STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-101
January 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, Chad Poppell served as Department Secretary.

The team leader was 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:

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

Integrated Retirement Information System

SUMMARY

This operational audit of the Department of Management Services (Department) focused on evaluating selected information technology (IT) controls applicable to the Integrated Retirement Information System (IRIS) and included a follow-up on the findings included in our report No. 2016-018. Our audit disclosed the following:

Finding 1: Complete and accurate IRIS access authorization documentation was not maintained, thereby limiting management's assurance that IRIS user access privileges were authorized and appropriately assigned.

Finding 2: 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.

Finding 3: The Department did not have procedures for timely deactivating IRIS accounts for users who no longer required access and did not timely deactivate the IRIS accounts for some users.

Finding 4: Department procedures did not ensure the timely and effective review of the appropriateness of user access privileges granted to IRIS.

Finding 5: Some service accounts inappropriately allowed interactive log-on increasing the risk that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

Finding 6: Certain security controls related to user authentication and monitoring for IRIS-related IT resources need improvement to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.

BACKGROUND

The Department uses the Integrated Retirement Information System (IRIS) to support the Department's business processes relating to the retirement of employees covered by the Florida Retirement System (FRS). The business processes supported by IRIS include the enrollment and maintenance of members in the system, tracking of members' employer contributions and services histories throughout their 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 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: Access Authorization Documentation

Agency for State Technology (AST) rules[1] require each agency to manage identities and credentials for authorized devices and users and establish control measures that address responsibilities of information stewards that include administering access to systems and data based on the documented authorizations and facilitate periodic review of access rights with information owners. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges authorized by management. Additionally, appropriately maintained access authorization documentation facilitates the complete and accurate assignment of user access privileges.

The Department uses access authorization forms for granting IRIS user access privileges. To determine whether the IRIS access privileges granted were authorized and appropriately assigned, we requested for our examination access authorization forms for 25 of the 223 IRIS users with update access privileges as of June 28, 2016. Our examination disclosed that some access authorization forms were missing or incomplete. Specifically:

- Department records did not evidence IRIS access authorization forms or other supporting access authorization documentation for 5 users.
- IRIS access authorization forms or other supporting access authorization documentation for 5 other users did not include the specific access roles requested.

The maintenance of appropriately authorized, complete, and accurate access authorization forms enhance management's ability to both ensure and demonstrate that access privileges granted for users are appropriate for the users' assigned job duties. Similar findings were noted in prior audits, most recently in our report No. 2016-018.

Recommendation: We recommend that Department management improve controls to ensure that properly completed and approved access authorization forms are retained.

Finding 2: 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:

[1] AST Rule 74-2.003(1)(a)6., Florida Administrative Code. Although AST Rules were not effective until March 10, 2016, rules promulgated by the Agency for Enterprise Information Technology (AEIT), AST's predecessor agency, included similar requirements. Specifically, AEIT Rule 71A-1.007(1), Florida Administrative Code, required agency owners to be responsible for authorizing access to information.

- **IRIS Application Users**. Our review of all 19 IRIS users with access to the IRIS application screen that allowed update access to the contribution rate master data as of June 28, 2016, disclosed that the update access for 16 of the 19 users was inappropriate based on the users' organizational placement within the Department.
- **Security Administrators**. During the 2015-16 fiscal year, the two IRIS security administrators had update access privileges to IRIS as end-users, update access privileges to production libraries, and update access privileges to the entire IRIS production database through the database administrator function. Additionally, the two security administrators had access, through the database administrator function, to change the log that showed who moved the IRIS changes and what IRIS changes were moved into the production environment. The combination of these access privileges results in an inappropriate separation of duties.
- **Application Programmers**. During the 2015-16 fiscal year, one programmer had access to move program changes into the production environment resulting in an inappropriate separation of duties. Additionally, the programmer had access to change the log that showed who moved the IRIS changes and what IRIS changes were moved into the production environment.
- **Database Administrators**. As of June 27, 2016, access for the four database administrators allowed them to change the log that showed who moved the IRIS changes and what IRIS changes were moved into the production environment.

Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

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.

Finding 3: Deactivation of Access Privileges

AST rules[2] require agency control measures that ensure IT access is removed when an IT resource is no longer required. Prompt action to deactivate access privileges when a user separates employment or access to the information is no longer required is necessary to help prevent misuse of the access privileges.

