

# STATE OF FLORIDA AUDITOR GENERAL

## Information Technology Operational Audit

Report No. 2026-073  
January 2026

### 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, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. Pedro Allende served as Department Secretary during the period of our audit.

The Auditor General conducts audits of government 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.

The team leader was Earl M. Butler, CISA, and the audit was supervised by Brenda Shiner, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at [brendashiner@aud.state.fl.us](mailto:brendashiner@aud.state.fl.us) or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

[FLAuditor.gov](http://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 Integrated Retirement Information System (IRIS) information technology (IT) controls and included a follow-up on applicable findings included in our report No. 2023-022. Our audit disclosed the following:

**Finding 1:** As similarly noted in our report No. 2023-022, Division of Retirement (Division) change management controls for IRIS program and database changes need improvement to ensure that all changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the production environment, and are managed by, and do not bypass, the Division's change management process.

**Finding 2:** IRIS access privilege controls continue to need enhancement to ensure access is promptly disabled when no longer necessary.

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

### **BACKGROUND**

---

State law<sup>1</sup> establishes the Division of Retirement (Division) within the Department of Management Services (Department) and the Department, along with the Division, uses the Integrated Retirement Information System (IRIS) to support business processes related to the Florida Retirement System (FRS). The business processes supported by IRIS (IRIS 1.0, a client-based application,<sup>2</sup> and IRIS 2.0, a Web-based application<sup>3</sup>) include member enrollment and the maintenance of member information, receipt of contributions from FRS participating employers, tracking of employee and employer contributions and employee service histories, calculation of retirement benefits, and issuance of the retiree payroll file processed by the Department of Financial Services. IRIS supports all essential Division business functions for the FRS and facilitates communication with employers, active members, retirees, and business partners. The public facing FRS Online application is an extension of IRIS and provides information and services to members, employers, employees, and other stakeholders, including retirees.

Application and database administration support for IRIS and the FRS Online application, and support for the Division's day-to-day information technology (IT) needs, were outsourced by the Department to 22nd Century Technologies, Inc. (TSCTI). TSCTI was responsible for, among other things, IRIS server

---

<sup>1</sup> Section 121.1905, Florida Statutes.

<sup>2</sup> A client-based application is an application that runs on a workstation or personal computer in a network.

<sup>3</sup> Web-based application software is accessed by users through a Web browser over the Internet.

and system infrastructure administration, including IRIS application programming and database administration functions.

## ***FINDINGS AND RECOMMENDATIONS***

---

### **Finding 1: Change Management Controls**

Effective change management controls are intended to ensure that all program code and database changes are properly authorized, tested, and approved for implementation into the production environment. Effective change management controls also include reconciling and reviewing all system changes implemented into the production environment for approval and appropriateness. Controls over the modification of programs, including the review of before and after images of program code prior to implementation, help ensure that only approved program code changes are made within the programs.

We evaluated the appropriateness of Division change management controls for IRIS program code changes implemented into the IRIS production environment by requesting from the Division a system-generated list of IRIS program code changes implemented into the production environment during the period July 1, 2024, through May 10, 2025. Additionally, we evaluated the adequacy of Division controls over the implementation of IRIS database changes. Our audit procedures found that the Division:

- Was unable to provide a system-generated list of the implemented program code changes because the production code servers only recorded the most-recent date a program code file was changed. Instead, the Division provided manually produced release notes documenting the implementation builds (grouped IRIS program code changes scheduled for implementation into the production environment) that occurred during the period July 1, 2024, through May 10, 2025. Although the Division used the release notes to document IRIS program code changes, Division management indicated that IRIS program code changes could be implemented to production outside the build process and therefore would not be included on the release notes.
- Had not established change management controls, such as a reconciliation process or other process, to ensure that all IRIS program code changes implemented into the production environment were recorded on the release notes.
- Logged IRIS database changes using the Oracle Unified Auditing Framework; however, the logs did not capture changes to actual data values (i.e., before and after values) and, instead, only captured the metadata of database operations (who, what, when, where, and how an action occurred). According to Division management, a periodic reconciliation or other process (e.g., data change logging and monitoring) to ensure that all IRIS database changes implemented were authorized and approved was not performed.

In response to our audit inquiry, Division management indicated that the Division did not have software that would provide a system-generated list necessary to perform a reconciliation of either IRIS program code or database changes.

