REPORT NO. 2015-096
FEBRUARY 2015

DEPARTMENT OF FINANCIAL SERVICES

INVESTMENT ACCOUNTING SYSTEM (IAS)
AND
CASH MANAGEMENT SUBSYSTEM (CMS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

CHIEF FINANCIAL OFFICER

Pursuant to Article IV, Sections 4.(c) and 5.(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Jeff Atwater served as Chief Financial Officer during the period of our audit.

The audit team leaders were Andrew Von Euw and Debra Clark, CPA, 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 can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF FINANCIAL SERVICES

Investment Accounting System (IAS)
and
Cash Management Subsystem (CMS)

SUMMARY

The Chief Financial Officer (CFO) is the head of the Department of Financial Services (Department) and as the chief fiscal officer of the State is responsible for settling and approving accounts against the State and keeping all State funds and securities. The CFO is designated the cash management officer for the State and is charged with the coordination and supervision of procedures providing for the efficient handling of financial assets under the control of the Division of Treasury (State Treasury) and each of the various State agencies and of the judicial branch. The State Treasury receives and disburses cash, invests available balances, and performs related accounting functions, cash management operations, and consultations.

Section 215.94(3), Florida Statutes, provides that the CFO shall be the functional owner of the Cash Management Subsystem (CMS) (a subsystem of the Florida Financial Management Information System), and that the CMS shall include, but shall not be limited to, functions for:

(a) Recording and reconciling credits and debits to State Treasury fund accounts.

(b) Monitoring cash levels and activities in State bank accounts.

(c) Monitoring short-term investments of idle cash.

(d) Administering the provisions of the Federal Cash Management Improvement Act of 1990.

The State Treasury operates separate business applications, including the Investment Accounting System (IAS), that collectively comprise the CMS. The State Treasury has completed Phase 1 of an upgrade to the CMS that included the Verifies, Receipts, and Chargebacks business applications. The remaining CMS business applications continue to operate as legacy systems. The State Treasury uses the legacy IAS to account for all investments made by the State Treasury and the upgraded CMS to process and store agency deposit details, to balance and store daily deposit and returned item details, and to account for all returned items charged to the State Treasury.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to the legacy IAS and the upgraded CMS. We also determined the status of corrective actions regarding audit findings included in our report No. 2011-173 that were applicable to the scope of this audit.

Our audit disclosed areas in which improvements in IAS and CMS controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: The access privileges of some users did not promote an appropriate separation of duties or restrict users to only those functions necessary for their assigned job duties related to IAS and CMS IT resources.

Finding No. 2: Department procedures for the periodic review of CMS user access privileges needed improvement.

Finding No. 3: Program change controls needed improvement to ensure that all program changes implemented into the IAS and CMS production environments were properly authorized.

Finding No. 4: Certain security controls related to IAS user authentication, security administration activity logging, and transaction logging needed improvement.

BACKGROUND

Section 17.57(1), Florida Statutes, states that the Chief Financial Officer (CFO), or other parties with the permission of the CFO, shall deposit the money of the State or any money in the Division of Treasury (State Treasury) in such qualified public depositories of the State as will offer satisfactory collateral security for such deposits. It is the duty of the CFO, consistent with the cash requirements of the State, to keep such money fully invested or deposited in order that the State may realize maximum earnings and benefits. Pursuant to Section 17.555, Florida Statutes, the State Treasury shall, among other things, account for all State funds and securities.

The CFO is the constitutional officer with the fiduciary responsibility over the State Treasury. As a core function of the Department, the State Treasury ensures that State moneys, employee deferred compensation contributions, State and local governments' public funds on deposit in Florida banks and savings associations, and cash and other assets held for safekeeping by the CFO are adequately accounted for, invested, and protected.

Within the State Treasury, the Bureau of Funds Management is responsible for posting State receipts and disbursements, performing cash management services, and investing available funds. The State Treasury receives and disburses cash; invests available balances; and performs related accounting functions, cash management operations, and consultations. The State Treasury operates several separate business applications known collectively as the Cash Management Subsystem (CMS) to carry out its responsibilities of monitoring cash levels and activities in State bank accounts, for keeping detailed records of cash transactions and investments for State agencies, and paying warrants and other payments issued by the CFO. The CMS interfaces with the Florida Accounting Information Resource Subsystem (FLAIR), Department of Revenue systems, other State agency systems, and bank business partner systems.

