STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-025
October 2017

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource Subsystem (FLAIR)
and
Origami Risk Insurance Management System (Origami)

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 Jeff Atwater served as Chief Financial Officer during the period of our audit.

For FLAIR, the team leader was Clark Evans, CPA, CISA, and the audit was supervised by Brenda Shiner, CISA.

For Origami, the team leaders were Chrystal Temples and Arthur Wahl, CPA, CISA, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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
Origami Risk Insurance Management System (Origami)

SUMMARY

The operational audits of the Department of Financial Services (Department) focused on evaluating selected information technology (IT) controls relevant to financial reporting and applicable to the Florida Accounting Information Resource Subsystem (FLAIR) and selected IT controls applicable to the Origami Risk Insurance Management System (Origami). Our audit also included a follow-up on the findings included in our report No. 2017-089. Our audit disclosed the following:

Finding 1: The access privileges for some FLAIR users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for assigned job duties.

Finding 2: The Department's procedures and processes for assigning FLAIR user access privileges and conducting periodic reviews of these privileges need improvement to ensure access privileges assigned to users remain appropriate.

Finding 3: Change management controls related to hardware and systems software changes for network devices related to FLAIR need improvement to ensure that only approved hardware and systems software changes are implemented into the production environment.

Finding 4: The Department had not established a comprehensive policy for the performance of background screenings of employees and consultants in positions of special trust. Additionally, required background screenings for employees and consultants were not always performed.

Finding 5: Certain security controls related to physical security, access controls, user authentication, logging and monitoring, and configuration management 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. The functions of FLAIR, as provided 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.

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

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

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) 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 (SWFS) Subsystem of DAC is 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) 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 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 is a data storage and 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 (OIT), formerly the Division of Information Systems, operates the Chief Financial Officer's Data Center that maintains FLAIR.

In 2014, the Department, as the functional owner of FLAIR, created a multi-year project to replace FLAIR and the Department's Cash Management System (CMS) with a commercial off-the-shelf Enterprise Resource Planning (ERP) solution. The multi-year project is referred to as the Florida Planning, Accounting, and Ledger Management (Florida PALM) project. An Executive Steering Committee (ESC), together with the Florida PALM Project Director, are responsible for Florida PALM project governance. The ESC consists of 15 members and includes representatives from multiple State agencies.

The Florida PALM project is currently organized into three phases:

- Pre-Design, Development, Implementation (Pre-DDI) phase – This initial phase includes planning for DDI readiness, business process standardization, and procurement of the financial management software solution. The Florida PALM project is currently in this phase, expected to be completed in February 2018.
- DDI Phase 1 – This phase will implement the financial management software solution focusing on core functionality (at a minimum, functionality performed by the FLAIR CAC, DAC, Payroll Component, and Information Warehouse, as well as selected CMS functions).
- Future DDI Phases – Subsequent phases beyond what is defined for DDI Phase 1 (e.g., transition from Grant Accounting to full Grant Management functionality) will include the implementation of the remaining functionality necessary to meet the solution goals.

Pursuant to the 2016 General Appropriations Act,[3] the Department contracted with Computer Aid, Inc., to complete a business case for maintaining any of the agency business systems identified in the March 31, 2014, FLAIR study. The Department submitted the business case to the Executive Office of the Governor, President of the Senate, and Speaker of the House of Representatives on November 1, 2016. An Invitation to Negotiate (ITN) for Software and Systems Integrator procurement was created and approved by the ESC on October 26, 2016. Subsequently, on November 1, 2016, an ITN was advertised with an expected award date of February 2018.

The Division of Risk Management (Division) within the Department is responsible for the management of claims reported by or against State agencies and universities for coverage under the self-insurance fund, known as the State Risk Management Trust Fund (Trust Fund). Coverages provided through the Trust Fund include: workers' compensation, property, fleet automobile liability, general liability, Federal civil rights and employment discrimination, and court-awarded attorney fees. The Division also provides loss prevention services and technical assistance to State agencies and universities for managing risk.

