STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-077
December 2017

DEPARTMENT OF MANAGEMENT SERVICES

Integrated Retirement Information System (IRIS)

Sherrill F. Norman, CPA
Auditor General

Secretary of the Department of Management Services

The Department of Management Services is established by Section 20.22(1), Florida Statutes. The Head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, the following individuals served as Department Secretary:

Erin Rock	From April 1, 2017
Chad Poppell	Through March 31, 2017

The team leader was Chrystal Temples, 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 MANAGEMENT SERVICES

Integrated Retirement Information System (IRIS)

SUMMARY

This operational audit of the Department of Management Services (Department) focused on evaluating selected information technology controls applicable to the Integrated Retirement Information System (IRIS) and included a follow-up on the findings in our report No. 2017-101. Our audit disclosed the following:

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

BACKGROUND

The Department of Management Services (Department) uses the Integrated Retirement Information System (IRIS) to support the Department's business processes related to the Florida Retirement System (FRS). The business processes supported by IRIS include member enrollment and the maintenance of member information, receipt of contributions from FRS participating employers, tracking of members' employer and employee contributions and service histories, calculation of retirement benefits, and the issuance of the retiree payroll file processed by the Department of Financial Services. IRIS is also used to process and maintain FRS Investment Plan payroll and data. The FRS Online application is an extension of IRIS and uses Internet technology to provide information and services to members, employers, and retirees.

Application and database administration support for IRIS and the FRS Online application, as well as support for the Division of Retirement's (Division's) day-to-day information technology (IT) needs, were outsourced by the Department to Deloitte Consulting Limited Liability Partnership (Deloitte). Deloitte is responsible for providing the Division's IT functions, which include network and application security administration, application programming, and database administration functions.

FINDINGS AND RECOMMENDATIONS

Finding 1: Appropriateness of Access Privileges

Effective access controls include measures that restrict user 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. As discussed in the ***BACKGROUND*** section of this report, Deloitte is responsible for IRIS application security administration, application programming, and database administration functions.

Our audit procedures disclosed some inappropriate and unnecessary access privileges to IRIS data and IT resources. Specifically, during the 2016-17 fiscal year:

- The two IRIS security administrators had full update access privileges to production libraries. Additionally, the security administrators had inappropriate access to IRIS as end-users for part of the 2016-17 fiscal year.
- Two of the nine programmers had update access to the production environment resulting in an inappropriate separation of duties.
- Three database administrators were also application programmers. The combination of the access privileges granted to perform the duties for these roles resulted in an inappropriate separation of duties. Additionally, as of June 23, 2017, the access for the four database administrators allowed them to change the log that showed who moved the FRS Online application changes and what FRS Online application changes were moved into the production environment.

In response to audit inquiry, Department management stated that the update access privileges were appropriately updated for one security administrator in January 2017 and in April 2017 for the other security administrator. Additionally, in response to audit inquiry, Department management stated that the FRS Online application change logs were reviewed quarterly for the security administrators and database administrators and that the review process is being reviewed to identify other changes that may need to be made. Nevertheless, appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. Similar findings were noted in prior audits, most recently in our report No. 2017-101.

Recommendation: We recommend that Department management limit user access privileges to IRIS data and IT resources to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.

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. 2017-101.

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 IT operational audit from June 2017 through October 2017 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 IT controls applicable to IRIS during the period July 2016 through June 2017 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input, processing, output, master data, and interface controls and selected application-level general controls over access controls and logging

pertaining to configuration management as related to the audit findings disclosed in our report No. 2017-101. The overall objectives of the audit were:

- To evaluate the effectiveness of selected IT controls in achieving management's control objectives 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. 2017-101 that were applicable to the scope of this audit.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel and reviewed IRIS-related documentation to obtain an understanding of the IT computing platform for the IRIS application and to identify the applicable hardware and software such as servers, operating systems, and security software related to the application.
- Evaluated IRIS transaction data input controls related to the CO180 – Payroll Error Report. Specifically, we:
    - Reviewed the *Florida Retirement System Employer Handbook* to gain an understanding of the Department's process for correcting account and transaction errors.