The State Treasury was in the process of upgrading the current CMS platform to a Web-based system in two phases. Phase 1 went live in August 2013. It established a new integrated platform and replaced three existing business applications including Verifies, Receipts, and Chargebacks. Phase 2 was to replace the remaining CMS legacy business applications, including the Investment Accounting System (IAS) used to account for all investments made to the State Treasury, and add the capabilities to the new integrated CMS platform developed in Phase 1. Phase 2 was cancelled as of July 16, 2014, because it will be included in the FLAIR and CMS replacement project as recommended in the Department's *FLAIR Study*.[1]

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to data and IT resources that promote an appropriate separation of job duties and that restrict employees to only those functions necessary for their assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, or destruction. Our audit disclosed that some inappropriate and unnecessary access privileges existed to IAS production libraries, the CMS application, and the related CMS database management system as discussed in the following paragraphs:

[1] The *FLAIR Study*, with a final acceptance date of April 9, 2014, was performed as a result of Section 6 of the 2013 General Appropriations Act with the purpose of completing a study and recommending either enhancing FLAIR or replacing FLAIR together with other related subsystems including CMS.

IAS Production Libraries

We reviewed 16 active user accounts with access to the IAS production libraries as of June 30, 2014. Our review disclosed that 4 of the 16 user accounts belonged to developers that were granted inappropriate and unnecessary access privileges to the IAS production libraries. Specifically, the developers were granted access to both read and execute permissions for objects within the production libraries. In addition to the 4 user accounts, 1 of the 16 user accounts was a test environment user account that was granted inappropriate access privileges to read and execute permissions for objects within the production libraries. A similar finding was noted in prior audits of the Department, most recently our report No. 2011-173.

CMS Application

CMS users include users from all State agencies (external users) and users within the State Treasury (internal users). We reviewed 6 of 35 active internal CMS user accounts as of October 1, 2014. Our audit disclosed that 1 of the 6 user accounts was granted inappropriate and unnecessary update access privileges to the CMS. Specifically, the lead CMS application developer had update access privileges within the CMS application as an end user. This level of access within the application was not appropriate for application developers as it was contrary to an appropriate separation of application program development and application end-user duties.

Through additional audit procedures, we identified that inappropriate update access privileges were granted to the CMS users through the internal auditor role. A programming flaw existed within the CMS application that allowed user accounts with the internal auditor role to perform some administrator functions related to user access within the CMS. Specifically, a user account with the internal auditor role could enable internal and external roles for use within the CMS, disable internal and external roles from being used within the CMS, and could remove or add specific permissions within the roles. However, according to Department management, the internal auditor role was assigned as a read-only role within the CMS. Department management further stated that the programming flaw was within the application and allowed the inappropriate update access privileges to any read-only role. Upon notifying the Department of this condition, Department management indicated that immediate corrective action was being taken.

CMS Database Management System

Our review of 12 active user accounts with update access privileges to the CMS database management system as of October 9, 2014, disclosed 4 inappropriate user accounts. Specifically, 4 application developers, 1 of whom had terminated employment with the Department, had read and execute access privileges to the CMS database management system that were not appropriate or necessary for their job duties.

Inappropriate and unnecessary access privileges to the IAS production libraries, the CMS application, and the related CMS database management system increases the risk of unauthorized or erroneous disclosure, modification, or destruction of IAS and CMS data.

Recommendation: The Department should limit user access privileges to IAS and CMS IT resources to promote an appropriate separation of duties and to restrict users to only those functions necessary for their assigned job duties.

Finding No. 2: Periodic Review of CMS User Access Privileges

Agency for Enterprise Information Technology (AEIT)[2] Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that only authorized individuals have access and that the access provided to each user remains appropriate.

Our audit disclosed that the Department had a monthly process in place to review all users with CMS access privileges. The CMS utilized a single sign-on that is the front-end interface for State Treasury applications to authenticate internal Department users. The monthly access control process was based on a *Single Sign-on Funds Management Applications Monthly User Access Report* (*Report*) that included user access control lists by application for all State Treasury applications. This *Report* identified single sign-on users for each application but did not identify all of the CMS roles assigned to each user. As a result, management could not be assured that the periodic reviews of all users with CMS access privileges were adequate and, in turn, that the defined access privileges continued to be appropriate. Without adequate periodic reviews of all users with CMS access privileges that includes the assigned CMS roles, the risk is increased that inappropriate CMS user access privileges may exist and not be timely detected.

Recommendation: The Department should improve the periodic review procedures of CMS user access privileges by including all CMS user roles assigned to ensure the continued appropriateness of CMS user access privileges.