The Division contracted with Origami Risk® in June 2014 to implement the Origami Risk Insurance Management System (Origami) to replace its previous risk management information system. The Division completed the full implementation of Origami in June 2016. Origami performs functions related to, among other things, claims processing, policy management, financial management, and reporting.

FINDINGS AND RECOMMENDATIONS

Finding 1: Appropriateness of Access Privileges

Effective access controls include measures that restrict access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Department policy[4] requires that accounts with administrative rights be created, maintained, monitored, and removed in a manner that protects IT resources. Department policy[5] also states that access shall be granted on the principles of least privilege and a need to know 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 some inappropriate and unnecessary access privileges for CAC user accounts, Payroll Component user accounts, and the Payroll Component program change management process. Specifically:

- We evaluated the appropriateness of access for 20 of the 183 user accounts granted update access privileges to 1 or more of the 16 key CAC functions during the period July 1, 2016, through February 28, 2017. Our audit procedures disclosed that 1 of the 20 user accounts evaluated had unnecessary update access privileges to the Vendor Payment, Prior Year 1099 Info, Prior Year

[3] Chapter 2016-066, Laws of Florida, Specific Appropriation 2317A.

[4] Administrative Policies and Procedures, *Information Technology Security Policy,* 4-03.

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

1099 Payment, and Prior Year 1099 Adjustment functions. Additionally, 1 of the 20 user accounts had unnecessary update access privileges to the Journal Transfer Audit Detail function.

Additionally, we evaluated the appropriateness of access for the 36 user accounts granted inquiry or update access to 3 electronic funds transfer (EFT) related CAC functions during the same period. Our audit procedures disclosed that 5 of the 36 user accounts evaluated had unnecessary inquiry access to the EFT Authorization Inquiry and EFT Payment functions, and 6 of the 36 user accounts had unnecessary inquiry access to the EFT Bank Title File function.

We also evaluated whether CAC access was timely deactivated for all 12 former employees with CAC access who separated from Department employment during the period July 1, 2016, through March 31, 2017. We determined that 5 of the former employees' access privileges to CAC were not timely deactivated and remained active for 3 to 68 days after the employees' separation dates.

- We evaluated the appropriateness of access for the 29 Statewide user accounts with update or override access privileges to 1 or more of the 40 key Payroll Component functions as of February 28, 2017. Our audit procedures disclosed that 4 user accounts had unnecessary update access privileges to the Retirement Input function. Additionally, 1 user account had unnecessary update access privileges to the Tax Collection Input function.

  We also evaluated whether Statewide user access was timely deactivated for the 10 former employees with Statewide access to the Payroll Component who separated from Department employment during the period July 1, 2016, through March 31, 2017. We found that the access privileges for 3 of the 10 former employees were not timely deactivated and remained active for 3 to 54 days after the employees' separation dates. A similar issue was noted in our report No. 2017-089.

- Our audit procedures disclosed that, as of May 9, 2017, all 8 employees in the OIT with the ability to implement program files into the Payroll Component production environment also had the ability to make program changes within the development environment, contrary to an appropriate separation of duties. In response to our audit inquiry, the OIT implemented a procedure on February 2, 2017, that required, prior to implementation into the production environment, the review of program changes by an individual not associated with the program changes. However, our subsequent review of the 30 Payroll Component program changes completed during the period February 2, 2017, through May 10, 2017, disclosed that, contrary to the new procedure, 26 implemented program changes had been reviewed by the same individual responsible for the program code change. A similar issue was noted in our report No. 2017-089.

Inappropriate or unnecessary access privileges increase the risk of unauthorized modification, loss, or disclosure of data and IT resources. Additionally, ineffective change management controls related to separation of duties increase the risk that erroneous or unauthorized program changes may be implemented into the production environment.

Recommendation: We recommend that Department management limit user access privileges to FLAIR to promote an appropriate separation of duties and to restrict users to only those access privileges and functions necessary for the users' assigned job duties. In doing so, Department management should ensure that the FLAIR access privileges of former employees are timely deactivated. We also recommend that Department management ensure that, prior to implementation into the production environment, program changes are reviewed by an individual not associated with the program changes.

