CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

REPORT IA 22-502

OFFICE OF INSPECTOR GENERAL

AUDIT OF THE DEPARTMENT OF FINANCIAL SERVICES' DIVISION OF RISK MANAGEMENT, BUREAU OF STATE EMPLOYEE WORKERS' COMPENSATION CLAIMS, ACCESS TO CONFIDENTIAL DATA

Audit performed by the Office of Inspector General to evaluate the Department of Financial Services' Division of Risk Management, Bureau of State Employee Workers' Compensation Claims, access to confidential data

David T. Harper, Inspector General
Office of Inspector General
Department of Financial Services

April 15, 2022

CONTENTS

EXECUTIVE SUMMARY

The Department of Financial Services (DFS), Office of Inspector General (OIG) conducted an audit of the DFS Division of Risk Management (DRM), Bureau of State Employee Workers' Compensation Claims (WC). The overall purpose of this audit was to determine if the DRM uses effective user access controls to manage access to WC's information technology (IT) application, Origami Information Management System. The OIG's objective was to determine if established IT controls effectively manage user access to Origami.

Effective IT general controls are required to maintain data confidentiality, integrity, and availability. Origami maintains confidential information used by the Bureau to perform their job duties. The audit disclosed that there are opportunities for WC to strengthen user access controls in Origami. The Department can strengthen their controls by updating their policies and procedures surrounding user access control, ensuring timely user access termination, and developing policies and procedures related to the monitoring, downloading and storage of confidential data in Origami.

INTRODUCTION, BACKGROUND, AUDIT OBJECTIVE AND SCOPE

Introduction

The Office of Inspector General (OIG) Audit Section conducted an audit of confidential data access controls for the Department of Financial Services' (DFS) Division of Risk Management (DRM), Bureau of State Employee Workers' Compensation Claims (WC). This audit was based on OIG's Fiscal Year (FY) 2020-2021 Annual Audit Work Plan and was conducted in conformance with professional standards.

Background

The DRM ensures that participating Florida agencies and universities receive assistance in managing risk and quality workers' compensation, liability, federal civil rights, automobile liability, and property insurance coverage at reasonable rates by providing self-insurance, purchase of insurance, and claims administration[1]. The DRM is divided into three bureaus: Risk Financing and Loss Prevention, State Employee Workers' Compensation Claims, and State Liability and Property Claims.

The Bureau of State Employee Workers' Compensation Claims is responsible for the administration of all workers' compensation claims filed by state and university employees and volunteers. During the 2019-2020 FY, the Bureau received 11,399 new claims and paid $106.5 million in medical and indemnity benefits. The Bureau's information technology (IT) application is Origami Information Management System. The application is critical to the Division's ability to efficiently and effectively process claims[2]. Origami houses the confidential data used by WC to perform claim adjustments. The Bureau of Risk Financing and Loss Prevention provides administrative support to WC which includes IT administrative support for Origami. During the 2019-2020 FY, Origami was improved to increase efficiency. New features were added to automate and streamline claims process.

Audit Objective and Scope

The audit's objective was to determine the effectiveness of selected Information Technology (IT) controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules and other guidelines; and ensuring the confidentiality, integrity, availability, and the safeguarding if IT resources.

The scope included the review of Division documentation and other evidence, for the audit period of July 1, 2019 through June 30, 2020, to ensure Division staff implemented and followed proper user access controls. In certain cases, the timeline was modified to account for agency retention schedules. The audit focused on the Division's main IT system, Origami Information Management System.

FINDINGS AND RECOMMENDATIONS

Finding 1: Authorization Documentation

Stated in DFS AP&Ps[3], Access Control Administrators (ACA) are to maintain access control records and comply with retention timelines established in State of Florida General Records Schedule for State and Local Government Agencies (GS1-SL). According to the GS1-SL[4], all employee access

[1] Department of Financial Services. (2021). *Division of Risk Management Fiscal Year 2020 Annual Report, p.* 2

[2] *Division of Risk Management Fiscal Year 2020 Annual Report,* pp. 3-4

[3] DFS AP&P 4-05 Application Access Control section VI. C, effective date January 16, 2013

[4] Florida Department of State GS1-SL Item #189

documentation must be stored for a minimum of one anniversary year after an employee's access rights are terminated.

The Division's IP&Ps[5] requires the ACA comply with GS1-SL regarding the maintenance of access control records. The Bureau utilizes Origami Access Request forms, implemented towards the end of 2016, to document access control authorizations. The OIG found that the Bureau could not produce an Origami Access Request form for seven of twenty-two (31.82%) employees included in the test.