Finding No. 3: IAS and CMS Program Change Controls

Effective controls over modification of application programs help ensure that only authorized program changes are implemented. The effectiveness of ensuring that only authorized program changes are implemented is enhanced when automated reports or system logs of program changes are generated and reviewed.

The Department did not have a process in place to ensure that all program changes implemented into the IAS and CMS production environments were properly authorized. A similar finding regarding program changes made to the production environments was noted in prior audits of the Department, most recently our report No. 2011-173. Without a process for ensuring that all program changes implemented into the IAS and CMS production environments are authorized program changes that have gone through the appropriate program change control procedures, the risk is increased that erroneous or unauthorized program changes, should they be moved into the production environment, will not be timely detected by management.

Recommendation: The Department should implement a process to ensure that all program changes implemented into the IAS and CMS production environments are properly authorized.

[2] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, in effect as of November 15, 2010; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

Finding No. 4: Security Controls – IAS User Authentication, Security Administration Activity Logging, and Transaction Logging

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls related to IAS user authentication, security administration activity logging, and transaction logging that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising IAS data and IT resources. However, we have notified appropriate Department management of the specific issues. A similar finding regarding security administration activity logging was communicated to Department management in connection with our report No. 2011-173 and a similar finding regarding user authentication was communicated to Department management in connection with prior audits of the Department, most recently our report No. 2011-173.

Weaknesses in security controls related to IAS user authentication, security administration activity logging, and transaction logging result in an increased risk that the confidentiality, integrity, and availability of IAS data and IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls related to IAS user authentication, security administration activity logging, and transaction logging to ensure the continued confidentiality, integrity, and availability of IAS data and IT resources.

PRIOR AUDIT FOLLOW-UP

IAS

The Department had taken corrective actions for one of the five findings included in our report No. 2011-173 that were applicable to the scope of this audit. Corrective actions were not taken for one of the five prior audit findings as described in the findings above. In addition, two prior audit findings were only partially corrected. There was no occasion to correct one of the prior audit findings included in our report No. 2011-173.

CMS

The Department had taken corrective actions for three of the five findings included in our report No. 2011-173 that were applicable to the scope of this audit. One prior audit finding was only partially corrected. There was no occasion to correct one of the prior audit findings included in our report No. 2011-173.

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 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational 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.

The scope of our audit focused on evaluating selected business process application controls over transaction data input, processing, and output applicable to the IAS during the period June 2014 through August 2014 and selected actions from January 1, 2014, and applicable to the CMS during the period July 2014 through October 2014 and selected actions from January 1, 2014. The audit also included selected application-level general controls related to security management, application access, and configuration management. An additional objective was to determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2011-173 that were applicable to the scope of this audit.

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

As described in more detail below, for the IT systems and controls included within the scope of our 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 our audit; obtaining an understanding of the IT systems 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our 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 our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of data input, processing, and output controls that ensure the completeness, accuracy, validity, and confidentiality of data input into the IAS and the CMS.
- Observed and evaluated selected transaction data input, processing, and output controls that ensure the completeness, accuracy, validity, and confidentiality of IAS and CMS data.
- Evaluated the adequacy of application transaction logging for the IAS and the CMS. Specifically, we made inquiries of management regarding the logging capabilities of the IAS as of July 22, 2014, and reviewed a CMS transaction log as of October 28, 2014.
- Evaluated application security management controls related to the IAS and the CMS, including the application security plans and the security awareness program.