Finding 2: Periodic Review of User Access Privileges

Effective access controls include policies and procedures for conducting comprehensive periodic reviews of all user access privileges to data and IT resources to verify that only authorized users have access

and that the access provided to each user remains appropriate and necessary for the user's assigned job duties. Agency for State Technology (AST) rules[6] require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Additionally, Department policy[7] requires business owners within the Division of Accounting and Auditing to maintain written procedures for access control to software applications and to effectively communicate these procedures to employees.

Our audit disclosed that Department procedures and processes for the periodic review of user access privileges for specific users need improvement. Specifically, we noted that:

- The Departmental FLAIR *Access Control Business Process Procedure* (*DAC Procedure*) used for authorizing and reviewing DAC user access privileges for operating level organization (OLO) 4390 was last updated in June 2013. As of April 7, 2017, one position number in the *DAC Procedure* was listed as the designated Access Control Custodian for OLO 4390 and authorized user access privileges. However, this position was moved to a different area within the Department and no longer required access as an Access Control Custodian. Additionally, we determined that one of the positions authorized as the Access Control Custodian was not documented in the *Procedure*. In response to our audit inquiry, Department management stated that the Director's Office in the Division of Accounting and Auditing would be completing a review of access prior to revision of the *DAC Procedure*. A similar issue was noted in our report No. 2017-089.
- The Central Accounting *Access Control Business Process Procedures* (*Central Procedures*) used for authorizing and reviewing CAC user access privileges was last updated in November 2013. As of April 6, 2017, one position number in the *Central Procedures* was listed as authorized for update access privileges to the Reconciliation File function as a Bureau of Vendor Relations position. However, this position was moved within the Department and no longer required access to this function.
- As of May 3, 2017, the Department's procedures for periodic review of user access privileges did not define the Statewide user access privileges for the DAC State Chief Financial Officer Files (SC) function and the related DAC SC Electronic Funds Transfer Authorization Inquiry Request (ET) mini-menu function. In response to our audit inquiry, Department management stated that a change request was implemented into the production environment on June 22, 2017, which incorporated an additional report containing the necessary information to review the ET mini-menu function in the DAC Statewide access review process. A similar issue was noted in our report No. 2017-089.

Up-to-date access review procedures facilitate the effective review of user access privileges. Additionally, periodic reviews of user access privileges reduce the risk that inappropriate access to programs and data may exist that could result in compromised data integrity.

Recommendation: We recommend that Department management ensure that FLAIR access review procedures are current and that the access privileges granted for all applicable FLAIR functions are reviewed.

[6] AST Rule 74-2.003(1)(a)6, Florida Administrative Code.

[7] Division of Accounting and Auditing, *System Access Control Policy*.

Finding 3: Change Management Controls

Effective change management controls over modifications to hardware and systems software ensure that only approved changes are implemented into the production environment. Department policy[8] requires all network device change requests to be evaluated by both the Network Services team and the Information Security Office to ensure the changes conform to current security best practices and OIT security policies.

As part of our audit, we evaluated 46 of the 260 change requests related to network devices that were implemented into the production environment between July 1, 2016, and March 30, 2017, to determine whether network device change requests were appropriately approved at all required levels prior to being implemented into the production environment. We noted that, for 4 of the 46 network device change requests evaluated, the approval of the Information Security Office was not documented as required.

Effective change management controls ensure that all hardware and systems software changes are appropriately documented to evidence that changes are approved. Without proper controls including approval, the risk is increased that erroneous or unauthorized changes may be implemented into the production environment.

Recommendation: We recommend that Department management improve change management controls to ensure that approvals are appropriately documented for all network device changes prior to implementation into the production environment.

Finding 4: Background Screenings

Effective security controls include the performance of security background screenings for new personnel and the periodic reperformance of screenings for existing personnel who are 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, as provided in State law,[9] each State agency must designate positions which, because of the special trust, responsibility, or sensitive location, require security investigations (i.e., background screenings). All persons and employees in such positions must undergo background screenings, including fingerprinting, as a condition of employment and continued employment.