To further evaluate the appropriateness of IRIS change management controls using the release notes for program code changes implemented during the period July 1, 2024, through May 10, 2025, we

selected for audit the seven IRIS 1.0 change request tickets that included 14 program code changes.<sup>4</sup> For each of the seven IRIS 1.0 change request tickets, we requested from the Division documentation evidencing that the program code changes associated with the change request tickets were properly authorized, user acceptance tested, code reviewed, approved for implementation, and implemented into production by someone other than the personnel who made the program code change. Our review of the change request ticket documentation found that:

- Two of the change request tickets did not evidence business user authorization for the change. Although we inquired, Division management was unable to determine why business user authorization was not documented.
- Five of the change requests tickets were not supported by a *Technical Peer Review Form* evidencing who performed the technical peer review and when the review was performed. According to Division management, the program code changes related to these tickets were minor in nature and, while the code changes were peer reviewed, a *Technical Peer Review Form* was not completed to evidence such a review.
- One change request ticket did not evidence the business user who performed user acceptance testing. In response to our audit inquiry, Division management provided a meeting invitation to the business user as evidence of user acceptance testing; however, our examination of the documentation found that the invitation did not include information on the purpose of the meeting or reference the change request ticket number.
- Two change request tickets did not evidence business user approval for implementation. Although we inquired, Division management was unable to explain why such evidence was not available.

Additionally, our evaluation of the Division program code review process found that the Division did not perform a program code review (i.e., reviewing before and after images) to ensure that programmers did not make unauthorized program code changes. Also, the Division had not established a mechanism to prevent programmers from changing the approved program code after the technical peer review was completed and prior to implementation into production. In response to our audit inquiry, Division management indicated that the release software used did not allow for a review of before and after images of code. While Division management indicated that modifications to program code were reflected in object history, object histories were not reviewed due to resource constraints (time and personnel) and a lack of perceived value in performing such reviews.

Absent sufficient IRIS change management controls, the risk is increased that unauthorized IRIS program code and database changes may be implemented into the IRIS production environment and not timely detected. A similar finding was noted in our report No. 2023-022 (Finding 4).

**Recommendation: We again recommend that Division management enhance IRIS change management controls to ensure that all program code changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the production environment, and are managed by, and do not bypass, the Division's change management process. We also recommend that program code reviews are performed using before and after images of the program code prior to implementation of program changes and that Division management ensure that all IRIS database changes are appropriately authorized and approved.**

---

<sup>4</sup> According to the release notes, no IRIS 2.0 program code changes were made during the selected period.

## Finding 2: Timely Disablement of IRIS Access Privileges

Department rules<sup>5</sup> require IT access privileges be removed when access to an IT resource is no longer required. Prompt action to disable access privileges when a user separates from employment or access to the IT resource is no longer required is necessary to help prevent misuse of the access privileges. Department policies<sup>6</sup> specified that retaining open accounts for users beyond their last workday was a security risk and prohibited, and that inactive user identifiers (user accounts) were to be disabled after 90 days of inactivity.

For the 48 IRIS 1.0 users (47 employees and 1 contractor) and the 45 IRIS 2.0 users (44 employees and 1 contractor) who separated from Department employment during the period July 1, 2024, through April 3, 2025, we examined access removal records for IRIS 1.0 and IRIS 2.0 to determine whether IRIS user access privileges were timely removed upon employment separation. Our examination found that 6 former employees retained access to IRIS 1.0 and IRIS 2.0 for 1 to 19 days (an average of 7 days) after the employees' separation dates. According to Division management, the access privileges were not timely removed due to late employment termination notifications by supervisors, incorrect separation dates provided by a supervisor, and late deactivations by security administrators. A similar finding has been noted in prior audits of the Department, most recently in our report No. 2023-022 (Finding 1).

Additionally, we reviewed the last logon date for the 448 IRIS user accounts (229 IRIS 1.0 user accounts and 219 IRIS 2.0 user accounts) active as of April 3, 2025, and identified 29 dormant user accounts that were not used after December 19, 2024, or never used (no user log on). Specifically, our examination of the 29 dormant user accounts found:

- 10 IRIS 1.0 user accounts with a last logon date during the period September 15, 2023, through November 18, 2024, that were no longer necessary.
- 14 IRIS 2.0 user accounts with a last logon date during the period November 28, 2022, through December 19, 2024, that were no longer necessary.
- 5 IRIS 2.0 user accounts that had never been used and were unnecessary.

In response to our audit inquiry, Division management indicated that, to address the issues noted on audit, additional controls would need to be designed such as system alerts to both IRIS users and System Administrators of IRIS user accounts that were inactive for more than 90 days or automatic system disablement after 90 days of non-use.

Timely disablement of IRIS user access privileges when the access privileges are no longer required reduces the risk that the access privileges may be misused by former employees or others.

**Recommendation:** We again recommend that Division management enhance controls to ensure that IRIS user accounts are promptly disabled upon employment separation. We also recommend that Division management enhance controls to identify and promptly disable dormant IRIS user accounts.

<sup>5</sup> Department Rule 60GG-2.003(1)(a)8., Florida Administrative Code.