Department guidelines[3] require supervisors to complete an Employee Notification Form (Form) when a staff member separates from Department employment. The Form specifies that it should be e-mailed to the Administrative Services section of the Division and the Deloitte Technical Support Center no later than one week prior to an employment action (e.g., an employment termination); however, Department guidelines do not address when the access privileges of separated employees must be deactivated.

As part of our audit, we evaluated the Department's process for periodically reviewing IRIS access privileges and noted one former employee and one transferred user, whose IRIS access privileges were modified due to the performance of a periodic review of access privileges. However, although deactivated at the time of our review, the access privileges for these two individuals were not deactivated timely. The IRIS access privileges remained active for 6 days after the employee's separation date and for 10 days

[2] AST Rule 74-2.003(1)(a)8., Florida Administrative Code. Although AST Rules were not effective until March 10, 2016, AEIT Rule 71A-1.007(6), Florida Administrative Code, required that access authorization be promptly removed when the user's employment is terminated or access to the information is no longer required.

[3] *Security Guidelines Manual*, Section 6.

after the date of the user's transfer. Through our review of Department records, we determined that the accounts were not used subsequent to the dates of the users' employment separation and transfer.

Our audit procedures also disclosed that, prior to providing us the list of IRIS users as of June 16, 2016, the IRIS security administrator removed four IRIS user accounts. These accounts were for users who had separated employment with the Department. Our evaluation of the four user accounts as of June 16, 2016, disclosed that three of the user accounts were deactivated from 2 to 7 days after the users separated from Department employment. Through our review of Department records, we determined that the accounts were not used subsequent to the dates of the users' employment separation.

Without appropriate procedures for timely deactivating IRIS access privileges when a user separates employment or access to the information is no longer required, the risk is increased that the access privileges may be misused by the user or others to inappropriately disclose or make changes to IRIS data or could be used to inappropriately access IRIS confidential data.

Recommendation: We recommend that Department management establish procedures that specify when a user's access privileges should be deactivated and take appropriate action to ensure that IRIS accounts are timely deactivated when a user separates employment or access to the information is no longer required.

Finding 4: Periodic Review of User Access Privileges

AST rules[4] require agency control measures to address responsibilities of information stewards that facilitate periodic review of access rights with information owners. The frequency of reviews is to be based on system categorization or assessed risk. Department procedures[5] require the Technical Support Center to conduct an IRIS security audit every 6 months by providing a listing of active employees and other users with IRIS access privileges and the role that they have within IRIS to the Bureau Chiefs for review and validation. The periodic review of user access privileges helps ensure that only authorized users have access and that the access provided to each user remains appropriate.

As part of our audit, we evaluated Department procedures and reviewed Department documentation related to the periodic review of IRIS access privileges. Our evaluation of Department procedures disclosed that the procedures did not specify the time frame within which the Bureau Chiefs must complete the IRIS access privileges review. Our review of Department documentation found that the Department conducted a periodic review of IRIS user access privileges in October 2015; however, although the next review should have been performed in April 2016, the Department did not begin conducting that review until June 2016. Additionally, our review of the October 2015 review records disclosed that the periodic review process was ineffective. Specifically, the access listing of active IRIS users provided to the Bureau Chiefs for review was not system-generated and contained errors. For example, the listing included deactivated users. We also noted that one Bureau Chief did not provide a response regarding changes in access privileges until approximately 4 months after the initiation of the

[4] AST Rule 74-2.003(1)(a)6., Florida Administrative Code. Although AST Rules were not effective until March 10, 2016, AEIT Rule 71A-1.007(2), Florida Administrative Code, required agency owners to review access rights periodically based on risk, access account change activity, and error rate.

[5] *Procedure for Reviewing IRIS Security Accounts*.

periodic review process, prolonging users' inappropriate access. In response to our audit inquiry, Department management indicated that the periodic reviews of access privileges were ineffective due to a lack of detailed procedures related to the periodic review of IRIS user access privileges.

Without effective and timely periodic review of IRIS user access privileges, management's assurance that user access privileges are authorized and appropriate is limited.

Recommendation: We recommend that Department management improve controls and enhance Department procedures addressing the conduct of periodic reviews of IRIS access privileges. Such enhancements should require the use of system-generated lists of users and a specified time frame within which Bureau Chiefs must complete their review. Department management should also ensure that the reviews are performed every 6 months as required by Department procedures.