Our audit procedures disclosed that as of May 5, 2017, the Department had not established a comprehensive policy related to background screenings that required the periodic reperformance of background screenings for existing personnel and contracted consultants in positions of special trust. However, the Department required new employees hired into a position of special trust to be screened as a condition of employment and that employees transferring to a position of special trust be screened if it had been more than 6 months since their last screening. Department management within the Division of Administration stated that a Departmentwide background screening policy was currently being developed.

[8] Office of Information Technology – OIT Operating Procedures, OIT-028, *Firewall Configuration Procedure*.

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

As part of our audit procedures, we evaluated background screening reports for 71 of the 223 BOSP and OIT employees in positions of special trust as of March 27, 2017. We also evaluated background screening reports for 5 of the 39 OIT consultants requiring background screening as a condition of providing services to the OIT as of April 28, 2017. Our audit procedures disclosed that:

- The required background screening for 1 employee in the OIT who was hired on July 9, 2012, had not been performed as of May 8, 2017. In response to our audit inquiry, Department management stated that the missing background screening was an oversight because, although the employee was assigned to a position of special trust within the OIT, the employee's position was funded by another Division.
- The background rescreening required due to 1 OIT employee's job transfer effective July 1, 2015, had not been performed as of July 26, 2017.
- The required background screenings for 3 of 5 selected consultants providing services to the OIT were not available. For 2 of the 3 consultants, OIT staff indicated that the background screenings were performed but the Department did not have evidence of the screenings. For the remaining consultant, who started work with the Department on April 24, 2017, the required background screening had not been performed as of May 18, 2017.

Without a comprehensive 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 recommend that Department management continue efforts to establish a comprehensive background screening policy and ensure the timely performance and reperformance of required background screenings for employees and consultants in positions of special trust, responsibility, or sensitive location.

Finding 5: Security Controls – Physical Security, Access Controls, User Authentication, Logging and Monitoring, and Configuration Management

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, access controls, user authentication, logging and monitoring, and configuration management 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 physical security, access controls, user authentication, logging and monitoring, and configuration management, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised. Similar findings related to physical security, user authentication, and configuration management were communicated to Department management in connection with our report No. 2017-089.

Recommendation: We recommend that Department management improve certain security controls related to physical security, access controls, user authentication, logging and monitoring, and configuration management 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 applicable findings included in our report No. 2017-089.

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 the IT operational audit for FLAIR from March 2017 through June 2017 and for Origami from August 2016 through November 2016 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.

The IT operational audit focused on evaluating selected IT controls relevant to financial reporting and applicable to FLAIR during the period July 2016 through June 2017 and selected actions subsequent thereto and selected IT controls applicable to Origami during the period July 2016 through November 2016.

The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2017-089.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

The 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 the 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 the 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 audits; 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.

The 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 the audit, we:

FLAIR

- Interviewed Department personnel and reviewed related documentation to obtain an understanding of:
  - Business process and data flows for FLAIR, including CAC and Payroll Component processing.
  - Logical access controls and the paths and methods for authenticating to FLAIR, FLAIR's underlying infrastructure, and the Department's network.
  - Configuration management processes for FLAIR, FLAIR's underlying infrastructure, and the Department's network.
  - Physical access controls for the Department's Data Center and OIT secure areas.
  - Background screening processes for Department employees and consultants employed in positions of special trust.
  - The strategic IT planning process and status of the Florida PALM project.
- Obtained an understanding of the FLAIR Payroll Component changes required to the fund identifier for the pension allocation and determined whether the changes were authorized, sufficiently tested, and approved prior to implementation on January 23, 2017.
- Observed on March 24, 2017, and on March 27, 2017, the Department's physical security control processes implemented for OIT secure areas to determine whether access to sensitive areas and IT resources were appropriately restricted.
- Evaluated user authentication controls related to the Department's IT infrastructure supporting FLAIR.
- Evaluated the effectiveness of the Department's logging and monitoring controls related to FLAIR.
- Evaluated the logical design, appropriateness, and administration procedures for logical access privileges to FLAIR, FLAIR's underlying infrastructure, and the Department's network. Specifically, we evaluated:
  - The appropriateness of access privileges for 20 of the 183 users with update access privileges to 1 or more of 16 key CAC FLAIR functions, granted during the period July 1, 2016, through February 28, 2017.

