Report No. 2023-022
September 2022

State of Florida Auditor General

Information Technology Operational Audit

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. J. Todd Inman served as Secretary during the period of our audit.

The team leader was B.Y. Yang, 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 or by telephone at (850) 412-2946.

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

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General
Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

DEPARTMENT OF MANAGEMENT SERVICES

Integrated Retirement Information System (IRIS)

SUMMARY

This operational audit of the Department of Management Services (Department) focused on evaluating selected Integrated Retirement Information System (IRIS) information technology (IT) controls and included a follow-up on applicable findings included in our report No. 2019-220. Our audit disclosed the following:

Finding 1: Access privileges to IRIS and related IT resources were not always promptly disabled when no longer necessary.

Finding 2: As similarly noted in our report No. 2019-220, Department records did not evidence periodic reviews of the Department network domain privileged accounts' access privileges.

Finding 3: Division documentation of IRIS end-user role-based access privileges needs improvement to help ensure that IRIS end-user access is appropriately assigned.

Finding 4: Division change management controls for IRIS program changes need improvement to ensure that all program 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 5: Certain security controls related to logical access, user authentication, configuration management, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.

BACKGROUND

State law[1] 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,[2] and IRIS 2.0, a Web-based application[3]) 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.

[1] Section 121.1905, Florida Statutes.

[2] A client-based application is an application that runs on a workstation or personal computer in a network.

[3] Web-based application software runs in a Web browser. Web-based applications are delivered on the World Wide Web to users with an active Internet connection.

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

FINDINGS AND RECOMMENDATIONS

Finding 1: Timely Disablement of IT Access Privileges

Department rules[4] 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 policy[5] specified that retaining open accounts for users beyond their last workday was a security risk and prohibited.

For the 42 IRIS users who separated from Department employment during the period July 1, 2021, through February 11, 2022, we examined access removal records for IRIS 1.0 and IRIS 2.0 to determine whether IRIS user access privileges were timely disabled upon employment separation. Our examination found that:

- The IRIS 1.0 user accounts for 15 former employees were disabled 1 day late and the user accounts for 8 other former employees were disabled 2 to 78 days (an average of 18 days) after the employees' separation dates.
- The IRIS 2.0 user accounts for 13 former employees were disabled 1 day late and the user accounts for 6 other former employees were disabled 2 to 78 days (an average of 22 days) after the employees' separation dates.

According to Division management, the Department had a process to remove access to employee network domain accounts upon employment separation, and that this action would disable access to both IRIS 1.0 and IRIS 2.0, regardless of whether user access privileges were removed at the application level. However, although we requested, Department personnel were unable to provide system-generated evidence of the disablement of any of the IRIS user network domain accounts. Division management indicated that security administrators responsible for disabling IRIS user accounts were not always timely notified when employees separated from Department employment. Further, Division management indicated that the Division was unaware that Department policy specified that retaining open accounts for users beyond their last workday was a security risk and prohibited and, instead, the Division followed the IRIS Desk Guide[6] that permitted 1 day for access removals upon employment separation. A similar finding was noted in our report No. 2019-220 (Finding 1).

We also examined access control records as of February 1, 2022, for Team Foundation Server (TFS) to determine whether user access privileges were timely disabled for former contractors responsible for

[4] Department Rule 60GG-2.003(1)(a)8., Florida Administrative Code.

[5] Department Policy Number 21-107, *Access Control Policy*.

[6] Division Desk Guide: *IRIS 1.0, IRIS 2.0, FRS Online Security Access Authorization, Deactivation, and Periodic Reviews*.

maintaining IRIS. TFS access allowed a user to modify IRIS application source code. Our examination found that the TFS access privileges for 4 of the 10 former contractors with access privileges to either IRIS 1.0, IRIS 2.0, or both remained active 3 to 127 days (an average of 48 days) after the contractors ceased providing services to the Division. In response to our audit inquiry, Division management indicated that the former contractors' TFS access privileges were not timely disabled due to oversight.

Timely disabling IRIS and TFS user access privileges when the access privileges are no longer required reduces the risk that the access privileges may be misused by the former employee, contractor, or others.