- Evaluated the adequacy of security administration activity logging related to the IAS and the CMS. Specifically, we made inquiries of management regarding the security administration activity logging capabilities related to the IAS as of August 6, 2014, and reviewed a CMS access change log as of October 7, 2014.
- Evaluated the effectiveness of selected user authentication controls for the IAS and the CMS. Specifically, we reviewed Department policies and other documentation regarding authentication settings and we reviewed authentication settings to determine if the settings were sufficient to restrict access.
- Evaluated the effectiveness of selected access controls to ensure that access privileges to the IAS and the CMS were appropriately authorized. Specifically, we reviewed the access authorization forms as of July 1, 2014, for all 7 IAS users and the access authorization forms as of October 1, 2014, for 6 of 35 CMS users to determine if the access privileges granted were authorized.
- Evaluated the effectiveness of selected logical access controls for the IAS and the CMS to ensure that user access privileges were appropriately restricted. Specifically, we reviewed user access privileges as of July 1, 2014, for all 7 IAS users and the user access privileges as of October 1, 2014, for 6 of 35 CMS users to determine if the access privileges granted were appropriate.
- Evaluated the appropriateness of user account access privileges to the production system libraries for the IAS. Specifically, we reviewed the access privileges for all 16 user accounts with access to the production system libraries for the IAS including special permissions and the ability to update objects or data within the libraries as of June 30, 2014. We also evaluated the password settings for the user accounts accessing the production system libraries for the IAS as of August 22, 2014.
- Evaluated the appropriateness of user server access privileges to the CMS database file, log file, and backups residing on the server. Specifically, we reviewed the access privileges related to 7 of 41 CMS files on the production server as of October 14, 2014.
- Evaluated the appropriateness of user database access privileges to the CMS database management system. Specifically, we reviewed the access privileges for all 12 user accounts with access to the CMS database management system as of October 9, 2014.
- Evaluated the effectiveness of application configuration management controls related to the IAS and the CMS. Specifically, we reviewed all 8 IAS program change requests that were closed between January 1, 2014, and July 8, 2014, and 11 of 104 CMS program change requests that were closed between January 1, 2014, and September 24, 2014, to determine whether the program changes were appropriately authorized, documented, tested by an independent party, and authorized and implemented into the production environments.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing 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 those matters requiring corrective action.

AUTHORITY

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.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated February 5, 2015, the Chief Financial Officer provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

February 5, 2015

Mr. David W. Martin
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(3)(b), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's information technology operational audit of the *Department of Financial Services, Cash Management Subsystem (CMS) and Investment Accounting System (IAS).*

If you have any questions concerning this response, please contact Teresa Michael, Inspector General, at (850) 413-4970.

Sincerely,

Jeff Atwater

JA:rlg

Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 FAX (850) 413-2950

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
Investment Accounting System (IAS) and Cash Management Subsystem (CMS)

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Appropriateness of Access Privileges

The access privileges of some users did not promote an appropriate separation of duties or restrict users to only those functions necessary for their assigned job duties related to IAS and CMS IT resources.

Recommendation: The Department should limit user access privileges to IAS and CMS IT resources to promote an appropriate separation of duties and to restrict users to only those functions necessary for their assigned job duties.

Response: We concur. The IAS Production Library access for the four developers noted to have inappropriate access was terminated on September 11, 2014. Also, the Division of Information Systems is currently exploring options to address the test environment user account execute access to the production libraries. The CMS Application access for the one developer noted as having inappropriate access was removed on January 20, 2015. Additionally, the CMS internal auditor role correction was moved into production on December 18, 2014. As of October 29, 2014, changes to remove unnecessary access to the CMS Database Management System were complete.

The Department will continue to monitor access to the systems to ensure that it remains appropriate on an ongoing basis.

Expected Completion Date for Corrective Action: Ongoing

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
Investment Accounting System (IAS) and Cash Management Subsystem (CMS)

Finding No. 2: Periodic Review of CMS User Access Privileges

Department procedures for the periodic review of CMS user access privileges needed improvement.

Recommendation: The Department should improve the periodic review procedures of CMS user access privileges by including all CMS user roles assigned to ensure the continued appropriateness of CMS user access privileges.

Response: We concur. The Department will pursue the addition of user roles to the monthly CMS user access reviews.

Expected Completion Date for Corrective Action: February 1, 2015

2

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
Investment Accounting System (IAS) and
Cash Management Subsystem (CMS)

Finding No. 3: IAS and CMS Program Change Controls

Program change controls needed improvement to ensure that all program changes implemented into the IAS and CMS production environments were properly authorized.

Recommendation: The Department should implement a process to ensure that all program changes implemented into the IAS and CMS production environments are properly authorized.

Response: The Department is evaluating the comprehensive change management process to determine whether additional controls for monitoring program changes would provide further assurance that all production environment changes are authorized.

Expected Completion Date for Corrective Action: December 2015

3

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
Investment Accounting System (IAS) and
Cash Management Subsystem (CMS)

Finding No. 4: Security Controls – IAS User Authentication, Security Administration Activity Logging, and Transaction Logging

Certain security controls related to IAS user authentication, security administration activity logging, and transaction logging needed improvement.

Recommendation: The Department should implement appropriate security controls related to IAS user authentication, security administration activity logging, and transaction logging to ensure the continued confidentiality, integrity, and availability of IAS data and IT resources.

Response: We concur. The Department will continue to evaluate and address security controls, as appropriate.

Expected Completion Date for Corrective Action: Ongoing

4