- The appropriateness of access privileges for the 36 users with update or inquiry access privileges to three confidential CAC electronic funds transfer (EFT) functions, EFT Authorization File; EFT Payment Detail; and EFT Bank Title file, granted during the period July 1, 2016, through February 28, 2017.
- The appropriateness of access privileges for the 17 OIT users with CAC access during the period July 1, 2016, through February 28, 2017.
- The appropriateness of access privileges for the 29 users with update or override access privileges to 1 or more of 40 key functions within the Payroll Component of FLAIR as of February 28, 2017.
- The timely deactivation of CAC access privileges for the 12 former employees who separated from the Department during the period July 1, 2016, through March 31, 2017, with CAC access.
- The timely deactivation of Payroll Component Statewide access privileges for the 10 former employees who separated from the Department during the period July 1, 2016, through March 31, 2017.
- The appropriateness of access privileges for all network user accounts with administrative access privileges as of March 27, 2017, and help desk and desktop support accounts as of April 3, 2017.
- The appropriateness of access for local user accounts with administrative privileges on Department workstations in 21 Organizational Units in the network domain as of April 23, 2017.
- The appropriateness of access privileges for 14 user accounts with administrative access privileges used to administer network devices as of April 25, 2017.
- The appropriateness of access privileges for the 13 user accounts with administrative access to the Security Incident and Event Management (SIEM)[10] environment as of April 14, 2017.
- The appropriateness of access privileges assigned to the 8 OIT Payroll Component programmers as of May 9, 2017, to determine whether the access privileges granted promoted an appropriate separation of duties between the development of Payroll Component changes and the implementation of Payroll Component changes into the production environment.

- Evaluated the effectiveness of periodic access review processes for FLAIR and the underlying infrastructure. Specifically, we evaluated the adequacy of periodic reviews of user access privileges:
  - To the network and related environments.
  - Of CAC users and users with Statewide access to the Payroll Component of FLAIR.
  - To the Common Business-Oriented Language (COBOL) environment.
  - To DAC State CFO Files (SC) function and the related DAC SC ET mini-menu function.
  - To DAC utilized by the Division of Accounting and Auditing (OLO 4390).
- Evaluated the appropriateness of physical access controls implemented at the Department's Data Center to protect its IT resources and data. Specifically, we evaluated:

[10] Security Incident and Event Management (SIEM) is the process of identifying, monitoring, recording, and analyzing security events or incidents within a real-time IT environment.

- The appropriateness of physical access privileges to the Data Center and OIT secure areas for the 87 active key cards as of March 30, 2017.
- Adequacy of the quarterly access reviews of physical access privileges to the Data Center and OIT secure areas for July 2016 and April 2017.

- Evaluated the effectiveness of Department's procedures for reviewing FLAIR Payroll Component program changes prior to implementing the changes into the production environment. Specifically, we evaluated 30 program changes made between February 2, 2017, and May 10, 2017, to verify that a review independent of the individuals responsible for the program code changes was conducted prior to implementing the Payroll Component changes into the production environment.
- Evaluated the effectiveness of change controls for 46 of the 260 network device changes implemented into production during the period July 1, 2016, through March 30, 2017.
- Evaluated the effectiveness of firewall firmware patch management controls for 4 of the 15 physical firewall devices as of April 19, 2017.
- Evaluated the timeliness of background screenings for 71 of the 223 BOSP and OIT employees in positions of special trust as of March 27, 2017, and for 5 of the 39 OIT consultants requiring background screenings as a condition of providing services to the OIT as of April 28, 2017.