<sup>6</sup> Department Policy Number 21-107, *Access Control Policy*, and Policy Number 21-111, *Information Technology Security Policy*, respectively.

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

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

Without appropriate security controls related to logical access, user authentication, configuration management, vulnerability management, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of Department data and related IT resources may be compromised. Similar findings related to logical access, user authentication, and configuration management were communicated to Department management in connection with our report No. 2023-022.

**Recommendation: We recommend that Department management improve certain security controls related to logical access, user authentication, configuration management, vulnerability management, and logging and monitoring to ensure the confidentiality, integrity, and availability of Department data and related 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. 2023-022.

## ***OBJECTIVES, SCOPE, AND METHODOLOGY***

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this information technology (IT) operational audit from March 2025 through August 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant Department of Management Services (Department) and Division of Retirement (Division) IT controls applicable to the Integrated Retirement Information System (IRIS) during the period July 2024 through June 2025 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To evaluate 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 has corrected, or is in the process of correcting, all deficiencies disclosed in our audit report No. 2023-022.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

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

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

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

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

In conducting this audit, we:

- Reviewed applicable laws, rules, Department and Division policies and procedures, and other guidelines, and interviewed Department and Division personnel to obtain an understanding of the Division's organizational structure, statutory requirements, Department and Division operational processes, and the IRIS computing platform.
- Obtained an understanding of Division processes for authorizing, assigning, disabling, and periodically reviewing access to the Division IRIS production code, Division network domain, and IRIS, including processes for ensuring an appropriate separation of incompatible duties for IRIS end-users; the paths and processes for authenticating to the Division network domain, IRIS application and database, and related IT resources; Division processes for authorizing, programming, approving, and implementing IRIS program changes to production; Division configuration management processes related to patches, upgrades, and other configuration changes for IRIS database appliances, database, servers, and other network devices; logging

and monitoring controls for IRIS and related IT resources; and database vulnerability management processes.

- Evaluated logical access controls, including policies, procedures, and processes, for assigning, periodically reviewing, and disabling user and security administration accounts for the IRIS application, database, and related IT resources, and administrative-level user and service accounts for the Department and Division network domains. Specifically, we evaluated:
  - Department and Division procedures and examined Department and Division records to determine whether periodic access reviews were performed to evaluate the appropriateness of IRIS end-user access, administrative-level access to the Department and Division network domains, and IRIS database and production code.
  - The appropriateness of access for 25 of the 205 end-users with update access privileges to the IRIS application as of April 3, 2025.
  - The timeliness of disabling dormant (not used for more than 90 days or never used) IRIS end-user accounts as of April 3, 2025.
  - The timeliness of disabling IRIS end-user account access for the 47 Department employees and 1 contractor with IRIS 1.0 access privileges (of which 44 Department employees and 1 contractor also had an IRIS 2.0 user account) who separated from Department employment during the period July 1, 2024, through April 3, 2025.
  - The appropriateness of access for ten end-users with access privileges to Team Foundation Server (TFS) source code as of June 2025.
  - The timeliness of disabling TFS access privileges for the one Division contractor with TFS access as of May 30, 2025, who had ceased providing services to the Division.
  - The appropriateness of access privileges assigned to the two IRIS security administrators, including whether access to IRIS end-user roles and the IRIS application production code libraries was sufficiently restricted as of April 17, 2025.
  - The appropriateness of the three administrative user accounts and one administrative service account as of April 2, 2025, for the Division network domain.
  - The adequacy of security controls for the default *Administrator* account for the Division network domain.
  - The appropriateness of the 22 administrative-level user and service accounts with direct update access to the IRIS database and whether an appropriate separation of duties was maintained between IRIS database administrative-level access privileges and application programmer privileges as of April 7, 2025.
- Evaluated the adequacy of user authentication controls for the IRIS application and database, the Department and Division network domains, Division virtual private network, and a Division-managed high-risk network device.
- Interviewed Division personnel and examined Division policies, procedures, and processes for IRIS program and database change requests, including change reconciliation processes and program code reviews. Specifically, we examined the 7 IRIS 1.0 program change tickets representing 14 program changes implemented during the period July 1, 2024, through May 10, 2025, as documented on the release notes, to determine whether the program changes were appropriately authorized, reviewed, tested, approved for and implemented into production.
- Evaluated the adequacy of selected logging and monitoring controls for IRIS and related IT resources.
- Evaluated the adequacy of selected vulnerability management controls for the IRIS database.

