components of the Cash Management Subsystem (CMS)[3] with a cloud-based financial management solution designed to modernize the State's financial management processes and system. As shown in Table 1, beginning in 2021, this multi-year project will transition FLAIR and CMS functions, as well as additional functionality, to the Florida PALM System using defined project timeline waves, with production support commencing upon implementation of initial functionality.

Table 1
Florida PALM System Transition Timeline
As of August 9, 2021

Project Wave	Functionality	Planned or Actual Transition Date
CMS	Cash management functions	July 2021
Payroll	Payroll functions	July 2024
Financials	State budgeting functions, agency accounting records and budget management functions, and additional functionality for all agencies	July 2024

Source: Melissa Turner, Project Director, Florida PALM Project.

During the CMS project wave, the business processes previously supported by the CMS were implemented into the Florida PALM System and the Department removed State agency update access to the CMS on July 21, 2021. State agencies will continue using the FLAIR components to execute payroll and financial functions until 2024, while using the Florida PALM System to execute cash management transactions.

An Executive Steering Committee, together with the Florida PALM Project Director, are responsible for Florida PALM project governance. The Executive Steering Committee consists of 17 members representing multiple State agencies.

[3] The CMS included 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 Deposits (CD). Florida PALM replaced eight of these applications, excluding Archive, SPIA, and CD.

FINDINGS AND RECOMMENDATIONS

Finding 1: Change Management Controls

Effective change management controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation into the production environment. Effective change management controls include reviewing all program changes implemented into the production environment for approval and appropriateness.

As part of our audit, we reviewed Department policies and procedures, interviewed Department management and personnel responsible for the FLAIR change control process, and examined change control records and found that FLAIR change controls need improvement. Specifically, we requested from the Department for each of the 12 significant FLAIR change requests implemented during the 2020-21 fiscal year documentation evidencing that the program changes associated with the change requests were properly authorized, tested by the programmer and user, approved for implementation into the production environment, and implemented into the production environment by someone other than the programmer who made the program change. Our examination found that Department records did not evidence:

- The authorization for 2 change requests and the date of authorization for another change.
- Programmer testing sign off for 1 change request and, for 2 change requests, Department records indicated that programmer testing was completed after the change requests were implemented into the production environment.
- For 1 change request, that an appropriate separation of duties existed between the programmer and implementor of the change request nor the date the change request was implemented into the production environment.

In response to our audit inquiry, Department management indicated that, during the transition to a new change management system, records evidencing authorization, programmer testing, and implementation were not always updated.

Without effective change management controls, the Department has limited assurance that all program code changes associated with a change request are appropriately authorized, tested, approved, and implemented. The absence of appropriate change management controls also increases the risk that program changes may not be implemented in a manner consistent with management's expectations.

Recommendation: We recommend that Department management improve change management controls to ensure that Department records evidence that all program changes are appropriately authorized, tested, and implemented into the production environment.

Finding 2: Security Controls – Logical Access, Configuration Management, 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 logical access, configuration management, 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 Department management of the specific issues.

Without appropriate security controls related to logical access, configuration management, 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. Similar findings were communicated to Department management in connection with prior audits of the Department, most recently in connection with our report No. 2021-131.

Recommendation: We recommend that Department management improve certain security controls related to logical access, configuration management, 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. 2021-131.

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 2021 through November 2021 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 significant Department of Financial Services (Department) IT controls applicable to financial reporting, the Florida Accounting Information Resource Subsystem (FLAIR), and other significant Departmentwide IT general controls during the period July 2020 through June 2021 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, the deficiencies disclosed in our report No. 2021-131.
- 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 included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of 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 related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of 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:

- Reviewed applicable laws, rules, Department policies and procedures, and other guidelines, and interviewed Department personnel to obtain an understanding of selected significant IT business process application controls and IT general controls applicable to financial reporting and FLAIR.
- Obtained an understanding of Department processes for approving, assigning, reviewing, and deactivating access to the FLAIR Central Accounting Component (CAC) and Payroll Component Statewide functions, including processes for ensuring an appropriate separation of incompatible duties; logical access controls for the network domain; the paths and processes for authenticating to the network domain, FLAIR components, and the Statewide Reporting System (Wdesk); management and operational processes for conducting background screenings of employees and contractors employed in positions of special trust; logging and monitoring controls for system activity; physical access controls to protect Department data and IT resources; processes for requesting, authorizing, testing, approving, implementing, and reconciling FLAIR program changes; configuration management processes for servers; and the strategic IT planning process, including the status of Florida Planning, Accounting, and Ledger Management (PALM) project funding, planned system architecture, project oversight, and implementation schedule; and the Statewide Reporting System adjustment process.
- Evaluated logical access controls, including policies, procedures, and processes, for assigning, periodically reviewing, and deactivating user accounts for the FLAIR CAC and Payroll

Component, and the administrative-level user and service accounts for the Department's network domain. Specifically, we evaluated:

  - Department procedures and examined Department records to determine whether periodic reviews were performed to evaluate the appropriateness of administrative-level access to the Department's network domain.
  - The appropriateness of access for 40 of the 82 user accounts with update access privileges to one or more of the 13 selected CAC high-risk functions or selected inquiry access to confidential data as of May 31, 2021.
  - The timeliness of FLAIR CAC access privilege deactivations for the nine Department employees with FLAIR CAC access who separated from Department employment during the period July 2020 through May 2021.
  - The appropriateness of access as of May 31, 2021, for the 43 Statewide Payroll Component users to the 38 selected Statewide Payroll Component high-risk functions.
  - The appropriateness of the 21 administrative user accounts and the 11 administrative service accounts as of June 18, 2021, for the Department network domain.

- Evaluated FLAIR program change controls including policies, procedures, and processes and examined the 12 significant FLAIR change requests implemented during the 2020-21 fiscal year to determine whether the change requests were appropriately authorized, tested, approved for production, and implemented into production.
- Evaluated the adequacy of selected logging and monitoring controls.
- Evaluated the appropriateness of physical access controls for the Department's Data Center and other Office of Information Technology (OIT) secured areas, including the adequacy of policies, procedures, and processes established to protect Department IT resources and data. Specifically, we:
  - Evaluated the appropriateness of physical access privileges to the Data Center and OIT-secured areas assigned to the 48 active key cards as of June 1, 2021.
  - Examined Department records to determine the adequacy of the quarterly access reviews performed for July 2020, October 2020, January 2021, and May 2021 of physical access privileges to the Data Center and the OIT-secured areas.
- Examined Departmentwide and OIT background screening policies and procedures for employees and contractors in positions of special trust and evaluated Department records for 20 of the 53 contractors providing services to the OIT during the 2020-21 fiscal year to assess the timeliness of background screenings performed.
- Evaluated the adequacy of user identification and authentication controls for the FLAIR Departmental Accounting Component (DAC), CAC, Payroll Component, Wdesk, and the Department's network domain.
- Evaluated the adequacy of configuration management policies, procedures, and processes for ensuring that server operating systems are supported and current. Specifically, we evaluated whether the operating systems for the:
  - Eight domain controllers were timely patched as of June 29, 2021.
  - Eight FLAIR-related servers were supported as of June 15, 2021.
- 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

February 10, 2022

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 *Department of Financial Services, Florida Accounting Information Resource Subsystem (FLAIR) and Selected Information Technology Controls.*

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/DC
Enclosure

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

2021 Florida Accounting Information Resource Subsystem (FLAIR) Information Technology Operational Audit

DEPARTMENT OF FINANCIAL SERVICES
RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Change Controls

FLAIR program change controls need improvement to ensure that all program changes are appropriately authorized, tested, and implemented into the production environment.

Recommendation: We recommend that Department management improve change management controls to ensure that Department records evidence that all program changes are appropriately authorized, tested, and implemented into the production environment.

Response: The Office of Information Technology is currently working on standardizing the FLAIR change management procedures across the CAC, DAC, and PYRL areas to assist with training of the managed services vendor and state staff.

Expected Completion Date for Corrective Action: 09/30/2022

Finding No. 2: Security Controls

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

Response: The Office of Information Technology agrees to assess and improve certain security controls related to logical access, configuration management, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.

Expected Completion Date for Corrective Action: To be determined