Origami

- Interviewed Department personnel and reviewed Origami-related documentation to obtain an understanding of:
  - Origami background information including the system's purpose or goals involving financial, operations, and compliance requirements.
  - Origami data and business process flows, including key sources of data input (including interfaces), key application transactions and processes, and key types of application data output.
  - Origami computing platform, including the applicable hardware, operating system, database management system, and security software.
  - User account management processes for authorizing, creating, modifying, and revoking Origami user accounts.
  - The Department's change management processes, including policies and procedures for application change control and the system development lifecycle methodology applicable to Origami.
  - Cryptographic tools and related user guides, as of September 26, 2016, used in Origami to protect sensitive or privileged information.
  - List of available reports as of November 2, 2016, that the Department developed to run on an as needed basis to assist in monitoring Origami activity.
- Evaluated the effectiveness of application access authorization and appropriateness controls for 40 of the 191 users with active Origami access privileges as of September 15, 2016, to determine whether the access privileges granted were documented, authorized, and appropriate.
- Evaluated the effectiveness of Origami change management controls related to the authorization, testing, approval, and implementation of application program changes into the production environment. Specifically, we evaluated the six application program changes requested by the Department during the period July 2016 through September 2016 and completed by the vendor that were in addition to the contractual obligations for Origami.

- Reviewed the documentation of the June 2016 quarterly periodic review of Origami access appropriateness of internal and external users (i.e., Department users, State agencies, universities, and third-party adjusters) to determine whether the quarterly periodic reviews of Origami access appropriateness were being performed and documented.
- Evaluated the Origami Active User Listing as of September 30, 2016, to determine whether the access changes requested by a supervisor for three external users during the June 2016 quarterly review were changed as requested.
- Reviewed the September 30, 2016, Origami Active User Listing used to monitor user activity and last logon dates on October 4, 2016, to determine whether the report captured the last logon dates.
- Evaluated Origami application and related IT resources authentication and identification controls as of September 14, 2016.
- Inspected Origami user activity reports on September 28, 2016, for an internal user for the period August 31, 2016, through September 28, 2016, and an external user for the period August 31, 2016, through September 26, 2016, to verify that the Department has the capability to identify what actions specific user IDs perform within the system for any given time period.
- Evaluated the effectiveness of 10 of the 35 custom on-line edits the Department requested the vendor to build into Origami, 7 of which were specific to the processes related to Workers' Compensation as of October 25, 2016, to determine whether the edits were in place and working as intended.
- Reviewed the Origami Conversion Plan and verification documentation on November 2, 2016, to determine whether the conversion process from the previous risk management information system to Origami was controlled and reviewed.
- Examined Department records and performed inquiries of Department personnel in October 2016 related to Origami error handling procedures for uploaded data to determine whether the Department had adequately designed and implemented controls for identifying, investigating, and correcting Origami data input errors.
- Examined on October 18, 2016, automatic e-mail notifications and the Origami log generated on September 20, 2016, to determine whether the Department had designed and implemented Origami controls for identifying processing errors or failures.
- Evaluated on October 14 and 17, 2016, controls over Origami interfaces with workers' compensation provider systems.
- Examined Department records and performed inquiries of Department personnel during our audit period related to contingency planning procedures to determine whether the Department was adequately addressing contingency planning controls for the Origami system, both on the vendor side as well as on the Department side.
- Examined Department records on November 2, 2016, related to a file that was deleted in October 2016 that the Department was able to restore from Origami records.
- Examined Department records and performed inquiries of Department personnel related to monitoring the status of sub-annual claim cost reports required to be submitted to the Division of Workers' Compensation[11] by reviewing the Origami-generated notices pertaining to sub-annual claim cost reports as of October 2016.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.

[11] Department of Financial Services Rule 69L-56.3013(4)(a), Florida Administrative Code.

- 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 audits.



Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

October 20, 2017

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) and Origami Risk Insurance Management System (Origami)*.

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

Sincerely,

Jimmy Patronis
Chief Financial Officer

Enclosure

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

Florida Accounting Information Resource Subsystem (FLAIR) and Origami Risk Insurance Management System (Origami) Information Technology Operational Audit

DEPARTMENT OF FINANCIAL SERVICES' RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Appropriateness of Access Privileges

The access privileges for some FLAIR users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for assigned job duties.