Recommendation: We recommend that Division management enhance controls to ensure that Department records evidence that former employee and contractor IRIS and TFS user access privileges are promptly disabled.

Finding 2: Periodic Review of Network Domain Access Privileges

Department rules[7] require agency information owners to review access rights (privileges) periodically based on system categorization or assigned risk. Accordingly, Department policy[8] required access reviews be conducted at least quarterly and documentation of such reviews be retained for 1 year. Periodic reviews of privileged network user and service accounts with access to data and IT resources help protect the confidentiality, integrity, and availability of data and IT resources by ensuring that only authorized users have access and that the access privileges assigned to user and service accounts remain appropriate and necessary.

As part of our audit, we evaluated Department access review controls and found that, as of March 2022, Department management was unable to provide evidence of any quarterly access reviews of privileged network user and service accounts for the Department network domain. In response to our audit inquiry, Department management indicated that evidence of periodic access reviews, if conducted, was not retained due to recent changes in Department IT management.

Without documented periodic access reviews of network domain access privileges, management's assurance that access privileges were properly authorized and remained appropriate is limited. A similar finding was noted in our report No. 2019-220 (Finding 4).

Recommendation: We again recommend that Department management conduct and document periodic access reviews of Department privileged network accounts in accordance with established policy.

Finding 3: IRIS End-User Access Documentation

Department rules[9] require each agency to ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. Department rules[10] also require agencies to establish a policy and procedure review process that facilitates continuous improvement to protection processes and information system owners to define application and security

[7] Department Rule 60GG-2.003(1)(a)6., Florida Administrative Code.

[8] Department Policy Number 21-107, *Access Control Policy*.

[9] Department Rule 60GG-2.003(1), Florida Administrative Code.

[10] Department Rule 60GG-2.003(5)(g), Florida Administrative Code.

related business requirements using role-based access controls and rule-based security policies where technology permits, as well as establish and authorize the types of privileges and access rights appropriate to system users, both internal and external. Policies and procedures are established to reasonably assure that application security audit and monitoring is effective. The monitoring program should have built-in procedures to identify inappropriate user assignments and monitoring should be performed on a regular basis.

As part of our audit, we reviewed Division policies and procedures and records and interviewed Division personnel responsible for assigning IRIS end-user access privileges and found that IRIS end-user role description documentation was incomplete. Specifically, IRIS end-user role documentation as of February 3, 2022, did not include descriptions for the *Member Security Dashboard, POLICYADMIN*, *RET1*, and *RET-TRAINING* end-user access roles and lacked sufficient information to determine whether the roles *Authentication*, *BP-All-Ref Table Admin*, *CCCRM1*, *Director's Office*, and *Legal* had update access privileges. While Division management was able to provide sufficient information on the access privileges associated with five of the roles, as of the date of our IRIS end-user access testing in February 2022, Division management was unable to provide specific information for the other four roles (*CCCRM1*, *POLICYADMIN*, *RET1*, and *RET-TRAINING*). As a result, we could not determine whether IRIS end-user access privileges for the 72 individuals assigned one of the four IRIS end-user roles were appropriate. According to Division management, IRIS end-user role documentation had not been updated to include the necessary information due to oversight.

Up-to-date application access documentation facilitates the assignment of appropriate end-user access privileges and decreases the risk that inappropriate or unauthorized IRIS application access privileges would be granted.

Recommendation: We recommend that Division management improve IRIS end-user role documentation to ensure that all IRIS end-user roles and their associated access privileges are documented.

Finding 4: Change Management Controls

Effective change management controls are intended to ensure that all program changes are properly authorized, tested, and approved for implementation into the production environment. 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.

To evaluate the appropriateness of Division change management controls for IRIS program changes implemented into the IRIS production environment, we requested from the Division a system-generated list of IRIS program changes implemented into the production environment during the period July 2021 through January 2022. However, the Division was unable to provide a system-generated list of the implemented program changes and, instead, the Division provided manually produced release notes for the implementation builds (grouped IRIS program changes scheduled for implementation into production) that occurred during the period July 2021 through January 2022. Although the Division used the release notes to document IRIS program changes, Division management indicated that IRIS program changes could be implemented outside the build process and therefore would not be recorded on the release notes. Also, we noted that the Division had not established change management controls, such as a reconciliation process, to ensure that all IRIS program changes implemented into the production environment were recorded on the release notes.

