STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-018
September 2015

DEPARTMENT OF MANAGEMENT SERVICES

Division of Retirement
Integrated Retirement Information System (IRIS)

Sherrill F. Norman, CPA
Auditor General

Secretary of Management Services

Section 20.22, Florida Statutes, created the Department of Management Services. The head of the Department of Management Services is the Secretary of Management Services who is appointed by the Governor and subject to confirmation by the Senate. The following individuals served as Secretary during the period of this audit:

Chad Poppell	From December 22, 2014
Craig J. Nichols	Through December 16, 2014

The team leader was Earl M. Butler, CISA, CFE, 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:

www.myflorida.com/audgen

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

Division of Retirement
Integrated Retirement Information System (IRIS)

SUMMARY

Section 121.1905, Florida Statutes, created the Division of Retirement (Division) within the Department of Management Services (Department). The Division administers the Florida Retirement System (FRS) Pension Plan along with various other retirement-related programs and funds. The Division uses the Integrated Retirement Information System (IRIS) to support the functions required to provide retirement services.

This operational audit focused on evaluating selected information technology (IT) controls applicable to IRIS and included a follow-up on the findings included in our report No. 2013-042. As summarized below, the audit disclosed areas in which improvements in IRIS IT controls and operational processes were needed.

Finding 1: Four IRIS database accounts continued to be assigned access privileges that should be granted only to database administrators.

Finding 2: Some generic database accounts continued to be active and were not expired or locked.

Finding 3: Access privileges granted to IRIS were not always appropriately authorized and documented.

Finding 4: Certain security controls related to IRIS database user authentication and logging for IRIS-related IT resources needed improvement.

BACKGROUND

The Division of Retirement (Division) uses the Integrated Retirement Information System (IRIS) to support the Division's business processes related to the retirement life cycle of Florida Retirement System (FRS) covered employees. The business processes supported by IRIS include the enrollment and maintenance of members in the system; tracking of participating employer contributions, employee contributions, and service histories throughout the members' careers; calculation of retirement benefits; and the issuance of the retiree payroll file that is processed by the Department of Financial Services. IRIS is also used to process and maintain FRS Investment Plan payrolls and data. The FRS Online application is an extension of IRIS that 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'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 access to sensitive system resources, such as database management systems, to individuals or processes that have a legitimate need for accomplishing a valid business purpose. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, and disclosure.

As discussed in the ***BACKGROUND*** section of this report, Deloitte is responsible for IRIS security and database administration functions. In our report No. 2013-042, Finding No. 1, we disclosed that five database accounts were assigned system privileges that were usually granted only to database administrators. As part of our follow-up procedures, we reviewed the five database accounts to determine whether the accounts continued to be assigned the inappropriate privileges. We noted that four of the database accounts continued to be assigned system privileges that should be granted only to database administrators.

Subsequent to our audit inquiry, Deloitte staff removed the inappropriate access privileges from one database account and locked two of the database accounts so that the accounts could not be used. In addition, Deloitte staff indicated that they would investigate the feasibility of removing the privileges from the fourth database account. Allowing the database accounts to retain inappropriate system privileges increases the risk of unauthorized modification, loss, or disclosure of IRIS data and IRIS-related IT resources.

Recommendation: Department management should require Deloitte management to improve access controls to ensure that system privileges are appropriately granted only to database administrators.

Finding 2: Generic Database Accounts

Effective access controls include a process for the unique identification and authentication of system users. The unique identification and authentication of system users allows management to affix responsibility for system activity to a specific individual.

In our report No. 2013-042, Finding No. 2, we disclosed that Deloitte IT staff used four generic user identification codes (user IDs) (i.e., database accounts) to access the IRIS database and used one generic user ID (i.e., database account) to move IRIS application programs into the production environment. As part of our follow-up procedures, we reviewed the five generic database accounts and made inquiries of Deloitte management. Our review disclosed that individual inquiry and update database accounts for the IT staff to use in place of generic database accounts had been established by Deloitte management. However, although the IT staff had been assigned individual database accounts, we noted that four of the five previously identified shared generic database accounts were not expired or locked and continued to be active database accounts.

On March 3, 2015, subsequent to our audit inquiry, Deloitte management locked two of the four generic database accounts as stated previously in Finding 1 of this report. During the period of our audit, we

also noted that Deloitte management had implemented logging of the other two active generic database accounts used to manage objects. Allowing generic database accounts to remain active without establishing responsibility for actions taken while using the accounts increases the risk of unauthorized modification, loss, or disclosure of IRIS data and IRIS-related IT resources.

Recommendation: Department management should require Deloitte management to ensure that all generic database accounts are expired or locked.

Finding 3: Access Authorization Documentation

Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. Additionally, appropriately maintained access authorization documentation facilitates the complete and accurate assignment of user access privileges.

We requested access authorization documentation for 16 active IRIS user accounts with update access privileges to the IRIS application as of March 2, 2015, to determine whether the access privileges granted to IRIS were appropriately authorized and documented. Our review of the access authorization documents for the 16 user accounts provided to us by the Department disclosed that 4 of the access authorization documents either did not authorize access privileges to IRIS or authorized access privileges to IRIS but did not specify the IRIS role. Specifically, we noted that:

- The access authorization documentation for 2 users did not specify authorization for access privileges to IRIS.
- The access authorization documentation for 2 users specified authorization for access privileges to IRIS but did not specify the IRIS roles.