Recommendation: We recommend that Department management limit user access privileges to FLAIR to promote an appropriate separation of duties and to restrict users to only those access privileges and functions necessary for the users' assigned job duties. In doing so, Department management should ensure that the FLAIR access privileges of former employees are timely deactivated. We also recommend that Department management ensure that, prior to implementation into the production environment, program changes are reviewed by an individual not associated with the program changes.

Response: We concur.

The Division of Accounting and Auditing (A&A) is updating access control procedures to FLAIR to promote an appropriate separation of duties and to restrict users to only the access necessary for the users' assigned duties. The Division will also improve controls to ensure that user accounts are timely deactivated.

The Office of Information Technology (OIT) is aware of the remediation responsibilities and will coordinate the effort over the next 12 months. The concerns are expected to be remediated or otherwise compensated for. FLAIR access control procedures will be updated to address separation of duty concerns and to ensure separated user accounts are timely deactivated, and to remediate the OIT program file change concern. The Compliance Office will be tracking this concern to ensure that the reviewer roles are appropriate and separate, and automated email access review requests will be tracked through our ticketing system.

Expected Completion Date for Corrective Action: November 1, 2018

Finding No. 2: Periodic Review of User Access Privileges

The Department's procedures and processes for assigning FLAIR user access privileges and conducting periodic reviews of these privileges need improvement to ensure access privileges assigned to users remain appropriate.

Recommendation: We recommend that Department management ensure that FLAIR access review procedures are current and that the access privileges granted for all applicable FLAIR functions are reviewed.

Response: We concur.

The Division of Accounting and Auditing (A&A) is updating OLO 4390 DACA Access Control Business Process Procedures and Central Accounting Access Control Business Process Procedures used for authorizing and reviewing user access privileges.

The Office of Information Technology is aware of the remediation responsibilities and will coordinate the effort over the next 12 months. The concerns are expected to be remediated or otherwise compensated for. The listed access control procedures will be reviewed and revised to address the associated concerns. Additionally, a report will be generated containing the access changes and will be reviewed weekly checking for anomalies and/or inappropriate changes. The Compliance Office will be tracking this concern to ensure that the access review emails are being generated and responded to, and the access change report is accurate and configured to be automatically generated and sent to the correct group in A&A. The corresponding procedure for reviewing the access change report will also be generated.

Expected Completion Date for Corrective Action: November 1, 2018

Finding No. 3: Change Management Controls

Change management controls related to hardware and systems software changes for network devices related to FLAIR need improvement to ensure that only approved hardware and systems software changes are implemented into the production environment.

Recommendation: We recommend that Department management improve change management controls to ensure that approvals are appropriately documented for all network device changes prior to implementation into the production environment.

Response: We concur. The Office of Information Technology will create a stronger process to ensure change request approvals are properly documented.

Expected Completion Date for Corrective Action: November 1, 2018

Finding No. 4: Background Screenings

The Department had not established a comprehensive policy for the performance of background screenings of employees and consultants in positions of special trust. Additionally, required background screenings for employees and consultants were not always performed.

Recommendation: We recommend that Department management continue efforts to establish a comprehensive background screening policy and ensure the timely performance and reperformance of required background screenings for employees and consultants in positions of special trust, responsibility, or sensitive location.

Response: We concur. The Division of Administration will continue its efforts to establish a comprehensive background screening policy. Background screenings for the two OIT employees and one of the three consultants cited in Finding No. 4 have been completed. The other two consultants are no longer under contract with the Department.

Expected Completion Date for Corrective Action: December 31, 2017

Finding No. 5: Security Controls – Physical Security, Access Controls, User Authentication, Logging and Monitoring, and Configuration Management – (OIT)

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

Response: As of October 10, 2017, the Office of Information Technology (OIT) implemented corrective action to address several of the physical security, access control, and authentication concerns. The OIT will evaluate the additional security concerns and, where appropriate, implement additional controls.

Expected Completion Date for Corrective Action: November 1, 2018