Additionally, our evaluation of Division change management controls found that the Division had not established a process, such as a quality assurance function or program code review, to ensure that programmers did not make unauthorized program code changes in addition to the program changes approved for implementation into production. In response to our audit inquiry, Division management indicated that, while a technical peer review was performed for program changes identified as completed by the programmer in the IRIS change management ticketing system to ensure that Division program coding standards were followed, the Division did not have the ability to identify and review all program changes in an efficient manner to ensure that unauthorized program changes were not made in addition to approved program changes. Best practices for change management include reviewing before and after images of program code changes prior to implementation into production.

The absence of appropriate IRIS change management controls, including identification and review of program changes prior to implementation, increases the risk that unauthorized IRIS program changes may be implemented into the IRIS production environment.

Recommendation: We recommend that Division management improve IRIS change management controls to ensure that all program 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 5: Security Controls – Logical Access, User Authentication, Configuration 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, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising IRIS data and related IT resources. However, we have notified appropriate Department management of the five findings in the four areas needing improvement.

Without appropriate security controls related to logical access, user authentication, configuration management, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of IRIS data and related IT resources may be compromised. Similar findings related to user authentication, configuration management, and logging and monitoring were communicated to Department management in connection with our report No. 2019-220.

Recommendation: We recommend that Department and Division management improve certain security controls related to logical access, user authentication, configuration management, and logging and monitoring 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 applicable findings included in our report No. 2019-220.

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 December 2021 through May 2022 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) Integrated Retirement Information System (IRIS) IT controls during the period July 2021 through March 2022 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To evaluate the effectiveness of selected significant IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, all applicable deficiencies disclosed in our report No. 2019-220.
- 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 network domain and IRIS, including processes for ensuring an appropriate separation of incompatible duties for IRIS; logical access controls for the Division network domain; the paths and processes for authenticating to the Division network domain and IRIS application and related IT resources; Division processes for authorizing, programming, approving, and implementing IRIS program changes to production; IRIS backup processes; Division configuration management processes related to patches, upgrades, and other configuration changes for servers and network devices; identification and authentication processes for users of IRIS IT resources; significant IRIS data input, processing, and output controls; and logging and monitoring controls for security events for the IRIS application, database, and related high-risk network devices.
- Evaluated logical access controls, including policies, procedures, and processes, for assigning, periodically reviewing, and disabling user and security administration accounts for the IRIS application and related IT resources, and the administrative-level user and service accounts for the Department and Division network domains, the Division's high-risk network devices, and IRIS database. 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 and administrative-level access to the Department and the Division network domains, Division high-risk network devices, and IRIS database.
  - The appropriateness of access for 25 of the 200 end-users with update access privileges to the IRIS application as of February 2022.
  - The timeliness of disabling IRIS account access for the 42 Department employees with IRIS access privileges who separated from Department employment during the period July 1, 2021, through February 11, 2022.
  - The timeliness of disabling IRIS Team Foundation Server (TFS) access privileges for the ten Division contractors with TFS access as of February 1, 2022, 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 for the security administrators as of February 2022.
  - The appropriateness of the three administrative user accounts and the two administrative service accounts as of January 27, 2022, for the Division network domain.
  - The adequacy of the security controls for the default *Administrator* account for the Division network domain.
  - The appropriateness of the 24 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 January 31, 2022.
  - The appropriateness of access for the 13 service accounts with direct access to the IRIS production database as of January 31, 2022.
  - The appropriateness of administrative-level access privileges assigned to the four accounts as of January 27, 2022, for a Division-managed high-risk network device.
- Evaluated the adequacy of Division IT asset (inventory) tracking controls for maintaining a complete, accurate, and up-to-date inventory of IRIS servers as of January 5, 2022.
- Evaluated the adequacy of user authentication controls for the IRIS application and database, the Division network domain, and a high-risk network device.
- Interviewed Division personnel and examined Division policies, procedures, and processes for IRIS program change requests, including change reconciliation processes and program code reviews. Specifically, we examined the 18 IRIS program change tickets representing 102 program changes implemented during the period July 2021 through January 2022, as documented on the implementation builds, to determine whether the program changes were appropriately authorized, reviewed, tested, approved for and implemented into production.
- Interviewed Division personnel and examined Division backup policies, procedures, and processes. Specifically, we examined:
  - The daily and weekly backup records for 12 of the 30 IRIS application and database servers as of January 22, 2022, to determine whether IRIS backups were successfully performed.
  - Examined IRIS backup recoverability testing records from October 2021 and January 2022 to determine whether quarterly IRIS application and database backup media recoverability testing was performed.
- Evaluated the adequacy of selected logging and monitoring controls.
- Evaluated the effectiveness of Division configuration management policies, procedures, and processes for IRIS database and database management software and the Division's high-risk network devices. Specifically, we evaluated whether as of January 27, 2022:
  - The database appliance was current and up to date.
  - IRIS database management software was timely patched.
  - The operating system on the server hosting the database management software and on each of the two database servers was supported and timely patched.
  - The operating system for a Division-managed high-risk network device was supported and timely patched.

