STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2023-097
January 2023

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 Cara Hill and the audit was supervised by Brenda Shiner, 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) 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. 2022-128. Our audit disclosed the following:

Finding 1: FLAIR program change controls continue to need improvement to ensure that all program changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the FLAIR production environment, and are managed by, and do not bypass, the Department's change management process.

Finding 2: Department records did not evidence periodic reviews of the Department network domain privileged accounts' access privileges.

Finding 3: Certain security controls related to physical access, logical access, user authentication, configuration management, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of FLAIR data and 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.

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

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

- 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.
- 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. 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-hosted enterprise resource planning financial management solution designed to modernize the State's financial management processes and system. Beginning in July 2021, this multi-year project was to transition FLAIR and CMS functions, as well as additional functionality, to Florida PALM using defined project waves, with production support commencing upon implementation of initial functionality. The CMS wave was implemented in July 2021 and transitioned the functions related to the management of bank cash, participant invested cash, and State Treasury investments from the CMS to Florida PALM. As of November 8, 2022, development of the remaining Florida PALM waves was on hold until proviso language requirements included in the 2022-23 General Appropriations Act,[4] including CMS wave remediation and stabilization, an independent accounting and financial audit of the Division of the Treasury and its cash management transactions in Florida PALM,[5] validation and finalization of the business requirements for the remaining Florida PALM waves, and an assessment of options to replace the Information Warehouse, were addressed and completed. Revised implementation dates for the remaining Florida PALM waves are expected by March 2023.

An Executive Steering Committee, together with the Florida PALM Project Sponsor and Project Director, are responsible for Florida PALM project governance. The Executive Steering Committee consists of 17 members representing multiple State agencies. In February 2022, the Department formed the Florida PALM Advisory Council comprised of 15 FLAIR users, State agency technical staff who maintain applications that integrate with FLAIR, and State agency finance and accounting or budget directors. The Florida PALM Advisory Council is responsible for assisting the Executive Steering Committee and the Florida PALM Project Sponsor and Project Director by identifying potential solutions for future Florida PALM wave implementations.

[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.

[4] Chapter 2022-156, Laws of Florida, Section 6, Specific Appropriation 2395.

[5] Chapter 2022-156, Laws of Florida, Section 111.

Until Florida PALM is fully implemented, FLAIR remains the State's accounting system and, along with selected information technology (IT) general controls, was the subject of this audit.

FINDINGS AND RECOMMENDATIONS

Finding 1: Change Management Controls

Effective change management controls are intended to ensure that all program and related changes (e.g., database changes) are properly authorized, tested, and approved for implementation into the production environment. Controls over the modification of programs, including review of before and after images of program code prior to implementation, help ensure that only approved program code changes are made within the programs.

As part of our audit, we reviewed Department change management policies and procedures, interviewed Department personnel responsible for FLAIR change management processes, and examined change management records for FLAIR program and other related changes implemented into the production environment during the period July 1, 2021, through June 9, 2022, and found that:

- Although the Department had established change management controls, including a daily (Monday through Friday) reconciliation process, to ensure that FLAIR program changes implemented into the production environment were appropriately authorized, tested, and approved for production, documentation of the reconciliations performed for CAC and DAC program changes were not retained due to an oversight.
- While CAC program changes were sometimes implemented on weekends, the automated daily reports used to reconcile implemented program changes to change management records were not generated on weekends. Consequently, CAC program changes implemented on weekends were not subject to reconciliation. Specifically, our review of CAC implementation records found that on Sunday, June 5, 2022, 98 CAC program changes were implemented into the production environment and were not reconciled to the appropriate change management records to ensure that all implemented program changes were appropriately authorized, tested, and approved for production.

  In response to our audit inquiry, Department management indicated that, while the reconciliation reports were not automatically generated for weekend program change implementations, the information was available and could be run upon request; however, because weekend implementations did not occur when the reconciliation process was developed, the reconciliation had not been conducted.
- The Department had not established a code review process for CAC and DAC program changes to ensure that programmers did not make unauthorized or accidental program changes in addition to the program changes approved for implementation into the production environment. According to Department management, the Department had not developed and standardized procedures for CAC and DAC program code reviews but that, subsequent to our audit inquiry, the Department completed the procedures in September 2022 and implemented a code review process.