Finding 5: Service Accounts

Effective IT controls restrict access to sensitive system resources, such as service accounts (i.e., nonuser system accounts) to ensure that service accounts are enabled to perform automated system processes based on least functionality, service accounts are deactivated when no longer needed, and the access capability of service accounts is restricted to prevent interactive log-on (i.e., allowing the service account to be used to log on to the system as an individual). During our review of accounts with IRIS access privileges as of June 27, 2016, we determined that two service accounts had the parameter allowing interactive log-on, so that anyone who knows the password can log on to the system anonymously.

Appropriately restricting the use and access capabilities of service accounts helps protect the confidentiality, integrity, and availability of data and IT resources.

Recommendation: We recommend that Department management improve controls to ensure that the capability for interactive log-on for service accounts is appropriately restricted.

Finding 6: Security Controls – User Authentication and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to user authentication and monitoring of IRIS-related IT resources need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising IRIS data and IT resources. However, we have notified appropriate Department management of the specific issues. A similar finding was communicated to Department management in connection with our report No. 2016-018.

Without appropriate security controls related to monitoring for IRIS-related IT resources, the risk is increased that the confidentiality, integrity, and availability of IRIS data and related IT resources may be compromised.

Recommendation: We recommend that Department management improve certain security controls related to user authentication and monitoring for IRIS-related IT resources to ensure the confidentiality, integrity, and availability of IRIS data and 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. 2016-018.

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 2016 through August 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.

This IT operational audit focused on evaluating selected IT controls applicable to IRIS during the period July 2015 through June 2016 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. 2016-018. 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 Nos. 2016-018.
- 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 IRIS data and business process flows, including key sources of data input; key application transactions and process; key types of application data output; master data, and reconciliations related to IRIS.
  - The IRIS computing platform including applicable hardware, operating system, database management system, and security software.
  - The user account management process for authorizing, creating, modifying, and revoking IRIS user and related IT resources accounts.
- Evaluated IRIS business process application controls related to data input, processing, and output. Specifically, we:
  - Evaluated IRIS screen entries as of August 2, 2016, to assess the process for preventing the entry of an incorrect contribution amount and the Adjust Variance function that allowed the calculation and entry of the correct calculation amount in IRIS; IRIS error correction screen edits as of July 13, 2016, that disallow the same user to both correct a calculation error and perform the quality control review of the correction; and the Generate All Invoice screen option in IRIS as of July 14, 2016, which is used to ensure that all the corrected and quality control approved errors are invoiced for eventual correction or return of the appropriate funds. Throughout these IRIS screens, we also evaluated the use of drop down boxes that help ensure the use of valid values in the input of data.
  - Evaluated edits related to the payroll payment calculation for all four retirement plan types on a Payroll Error Corrections screen as of July 13, 2016.
  - Inspected the IRIS FRS Accounts Receivables Report as of July 5, 2016, used for tracking invoices and the FRS spreadsheet summaries as of August 3, 2016, used for final reconciliation and allocation of revenue categorization.
- Compared the 512 contribution rate master data elements in the IRIS database for the 2015-16 fiscal year to the Department's published contribution rates to determine if the contribution rate master data elements accurately reflected the Department's published contribution rates.
- Evaluated as of August 16, 2016, whether reconciliations were performed for the months of December 2015 and February 2016 for the IRIS transaction data and Florida Accounting Information Resource Subsystem interface. We also observed on June 28, 2016, the procedures for processing the data rejected in the interface process.