- Evaluated IRIS business process application controls related to data input and processing. Specifically, we evaluated:
  - The timeliness of IRIS data correction controls for the 784 Investment Plan employer contribution variances identified during the period July 2021 through November 2021.
  - The adequacy of various IRIS data processing controls to help ensure the accuracy of service credit calculations for Florida Retirement System participants.
- 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

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

Department of
MANAGEMENT
SERVICES
▶ We Serve Those Who Serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
850-488-2786

Ron DeSantis, Governor
Pedro Allende, Secretary

September 16, 2022

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 information technology operational audit of the Department of Management Services, Integrated Retirement Information System. Our responses correspond with the findings and recommendations related to the Department of Management Services contained in the preliminary and tentative findings.

If further information is needed concerning our response, please contact Sarah Beth Hall, Inspector General, at 850-488-5285.

Sincerely,

Pedro Allende
Secretary

PA/tam

Enclosure

cc: Andrea B. Simpson, Director, Division of Retirement
Sarah B. Hall, Inspector General

Response to Preliminary and Tentative Audit Findings and Recommendations

Finding 1: Timely Disablement of IT Access Privileges

Access privileges to IRIS and related IT resources were not always promptly disabled when no longer necessary**.**

Recommendation: We recommend that Division management enhance controls to ensure that Department records evidence that former employee and contractor IRIS and TFS user access privileges are promptly disabled.

Management Response (planned corrective actions):

The Department and Division will work together to enhance controls to ensure that Department records evidence that former employee and contractor IRIS and TFS user access privileges are promptly disabled.

Finding 2: Periodic Review of Network Domain Access Privileges

As similarly noted in our report No. 2019-220, Department records did not evidence periodic reviews of the Department network domain privileged accounts' access privileges.

Recommendation: We again recommend that Department management conduct and document periodic access reviews of Department privileged network accounts in accordance with established policy.

Management Response (planned corrective actions):

The Department will ensure that periodic access reviews of Department privileged network accounts are conducted and documented in accordance with established policy.