To further evaluate the appropriateness of Department change management controls for program and other related changes implemented into the FLAIR production environment, we selected 13 change tickets from a listing in the Department's ticketing system of the 76 FLAIR change tickets implemented during the period July 1, 2021, through June 9, 2022. For each of the 13 change tickets, we requested from the Department documentation evidencing that the program and other related changes associated

with the change tickets were properly authorized by OIT management, tested by OIT personnel independent of the OIT programmer, tested by users, approved for implementation into the production environment, and implemented into the production environment by someone other than the personnel who made or approved the changes. As similarly noted in our report No. 2022-128 (Finding 1), we found that neither ticketing system nor Departmental Project Request (DPR) System[6] records:

- Evidenced authorization for one change ticket by OIT management prior to the change being made and tested by OIT personnel due to a misconfiguration of the ticketing system.
- Demonstrated OIT testing of all program changes related to one change ticket due to an oversight in updating testing documentation.

Without an effective reconciliation process that ensures that all implemented FLAIR program changes are recorded in the ticketing system and accurate and complete change management records, the Department has limited assurance that all program and related changes are appropriately authorized, tested, approved, and implemented into the production environment. The absence of program code reviews prior to implementation into the production environment also increases the risk that unauthorized FLAIR program changes may be implemented into the FLAIR production environment.

Recommendation: We again recommend that Department management improve change management controls to ensure that Department records evidence that FLAIR program and related changes are appropriately authorized, tested, approved for production, and implemented into the production environment. We also recommend that Department management ensure that Department records evidence through reconciliations and program code reviews that all FLAIR program changes are managed by, and do not bypass, the Department's change management process.

Finding 2: Periodic Review of Network Domain Access Privileges

Department of Management Services (DMS) rules[7] require agency information owners to review access rights (privileges) periodically based on system categorization or assigned risk. Periodic reviews of administrative-level (privileged) network domain user and service accounts with access to data and information technology (IT) resources help protect the confidentiality, integrity, and availability of data and information IT resources by ensuring that only authorized users have access and that the access privileges assigned to user and service accounts remain appropriate and necessary.

Department policies and procedures[8] required that access privilege reviews be conducted at least quarterly for all secure applications and documentation of the reviews be retained for 1 year. As part of our audit, we interviewed Department personnel, reviewed Department policies and procedures, and evaluated Department processes for periodically reviewing privileged network domain accounts. According to Department management, access reviews of privileged network domain user and service accounts were performed for the quarters ended December 2021 and March 2022; however, documentation of the reviews was not maintained because the employee conducting the reviews was unaware of the documentation requirement.

[6] The Department uses the DPR System to record (track) change management activities.

[7] DMS Rule 60GG-2.003(1)(a)6., Florida Administrative Code.

[8] Department, OIT Administrative Policies and Procedures No. 4-05, *Application Access Control*.

Without documented periodic access reviews of privileged network domain access privileges, management's assurance that access privileges were properly authorized and remained appropriate is limited.

Recommendation: We recommend that Department management ensure that employees responsible for conducting periodic reviews of privileged network domain access privileges for user and service accounts understand and adhere to Department policies and procedures and maintain documentation of such reviews.

Finding 3: Security Controls – Physical Access, Logical Access, User Authentication, Configuration Management, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to physical access, logical access, user authentication, configuration management, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FLAIR data and other Department IT resources. However, we have notified appropriate Department management of the six findings in the five areas needing improvement.

Without appropriate security controls related to physical access, logical access, user authentication, configuration management, 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 related to logical access, user authentication, configuration management, and logging and monitoring were communicated to Department management in connection with prior audits of the Department, most recently in connection with our report No. 2022-128.

Recommendation: We recommend that Department management improve certain security controls related to physical access, logical access, user authentication, configuration management, 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. 2022-128.