- Evaluated the effectiveness of Division configuration management policies, procedures, and processes for the IRIS database and database management software and a Division-managed high-risk network device. Specifically, we evaluated whether:
  - As of June 5, 2025, the database appliance was current and up to date.
  - As of June 5, 2025, the IRIS database management software and related server operating system was timely patched.
  - As of June 5, 2025, the operating system on the two database servers was supported and timely patched.
  - As of April 24, 2025, the operating system for a Division-managed high-risk network device was supported and timely patched.
- 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

---



4050 Esplanade Way  
Tallahassee, FL 32399-0950

**Ron DeSantis, Governor**  
Tom Berger, Interim Secretary

---

January 5, 2026

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, enclosed is our response to your preliminary and tentative audit findings transmitted on December 5, 2025, for your information technology operational audit of the *Department of Management Services - Integrated Retirement Information System*.

If further information is needed concerning our response, please contact Inspector General Heather D. Robinson or Director of Audit Tabitha McNulty at (850) 488-5285.

Sincerely,



Tom Berger  
Interim Secretary

TB/tam

Enclosure

cc: Edric Sanchez, Deputy Secretary of Workforce Operations  
Heather D. Robinson, Inspector General  
Kathy Gould, Director, Division of Retirement



**Corrective Action Plan in response to:**  
Auditor General Preliminary and Tentative Audit Findings  
*Department of Management Services*  
*Integrated Retirement Information System (IRIS)*

**Finding 1: Change Management Controls**

As similarly noted in our report No. 2023-022, Division of Retirement (Division) change management controls for IRIS program and database changes need improvement to ensure that all changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the production environment, and are managed by, and do not bypass, the Division's change management process.

**Recommendation:** We again recommend that Division management enhance IRIS change management controls to ensure that all program code changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the production environment, and are managed by, and do not bypass, the Division's change management process. We also recommend that program code reviews are performed using before and after images of the program code prior to implementation of program changes and that Division management ensure that all IRIS database changes are appropriately authorized and approved.

**Management Response:** Concurs with the finding and recommendation.

**Description of Corrective Action(s):**

To further enhance change management controls, the Division will develop a plan and timeline to:

- (1) improve IRIS change management controls to ensure that all program code changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the production environment, and are managed by, and do not bypass, the Division's change management process,
- (2) perform program code reviews using before and after images of the program code prior to implementation of program changes, and
- (3) ensure that all IRIS database changes are appropriately authorized and approved.

In addition to the immediate corrective action detailed above, the current change management process includes a manual review of code before and after development – new Azure DevOps tools and their associated procedures will provide more automated code reviews of what ultimately ends up in production. Database changes include verification of objects deployed and logging of database operations that includes who, what, when, where and how and the change occurred. Changes included in biweekly releases are approved by business users as part of the system investigation request (SIR) management process.

As we continue to transition from legacy IRIS to the new web-based IRIS platform while modernizing our applications and change management processes using Azure DevOps, we will have increased traceability from "idea to implementation". This will allow us to link business requests to developed code, test cases, code reviews, and ultimately production releases. This transition and modernization effort will address the three items listed above.

**Expected Completion Date for Plan and Timeline:** June 30, 2026

**Corrective Action Plan in response to:**

Auditor General Preliminary and Tentative Audit Findings

Department of Management Services Integrated Retirement Information System (IRIS)

---

**Finding 2: Timely Disablement of IRIS Access Privileges**

IRIS access privilege controls continue to need enhancement to ensure access is promptly disabled when no longer necessary.

**Recommendation:** We again recommend that Division management enhance controls to ensure that IRIS user accounts are promptly disabled upon employment separation. We also recommend that Division management enhance controls to identify and promptly disable dormant IRIS user accounts.

**Management Response:** Concurs with the finding and recommendation.

**Description of Corrective Action(s):**

The Division proactively reviews IRIS access on a quarterly basis and will continue to enhance controls for promptly disabling IRIS user accounts. As the Division modernizes to the new web-based IRIS platform, the system will allow the Division to schedule a termination date within IRIS for a systematic termination at the future designated date for the timely disablement of IRIS privileges. During the quarterly review of IRIS access that began October 2025, the Division identified dormant accounts and removed access. The Division will continue to review IRIS accounts quarterly to identify dormant accounts and deactivate them, until an automated option is completed.

**Expected Completion Date for Plan and Timeline:** June 30, 2026

**Finding 3: Security Controls**

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

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

**Management Response:** Concurs with the finding and recommendation.

**Description of Corrective Action(s):**

Security is a priority for the Division and the Department, and the Division works closely with the Department's Office of Information Technology (OIT) to ensure security controls are in place. To continue enhancing the security of IT resources, the Division and Department will develop a plan and timeline to improve certain security controls related to logical access, user authentication, configuration management, vulnerability management, and logging and monitoring to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

As we continue to transition from legacy IRIS to the new web-based IRIS platform while modernizing our applications and processes using Azure DevOps, we will have increased abilities to improve certain confidential security controls related to logical access, user authentication, configuration management, vulnerability management, and logging and monitoring to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

**Expected Completion Date for Plan and Timeline:** June 30, 2026