Through inquiry, leadership indicated that COVID-19 disruptions caused access request forms to be overlooked or forgotten in some cases. In those cases, the Bureau had email documentation of the request. Also, changes in staff and their policy regarding the use of access request forms meant some documentation was either not stored or was misplaced.

Absent documentation to support that the user was authorized to access the system, the risk is increased that a user will have inappropriate access to confidential data, which in turn, increases the risk that confidential data may be inadvertently released to unauthorized parties.

Recommendation

The OIG recommends that the Bureau update their policies and procedures to include saving the Origami Access Request forms of all employees for the time established in the GS1-SL which requires that access control forms be maintained for one anniversary year after an employee's access rights are terminated.

Finding 2: Access Deactivation

The Department's AP&P 4-05[6] states that keeping open user accounts after the date of the user's separation is a security risk and is prohibited. AP&P 4-03[7] requires the Divisions to deactivate a user's access to IT applications on the day of an employee's separation. Per GS1-SL item #89, documentation of termination of user access must be retained for at least one anniversary year of the date of separation.

The OIG found that four of twelve separated WC employees (33.3%), did not have their access removed within the timeframe established by DFS AP&P 4-03. The documentation provided by the Bureau shows that their access to Origami was removed one to four days after separation.

Division leadership explained that they were unaware that some users' access to Origami was not terminated on the day of separation. The Bureau indicated that they don't keep documentation of the date a user's access to Origami is terminated.

Absent an effective process for the immediate removal of credentials, held by separating employees, the risk is increased that the credentials could be used to access and obtain confidential data without the Bureau's knowledge.

Recommendation

The OIG recommends that the Bureau terminate access to Origami on the day of employee separation and maintain that documentation for the time established in the General Records Schedule GS1-SL.

[5] DRM WC IP&P 3.81 IMS Access Control section VI. CI. 6

[6] DFS AP&P 4-05 section VI

[7] DFS AP&P 4-03 IT Security Policy section X. N. 11, effective date December 26, 2013

Finding 3: Security Controls– Logging, Monitoring, and Downloads

Security controls protect the confidentiality, integrity, and availability of data and IT resources. This audit disclosed that certain security controls related to logging, monitoring, and downloads need improvement. The OIG is not disclosing specific details of the issues in this report to avoid the possibility of compromising Origami data. However, the OIG have notified appropriate Division leadership of the specific issues.

Recommendation

We recommend that Division leadership improve certain security controls related to logging, monitoring, and downloads to ensure the integrity of Origami data.

METHODOLOGY

This IT operational audit conforms with The International Professional Practices Framework (IPPF), published by The Institute of Internal Auditors. The IPPF requires the OIG to consider risk when planning to perform the audit and obtain enough appropriate evidence to provide a reasonable basis for findings and conclusions that align with audit objectives. Additionally, the IPPF requires the auditors to meet objectivity requirements and possess necessary collective knowledge, skills and experience. The audit evidence obtained provides a reasonable basis for the OIG findings and conclusions.

To accomplish audit objectives, the OIG performed the following audit procedures:

- Conducted research to identify national, statewide, and agency-specific requirements, including GAO FISCAM chapter 3.2 *Access Controls*; Rule 60GG-2 F.A.C., *Information Technology Security*; DFS Administrative Policy and Procedure 4-03 *Information Technology Security Policy* and 4-05 *Application Access Control*; DRM Policy and Procedure 3.80 *DRM Compliance with DIS P&Ps* and 3.81 *IMS Access Control*
- Conducted interviews with key Division personnel, including fraud interviews
- Examined supporting documentation from Division personnel
- Performed test of user authorization
- Performed test of user authentication
- Performed test of access appropriateness
- Performed test of administrative access
- Performed test of user access reviews
- Performed test of user access deactivation
- Performed test of logging and monitoring
- Determined whether the Bureau's controls managed user access

ACKNOWLEDGEMENTS

The OIG would like to thank Division of Risk Management leadership and staff for their input, cooperation and assistance throughout the performance of this engagement.

The Office of Inspector General performs audits, consulting activities, and reviews of Department of Financial Services' programs, activities, and functions to promote accountability, integrity, and efficiency in state government.

This consulting engagement was conducted in conformance with The *International Standards for the Professional Practice of Internal Auditing*, published by The Institute of Internal Auditors, Inc., pursuant to Section 20.055, Florida Statutes, and *Principles and Standards for Offices of Inspectors General,* published by the Association of Inspectors General. This engagement was conducted by Jasmine London, Auditor, under the supervision of Debbie Clark, CPA, CISA, CIGA, Director of Audit.

Please address inquiries regarding this report to the DFS Office of Inspector General at 850-413-3112.