Subsequent to our audit inquiry, Department management notified Deloitte on June 15, 2015, that no changes, additions, or deletions to IRIS privileges were to be made without possession of the proper authorization documentation. By not appropriately documenting authorizations for IRIS access privileges, Department management's assurances that the access privileges granted to IRIS are authorized by management and do not exceed what is necessary for the accomplishment of assigned user job duties may be limited.

Recommendation: Department management should ensure that all access privileges granted to IRIS are appropriately documented as authorized by management and that such documentation specifies the IRIS roles.

Finding 4: Security Controls – User Authentication and Logging

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 user authentication and logging for IRIS-related IT resources needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising IRIS data and IRIS-related IT resources. However, we have notified appropriate Department management of the specific issues. A similar finding regarding user authentication was communicated to Department management in connection with our report No. 2013-042. Without adequate security controls related to user

authentication and logging for IRIS-related IT resources, the risk is increased that the confidentiality, integrity, and availability of IRIS data and IRIS-related IT resources may be compromised.

Recommendation: Department management should improve certain security controls related to user authentication and logging for IRIS-related IT resources to ensure the continued confidentiality, integrity, and availability of IRIS data and IRIS-related 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. 2013-042.

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 February 2015 through May 2015 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 2014 through May 2015 and selected actions through June 15, 2015. The audit included selected business process application controls relating to employer-entered data and reconciliation processes used in verifying reports, such as the Accumulated Benefit Obligation and the Contribution Summary Information reports, and controls relating to validation processes for the data the Division provides to the Department's actuary. The audit also included application-level general controls relating to IRIS application and database access and IRIS program change management controls related specifically to the deficiencies disclosed in our report No. 2013-042. 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, deficiencies disclosed in our report No. 2013-042.
- 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 ineffective or inefficient 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.

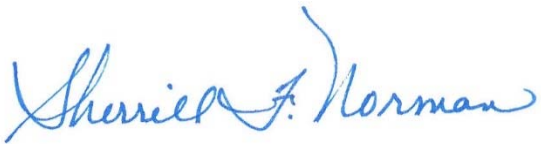
In conducting this audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the data and business process flows for the application with emphasis on employer-entered data and reconciliation processes used in verifying reports and validation processes for the data provided to the Department's actuary.
- Obtained an understanding of the IT computing platform for the application including identification of the applicable hardware, operating system and version, database management system and version, and security software and version related to the application.
- Evaluated the effectiveness of data input, processing, and output procedures to ensure that transaction data was complete, accurate, valid, and confidential; specifically related to employer-entered data and reconciliation processes used in verifying reports such as the Accumulated Benefit Obligation and the Contribution Summary Information reports.
- Evaluated the effectiveness of data input, processing, and output procedures to ensure that transaction data was complete, accurate, valid, and confidential; specifically related to validation processes for the data provided to the actuary.
- Evaluated the effectiveness of application access controls to ensure that IRIS users were appropriately identified and authenticated and that access privileges granted were appropriately authorized, restricted, and periodically reviewed for appropriateness. Specifically, we reviewed 16 of 169 IRIS user IDs as of March 2, 2015, to determine whether the IRIS access privileges granted were authorized, documented, and appropriate based on assigned job duties.

- Evaluated the effectiveness of procedures for disabling the IRIS user access privileges of former Department employees who had terminated employment.
- Evaluated the effectiveness of individual user identification and authentication controls.
- Evaluated the effectiveness of database access controls for access authorization and appropriateness to that resource owners had identified and authorized access privileges and periodically reviewed those access privileges for continued appropriateness.
- Evaluated the effectiveness of the IRIS program change management process. Specifically, we reviewed 7 of 69 System Investigation Requests that were closed between July 1, 2014, and March 10, 2015, to determine whether changes were authorized, tested, approved, documented, and appropriately moved into the production environment.
- Evaluated the logging of certain actions on the production servers.
- 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

Chad Poppell, Secretary

September 3, 2015

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

Dear Ms. Norman:

Pursuant to section 11.45(4)(d), Florida Statutes, the attached document represents our responses to your report, **Department of Management Services- Information Technology Operational Audit of the Integrated Retirement information System (IRIS)**. Our responses correspond with the order of the findings and recommendations in the report.

If further information is needed concerning our response, please contact Walter Sachs, Inspector General, at 488-5285.