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 June 2022 through November 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 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 controls during the period July 2021 through June 2022 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To evaluate the effectiveness of selected significant IT controls in achieving management's 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. 2022-128.
- 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 and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of 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, waste, 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 the Department's organizational structure, statutory requirements, operational processes, and FLAIR components, consisting of the Departmental Accounting Component (DAC), the Central Accounting Component (CAC), and the Payroll Component.
- Obtained an understanding of Department processes for approving, assigning, reviewing, and deactivating access to CAC and Payroll Component Statewide access, including processes for ensuring an appropriate separation of incompatible duties; logical access controls for the Department network domain and Wdesk; the paths and processes for authenticating to the Department network domain, FLAIR components, and Wdesk and related IT resources; Department configuration management processes related to patches and updates for servers; logging and monitoring controls for security activities for the Department network domain and Wdesk; physical access controls to protect Department data and IT resources; processes for requesting, authorizing, testing, approving, implementing, and reconciling FLAIR program code changes; the strategic IT planning process, including the status of the Florida Planning, Accounting, and Ledger Management (Florida PALM) project, planned system architecture, project oversight, and implementation schedule; and the Wdesk adjustment process and enhancements for lease reporting.
- Evaluated logical access controls, including policies, procedures, and processes, for assigning, periodically reviewing, and disabling user accounts for FLAIR CAC and Payroll Component Statewide access, Wdesk, and Department network domain administrative user and service accounts. Specifically, we evaluated:
    - Department procedures and examined Department records to determine whether periodic access reviews were performed to evaluate the appropriateness of access privileges for Department network domain administrative user and service accounts, Wdesk administrative and non-administrative user accounts, and FLAIR CAC and Payroll Component Statewide access user accounts.
    - The appropriateness of access privileges for the 24 active CAC user accounts as of May 31, 2022, that were created during the period July 2021 through May 2022.
    - The appropriateness of access privileges for the 13 active Payroll Component Statewide access user accounts as of May 31, 2022, that were created during the period July 2021 through May 2022.
    - The appropriateness of access privileges for the 16 Wdesk user accounts as of June 22, 2022.
    - The appropriateness of the 20 administrative user accounts and the 11 administrative service accounts as of June 15, 2022, for the Department network domain.
    - The appropriateness of interactive log on capabilities for the 11 administrative service accounts as of June 22, 2022, for the Department network domain.
    - The timeliness of disabling CAC and Payroll Component Statewide account access for the 16 Department employees with CAC access privileges and the 7 Department employees with Statewide Payroll Component access privileges who separated from Department employment during the period July 2021 through May 2022.
- Interviewed Department personnel and examined Department policies, procedures, and processes for FLAIR change management, including program change reconciliation processes and program code reviews. Specifically, we examined 13 of the 76 FLAIR change tickets implemented during the period July 1, 2021, through June 9, 2022, as documented in the Department's ticketing system, to determine whether the program code and other related changes

were appropriately authorized, tested, approved, and implemented into the production environment.

- 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:
  - Observed physical access controls to the Data Center and other OIT-secured areas as of June 22, 2022.
  - Evaluated the appropriateness of physical access privileges to the Data Center and OIT-secured areas assigned to the 43 active keycards as of June 3, 2022.
  - Examined Department records to determine the adequacy of the quarterly access reviews completed in January 2022 and April 2022 of physical access privileges to the Data Center and the OIT-secured areas.
- Evaluated the adequacy of user identification and authentication controls for DAC, CAC, the 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 Department-managed domain controllers and eight Department-managed FLAIR-related production servers were supported and timely patched as of July 8, 2022.
- Evaluated the adequacy of interface controls related to the enhancements for lease reporting for the State's Annual Comprehensive Financial Report. Specifically, we observed data input controls, including edits and validations in place as of October 25, 2022, and lease data input access controls as of October 12, 2022.
- 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 20, 2023

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 General Controls*.

If you have any questions concerning this response, please contact Julie Jones, Interim Inspector General, at (850) 413-2829.

Sincerely,

Peter Penrod
Chief of Staff

PP/DC
Enclosure

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

2022 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 Management Controls

FLAIR program change controls continue to need improvement to ensure that all program changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the FLAIR production environment, and are managed by, and do not bypass, the Department's change management process.

Recommendation: Part 1: We again recommend that Department management improve change management controls to ensure that Department records evidence that FLAIR program and related changes are appropriately authorized, tested, approved for production, and implemented into the production environment. Part 2: We also recommend that Department management ensure that Department records evidence through reconciliations and program code reviews that all FLAIR program changes are managed by, and do not bypass, the Department's change management process.

Response: Nancy Anderson, Office of Information Technology:

Part 1: Standardized change management desk procedures were implemented September 30, 2022. The procedures were developed with input from all FLAIR sections and cover the change process from the original request through implementation of changes and reconciliation of the audit reports.

Part 2: Code review checklists have been implemented for program code reviews. These checklists will be stored in a central location for each FLAIR section. Audit reports will now be run 7 days a week and the report results will be documented each day.

Expected Completion Date for Corrective Action: Completed

Finding No. 2: Periodic Review of Network Domain Access Privileges

Department records did not evidence periodic reviews of the Department network domain privileged accounts' access privileges.

Recommendation: We recommend that Department management ensure that employees responsible for conducting periodic reviews of privileged network domain access privileges for user and service accounts understand and adhere to Department policies and procedures and maintain documentation of such reviews.

Response: Office of Information Technology, Nickolas Donnell:

The Department has implemented a process to document access reviews for privileged accounts to its resources.

Expected Completion Date for Corrective Action: Completed 1/3/2023

CONFIDENTIAL Finding No. 3: Security Controls- Physical Access, Logical Access, User Authentication, Configuration Management, and Logging and Monitoring

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

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

Response: Office of Information Technology, Stephen McKeough:

The Office of Information Technology agrees to improve security controls related to physical access, logical access, user authentication, configuration management, 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: Various