- Evaluated the effectiveness of IRIS application access authorizations controls for 25 of the 223 IRIS user IDs (excluding the View Only role) as of June 28, 2016, to determine whether the access granted was documented and authorized.
- Evaluated the effectiveness of selected access controls related to access privileges for appropriateness for IRIS and related IT resources. Specifically, we:
    - Evaluated the access appropriateness for all 16 IRIS users granted IRIS access privileges as of June 16, 2016, who had not separated from Department employment but whose access privileges changed during the period June 15, 2016, through June 30, 2016.
    - Evaluated whether access privileges were timely deactivated for the 4 users granted IRIS access privileges as of June 16, 2016, who separated from Department employment during the 2015-16 fiscal year and whose access privileges changed during the period June 15, 2016, through June 30, 2016.
    - Reviewed logs to determine whether users could log on to the IRIS database using 2 service accounts of the 20 service and delivered accounts as of June 27, 2016.
    - Evaluated the appropriateness of the seven accounts with access privileges to the IRIS database SELECT_CATALOG_ROLE as of June 27, 2016.
    - Evaluated the appropriateness of the two IRIS security administrators' access to the DBA and PROJECT_DBA roles as of June 27, 2016.
    - Evaluated the appropriateness of the two IRIS security administrators' access to the IRIS production libraries as of June 28, 2016.
    - Evaluated the appropriateness of access privileges granted to contribution rate master data. Specifically, we evaluated the 19 users with access to update the contribution rate master data through the IRIS screens as of June 28, 2016, to determine whether the access granted was appropriate.
- Determined whether 6-month periodic reviews of IRIS access appropriateness were timely and accurately performed during the 2015-16 fiscal year. Additionally, we evaluated records for two IRIS users (one user who separated from Department employment and one user who transferred) whose IRIS access privileges were modified due to the performance of the periodic review to determine whether the users' access privileges were timely deactivated.
- Evaluated database identification and authentication controls.
- Reviewed the May 2016 FRS Online application object change logging and confirmed with Department management as of July 6, 2016, whether appropriate FRS Online application object change logging and monitoring were performed regarding who moved the changed FRS Online application object onto the production servers and when.
- 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

January 17, 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,

Chad Poppell
Secretary

CP/sk-a

Enclosure

cc: Erin Rock, Chief of Staff
Heather Best, Senior Director of Executive Operations
Elizabeth Stevens, Director of Retirement
Shirley Beauford, Assistant Director of Retirement
Bob Ward, Chief Information Officer
Dawn E. Case, Inspector General
Yolanda Lockett, Audit Director

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name	
1/17/17		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**	
Security	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement	Yes	**2/28/17**

Finding No. 1 / Date	**Access Authorization Documentation**
Finding	Complete and accurate IRIS access authorization documentation was not maintained, thereby limiting management's assurance that IRIS user access privileges were authorized and appropriately assigned.
Recommendation	We recommend that Department management improve controls to ensure that properly completed and approved access authorization forms are retained.
Management/Agency Response	In response to the finding in the prior audit, the Division revised the ENF to require supervisors to select the specific IRIS access role that was being authorized and made the field required. The Security Guidelines Manual was updated to reflect the new requirement and supervisors were advised of changes. This repeat finding resulted from previous changes being implemented prospectively. Of the accounts identified from the sample as having an issue related to the access authorization form, all but one had access that predated the changes enacted by the Division as a result of the prior audit. The last account was updated and documented by the bureau chief in the six- month review process. The Division will complete an overall review of our IRIS access authorization process. This includes requests for access, changes, and deactivations as well as the six-month review for appropriate access levels. Upon the completion of this project, the Security Guidelines Manual will be revised, and staff will be trained. Additionally, after we complete our process review and update our procedures, the Division will document the IRIS access authorizations for all persons that currently have IRIS access. The Division expects to complete this review and document authorizations by February 28, 2017.
Status Update-Adjustments ☐ Adjustments Made ☐ No Adjustments Made ☐ Partially Complete ☐ Management Assumes Risk ☐ Closed	
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	

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name		
1/17/17		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**	
Application Security	**Responsible Area**		**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement		No	**1/6/17**
Finding No. 2 / Date	**Appropriateness of Access Privileges**			
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	IRIS Application Users: The Division determined that the employees noted in the audit did not have a need to update the Contributions Rate Table for their assigned job duties and removed this access on October 7, 2016. Employees can only view the contributions rate information. The new process for updating the Contributions Rate Table is for appropriate management staff to send a change request with the spreadsheet of the updated rates to the IT help desk. Requests are logged and assigned a work number. Once the new rate information is updated to the IRIS table, the manager or the designated employee will review the rate information for accuracy. The manager will notify the help desk to close the ticket after verifying that the rate information is correct. The Division will complete a review of reference tables containing critical FRS information to determine whether employee access to edit the reference table is appropriate. If edit capability is not appropriate, the access will be removed. Security Administrators: The Division removed the database administrator function from the Security Administrators on 10/10/16 which restricts their access to the IRIS production database and prevents updates to the IRIS change log. In addition, the Division will make changes to the semi-annual PowerLock review process that will no longer require security administrators to have production end user update access to IRIS to generate IRIS role reports. Application Programmers: The Division removed the update privileges on the change log table from the programmer's account. Also, the Division has implemented a process to export and archive the IRIS change logs each time an IRIS change occurs, preserving the record as files in an archive folder with a timestamp on each file. Also, implemented are access restrictions that prevent the logs from being deleted or changed by application programmers and database administrators. Database Administrators: The Division implemented a process to export and archive the IRIS change logs each time an IRIS change occurs which preserves a record in an archive folder with a timestamp on each file. Also, implemented are access restrictions that prevent the logs from being deleted or changed by application programmers and database administrators.			
Status Update-Adjustments ☐ Adjustments Made ☐ No Adjustments Made ☐ Partially Complete ☐ Management Assumes Risk ☐ Closed				
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				