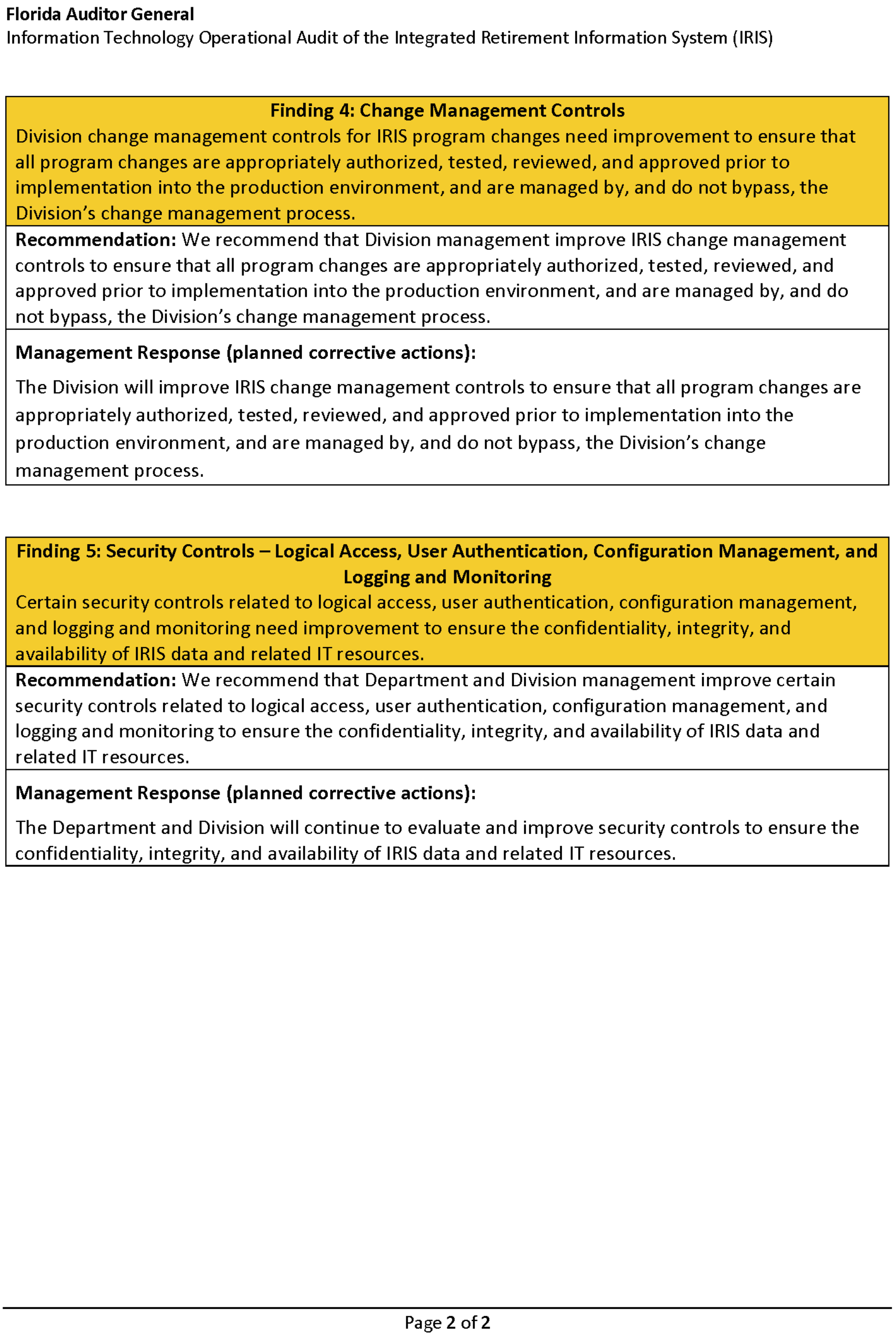
Finding 3: IRIS End-User Access Documentation

Division documentation of IRIS end-user role-based access privileges needs improvement to help ensure that IRIS end-user access is appropriately assigned.

Recommendation: We recommend that Division management improve IRIS end-user role documentation to ensure that all IRIS end-user roles and their associated access privileges are documented.

Management Response (planned corrective actions):

The Division will improve IRIS end-user role documentation to ensure that all IRIS end-user roles and their associated access privileges are documented.



Finding 4: Change Management Controls

Division change management controls for IRIS program changes need improvement to ensure that all program 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 recommend that Division management improve IRIS change management controls to ensure that all program 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.

Management Response (planned corrective actions):

The Division will improve IRIS change management controls to ensure that all program 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 5: Security Controls – Logical Access, User Authentication, Configuration Management, and Logging and Monitoring

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

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

Management Response (planned corrective actions):

The Department and Division will continue to evaluate and improve security controls to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.