Sincerely,

Chad Poppell
Secretary

CP/yl

Enclosure

cc: Ben Wolf, Chief of Staff
Darren Brooks, Deputy Secretary, Workforce Operations
Dan Drake, Director, Division of Retirement
Elizabeth Stevens, Assistant Director, Division of Retirement
Bob Ward, Chief Information Officer
Walter Sachs, Inspector General
Yolanda Lockett, Audit Director

Preliminary and Tentative Finding Report Status

Status Date	Report No.	Report Title
9/3/2015	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Application Security	IT	Yes	8/31/2015

Finding	
No.	1
Date	9/3/2015

Appropriateness of Access Privileges

Finding	Four IRIS database accounts continued to be assigned access privileges that should be granted only to database administrators
Recommendation	Department management should require Deloitte management to improve access controls to ensure that system privileges are appropriately granted only to database administrators.
Response/Action Plan	The Division believes it fully complied with the previous report by taking steps to eliminate or limit the use of these accounts and modifying the access privileges without adversely impacting operations based on the prior audit. However, the Division supports the current recommendation and has implemented additional measures. The Division has either locked or adjusted the access privileges of these accounts. In addition, the Division will enhance its monthly review of database access privileges to verify that only database administrators and approved system accounts have the appropriate access privilege granted. The enhanced monthly review process will be implemented by August 31, 2015.
Status Update-6mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	
Status Update-12mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	
Status Update-18mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	

Preliminary and Tentative Finding Report Status

Status Date	Report No.	Report Title
9/3/2015	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Security	IT	Yes	9/30/2015

Finding		
No.	2	Generic Database Accounts
Date	9/3/2015	
Finding		Some generic database accounts continued to be active and were not expired or locked.
Recommendation		Department management should require Deloitte management to ensure that all generic database accounts are expired or locked.
Response/Action Plan		The Division believes it fully complied with the previous report by taking steps to either discontinue the use of or implement logging on the accounts needed to manage objects. However, the Division supports the recommendation that additional measures can be implemented. In addition to the logging, the Division will make changes to the deployment processes for both developers and DBAs to enable deployments from DBA accounts. This will allow for locking generic database accounts. The Division will also enhance its monthly review of access privileges by reviewing all active database accounts that are not IRIS end-user accounts to ensure that generic accounts are expired or locked. These processes will be implemented by September 30, 2015.

Status Update-6mo	
☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete	

Status Update-12mo	
☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete	

Status Update-18mo	
☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete	

Preliminary and Tentative Finding Report Status

Status Date	Report No.	Report Title
9/3/2015	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Security		No	9/3/2015

Finding	
No.	3
Date	9/3/2015

Finding	Access Authorization Documentation
Finding	Access privileges granted to IRIS were not always appropriately authorized and documented.
Recommendation	Department management should ensure that all access privileges granted to IRIS are appropriately documented as authorized by management and that such documentation specifies the IRIS roles.
Response/Action Plan	All persons with IRIS access have the appropriate IRIS access. However, the Divison of Retirement concurs with this finding in that the authorization of appropriate access was not always properly documented. The Division has verified current processes and implemented process changes to ensure that access privileges granted to IRIS are appropriately documented as authorized by management and that such documentation specifies the IRIS role code. The recently revised Security Guidelines Manual (rev. July 2015), includes the policy and procedure for updating user access privileges in IRIS. As noted in the audit findings and recommendations, Division management notified the IT Operations and Maintenance (O & M) vendor (Deloitte), on June 15, 2015, that no changes, additions or deletions to IRIS privileges should be made without the proper authorization documentation. This document is internally referred to and titled the Employee Notification form. This is a multi-purpose form that documents and initiates employee related actions such as; new hires, terminations, promotions, location information, assigned equipment and resources, network access requests, building access and other information. Subsequent to the notification to the IT O & M vendor, the Employee Notification form was updated to include drop-down boxes to provide the role codes for managers to select from when initiating role code changes, additions or deletions in IRIS for their staff. A 'NA' (not applicable) check box was also added to be used if a particular employee action does not require an IRIS role code change. In addition to this, a listing of all of the role codes and definitions and a listing of role codes by position were provided to division managers and supervisors. In order to provide an additional level of review of assigned role codes and ensure role codes are current and appropriate, the Employee Database was modified to include information for assigned role codes for each position. Monthly reports will be run from the Employee Database and matched against the IRIS system information to verify that staff have appropriate role codes assigned in IRIS. Any discrepancies will be resolved on a monthly basis.
Status Update-6mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete	
Status Update-12mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete	
Status Update-18mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete	

Preliminary and Tentative Finding Report Status

Status Date	Report No.	Report Title
9/3/2015	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Security	IT	Partially	9/3/2015

Finding		
No.	4	Security Controls -- User Authentication and Logging
Date	9/3/2015	
Finding		Certain security controls related to IRIS database user authentication and logging for IRIS-related IT resources needed improvement.
Recommendation		Department management should improve certain security controls related to user authentication and logging for IRIS-related IT resources to ensure the continued confidentiality, integrity, and availability of IRIS data and IRIS-related IT resources.
Response/Action Plan		The Division believes it fully complied with the previous report by taking steps to improve user authentication controls based on the prior audit. However, the Division supports the current recommendation and will implement additional measures to further improve these security controls. In addition, the Division agrees to improve its logging procedures related to IRIS. The AG reports these conditions in a separate confidential document. In order to prevent compromising the confidentiality of the document, the Division has not responded directly to the recommendation.
Status Update-6mo		☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete
Status Update-12mo		☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete
Status Update-18mo		☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending ☐ Complete