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name		
1/17/17		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**	
Security	**Responsible Area**		**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement		**No**	**2/28/17**

Finding	
No.	3
Date	
Deactivation of Access Privileges	
Finding	The Department did not have procedures for timely deactivating IRIS accounts for users who no longer required access and did not timely deactivate the IRIS accounts for some users.
Recommendation	We recommend that Department management establish procedures that specify when a user's access privileges should be deactivated and take appropriate action to ensure that IRIS accounts are timely deactivated when a user separates employment or access to the information is no longer required.
Management/Agency Response	The Division is currently reviewing the IRIS access authorization process. One focus of the review is ensuring timely deactivations. The Security Guidelines manual will be updated with additional information for deactivating IRIS users who no longer need access to perform their job duties. Additionally, for terminated employees, the Division has implemented another control procedure to review the report of active IRIS accounts within one business day of a person's termination date to verify that the terminated employee is not listed with an active IRIS account. The Division expects to complete the review of the IRIS access authorization process by February 28, 2017.
Status Update-Adjustments ☐ Adjustments Made ☐ No Adjustments Made ☐ Partially Complete ☐ Management Assumes Risk ☐ Closed	
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	

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name		
1/17/17		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**	
Security	**Responsible Area**		**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement		**No**	**2/28/17**

Finding	
No.	4
Date	

Periodic Review of User Access Privileges

Finding	Department procedures did not ensure the timely and effective review of the appropriateness of user access privileges granted to IRIS.
Recommendation	We recommend that Department management improve controls and enhance Department procedures addressing the conduct of periodic reviews of IRIS access privileges. Such enhancements should require the use of system-generated lists of users and a specified time frame within which Bureau Chiefs must complete their review. Department management should also ensure that the reviews are performed every 6 months as required by Department procedures.
Management/Agency Response	The Division will create a new system generated report listing each user's IRIS access level for the scheduled six-month IRIS access review. The Division will update the six-month review procedures to include time frames for starting and completing all reviews. Staff will be trained on the updated procedures. The six-month review process is included in the overall access authorization process project that the Division expects to complete by February 28, 2017.

Status Update-Adjustments	
☐ Adjustments Made ☐ No Adjustments Made ☐ Partially Complete ☐ Management Assumes Risk ☐ Closed	
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	

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name	
1/17/17		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**	
Security	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement	**No**	**1/9/17**

Finding	
No.	5
Date	

Service Accounts

Finding	Some service accounts inappropriately allowed interactive log-on increasing the risk that the confidentially, integrity, and availability of Department data and IT resources may be compromised.
Recommendation	We recommend that Department management improve controls to ensure that the capability for interactive log-on for service accounts is appropriately restricted.
Management/Agency Response	The Division has implemented a database log-on trigger to only allow database service account authentication from trusted server sessions.

Status Update-Adjustments ☐ Adjustments Made ☐ No Adjustments Made ☐ Partially Complete ☐ Management Assumes Risk ☐ Closed	
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	

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name	
1/17/17		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**	
Security	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement	Yes	**2/28/17**

Finding		
No.	6	**Security Controls – User Authentication and Monitoring**
Date		

Finding	Certain security controls related to user authentication and monitoring for IRIS-related IT resources need improvement to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.
Recommendation	We recommend that Department management improve certain security controls related to user authentication and monitoring for IRIS-related IT resources to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.
Management/Agency Response	While the Division made changes to remediate this finding following the prior audit, the Division supports the recommendation and has implemented measures to enhance security controls related to user authentication and monitoring of IRIS related IT resources. 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-Adjustments ☐ Adjustments Made ☐ No Adjustments Made ☐ Partially Complete ☐ Management Assumes Risk ☐ Closed	
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-12 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	