- Reviewed the *Contribution Section Procedures – Payroll Processing Guidelines* and a *Bureau of Enrollment and Contributions* narrative to gain an understanding of the Department's process for correcting account and transaction errors.
- Reviewed the Batch Log screens and the *Load Error List* report for evidence that error reports were created and monitored.
- Reviewed the *Payroll Status* report for evidence that the Contributions Section Administrator monitored the status of employer retirement files received or whether such files are missing.
- Reviewed an example of a View Payroll Errors (CO180*)* screen and the *(AM311) Pending Error Statistic Report* for evidence that the Contribution Section staff monitored the timeliness of processing of edit errors by Retirement Specialists.
- Reviewed an example of an Adjust Unbalanced Non-State Agencies (CO150) screen for evidence that Contribution Section staff monitored employers with out-of-balance retirement reports.
- Reviewed the Notification of Unbalanced Payrolls e-mail for evidence that the Retirement Specialist provided e-mails allowing the Contributions Section staff to monitor the resolution status of employer unbalanced conditions.
- Reviewed Department controls to evaluate whether contribution transaction errors were investigated, corrected, and resubmitted promptly and accurately.
- Reviewed two error transactions related to the Investment Plan listed on the CO180 file during the period July 1, 2016, through June 30, 2017, with variances greater than $0.01 that were approved more than 5 business days from the date of correction for evidence that the error transactions were promptly investigated and timely corrected.

- Evaluated IRIS user access controls related to user authorization and appropriateness. Specifically, we:
  - Reviewed the *IRIS Security Procedures, Access Authorization, Deactivation, and Periodic Reviews* document for an understanding of how access to IRIS would be established.
  - Reviewed the Department's process for updating the contribution rates table to gain an understanding of how the table was updated and what IRIS roles, if any, had table update abilities.
  - Reviewed the *Procedure for the Reviewing the FRS Online Upload Log* to gain an understanding of which users would have access to the log and what the review included.
  - Reviewed IRIS user roles to evaluate whether application users had view-only access to the contribution rates update table.
  - Reviewed Employee Notification Forms used to establish access to IRIS to evaluate whether forms were on file and contained supervisory approval for 25 of 236 IRIS users as of June 22, 2017.
  - Reviewed the access for security administrators, application programmers, and database administrators as of June 23, 2017, to evaluate whether the access granted was appropriate for the users' job duties.
  - Reviewed the deactivations of access for 6 of the 56 employees who separated from Department employment during the period July 1, 2016, through June 30, 2017, to evaluate whether the access was timely deactivated.
  - Reviewed the Department's periodic review processes and procedures to evaluate whether periodic reviews of user access were performed by the Department. Specifically, on April 24, 2017, we reviewed the review processes conducted for 18 work units to evaluate

whether each work unit manager was sent a request for periodic review, and to evaluate whether each work unit manager reviewed, approved, and reported to Department management that user access privileges were accurate and appropriate.

- o Reviewed all IRIS service accounts to evaluate whether controls were in place to prevent interactive login.

- Evaluated IRIS database identification and authentication controls.
- Evaluated the auditing and monitoring controls related to IRIS IT resources.
- 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

FLORIDA DEPARTMENT of management SERVICES
We serve those who serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
Tel: 850-488-2786 | Fax: 850-922-6149

Rick Scott, Governor

Erin Rock, Secretary

December 20, 2017

Ms. Sherrill F. Norman, CPA
Auditor General
Suite G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to subsection 11.45(4)(d), Florida Statutes, this is our response to your report, ***Department of Management Services- Information Technology Operational Audit of the Integrated Retirement Information System (IRIS)***. Our response corresponds with the finding and recommendation related to the Department of Management Services contained in the preliminary and tentative finding report.

If further information is needed concerning our response, please contact Dawn E. Case, Inspector General, at 488-5285.

Sincerely,

Erin Rock
Secretary

ER/nw

Enclosure

cc: David Zeckman, Chief of Staff
Heather Best, Senior Director of Executive Operations
Elizabeth Stevens, Director of the Division of Retirement
Shirley Beauford, Assistant Director of the Division of Retirement
Bob Ward, Chief Information Officer
Eric Miller, Chief Inspector General
Dawn Case, Inspector General
Yolanda Lockett, Audit Director

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name
12/20/17		2017 IT Operational Audit of IRIS

Contact Person	Title	Phone No.	Email Address
Elizabeth Stevens	Division Director	(850) 778-4400	Elizabeth.Stevens@dms.myflorida.com

Activity	Accountability		Schedule
	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
Appropriateness of Access Privileges	Division of Retirement	Yes	2/28/18

Finding		Finding Category
No.	1	
Date	12/20/17	

Finding	The access privileges for some IRIS users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for their assigned job duties.
Recommendation	We recommend that Department management limit user access privileges to IRIS data and IT resources to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.
Management/Agency Response	The Department concurs with the finding and recommendation. The Department will develop a plan of action to further limit user access privileges where possible. If separation of duties is not feasible, efforts will be made to enhance our compensating controls. The plan will include: (1) assessing job duties assigned to IT staff that have application deployment responsibilities, (2) evaluating the use of log reviews to mitigate any remaining separation of duties issues, or (3) the implementation of other compensating controls should separation of duties not be fully achieved. The Department expects to have the plan finalized by Feb. 28th and will begin implementation afterward.

Status Update-6 months	
☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	

Status Update-12 months	
☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	

Status Update-18 months	
☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	