DISTRIBUTION LIST

Jimmy Patronis, Chief Financial Officer
Peter Penrod, Chief of Staff
Scott Fennell, Deputy Chief Financial Officer, Operations
Molly Merry, Director, Division of Risk Management
Sherrill Norman, Florida Auditor General

ATTACHMENT

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding 1: Authorization Documentation

Stated in DFS AP&Ps, Access Control Administrators (ACA) are to maintain access control records and comply with retention timelines established in State of Florida General Records Schedule for State and Local Government Agencies (GS1-SL). According to the GS1-SL, all employee access documentation must be stored for a minimum of one anniversary year after an employee's access rights are terminated.

The Division's IP&Ps requires the ACA comply with GS1-SL regarding the maintenance of access control records. The Bureau utilizes Origami Access Request forms, implemented towards the end of 2016, to document access control authorizations. The OIG found that the Bureau could not produce an Origami Access Request form for seven of twenty-two (31.82%) employees included in the test.

Through inquiry, leadership indicated that COVID-19 disruptions caused access request forms to be overlooked or forgotten in some cases. In those cases, the Bureau had email documentation of the request. Also, changes in policy, regarding the use of access request forms, and staff meant some documentation was either not stored or was misplaced.

Absent documentation to support that the user was authorized to access the system, the risk is increased that a user will have inappropriate access to confidential data which in turn, increases the risk that confidential data may be inadvertently released to unauthorized parties.

Recommendation

The OIG recommends that the Bureau update their policies and procedures to include saving the Origami Access Request forms of all employees for the time established in the GS1-SL which requires that access control forms be maintained for one anniversary year after an employee's access rights are terminated.

Response:

We agree the Division needs to update policies and procedures to accomplish this objective. The Division has implemented process updates that ensure system access is not granted with an email request only, but with a completed access request form. In addition, access request forms will be filed and maintained in accordance with GS1-SL.

The Division is revising the Division's IP&P #3.81 to clarify the use and maintenance of access request forms and document retention in accordance with the State of Florida Records Schedule for State and Local Government Agencies.

Expected Completion Date for Corrective Action: July 1, 2022

Finding 2: Access Deactivation

The Department's AP&P 4-05 states that keeping open user accounts after the date of the user's separation is a security risk and is prohibited. AP&P 4-03 requires the Divisions to deactivate a user's access to IT applications on the day of an employee's separation. Per GS1-SL item #89, documentation of termination of user access must be retained for at least one anniversary year of the date of separation.

The OIG found that four of twelve separated WC employees (33.3%), did not have their access removed within the timeframe established by DFS AP&P 4-03. The documentation provided by the Bureau shows that their access to Origami was removed one to four days after separation.

Division leadership explained that they were unaware that some users' access to Origami was not terminated on the day of separation. The Bureau indicated that they don't keep documentation of the date a user's access to Origami is terminated.

Absent an effective process for the immediate removal of credentials, held by separating employees, the risk is increased that the credentials could be used to access and obtain confidential data without the Bureau's knowledge.

Recommendation

The OIG recommends that the Bureau terminate access to Origami on the day of employee separation and maintain that documentation for the time established in the General Records Schedule GS1-SL.

Response:

We agree the Division needs to strengthen policies and procedures to accomplish this objective. The Division has implemented process updates that ensure termination of system access at the time of separation and terminating access request forms are filed and maintained for one year after access termination.

The Division will update and revise as appropriate the Division's policies and procedures to clarify the timeframe for access termination and the retention of access termination documentation in accordance with the State of Florida Records Schedule for State and Local Government Agencies. In addition, the Division has initiated a review of the access termination process to identify areas where process improvements can be made, and additional internal controls established.

Expected Completion Date for Corrective Action: July 1, 2022

Finding 3: Security Controls– Logging, Monitoring, and Downloads

Security controls protect the confidentiality, integrity, and availability of data and IT resources. This audit disclosed that certain security controls related to logging, monitoring, and downloads need improvement. The OIG is not disclosing specific details of the issues in this report to avoid the possibility of compromising Origami data. However, the OIG have notified appropriate Division leadership of the specific issues.

Recommendation

We recommend that Division leadership improve certain security controls related to logging, monitoring, and downloads to ensure the integrity of Origami data.

Response:

We agree the Division needs to strengthen policies and procedures to accomplish this objective. The Division will update and revise as appropriate the Division's policies and procedures to clarify and strengthen security controls related to Origami data.

The Division has initiated a review of security controls and reporting to identify areas where process improvements can be made, and additional internal controls established. The review includes discussions with Origami and the Department's Office of Information Technology regarding the appropriate steps to achieve this goal.

Expected Completion Date for Corrective Action: October 1, 2022