REPORT NO. 2009-032
NOVEMBER 2008

OFFICE OF INSURANCE REGULATION

FINANCIAL ANALYSIS AND MONITORING ELECTRONIC DOCUMENT MANAGEMENT SYSTEM (FAME)

Operational Audit

March 2006 through February 2008

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

COMMISSIONER OF INSURANCE REGULATION

The Office of Insurance Regulation (OIR) is administratively housed within the Department of Financial Services (DFS), but operates under the direction of the Financial Services Commission which consists of the Governor, Attorney General, Chief Financial Officer, and Commissioner of Agriculture. The Commission is responsible for appointing the Director of the Office of Insurance Regulation, who may also be known as the Commissioner of Insurance Regulation. Kevin M. McCarty served as Commissioner during the audit period.

This audit was conducted by Melisa Hevey, CPA, and supervised by Richard Munson, CPA. Please address inquiries regarding this report to Nancy Tucker, CPA, Audit Manager, by e-mail (nancytucker@aud.state.fl.us) or by telephone (850-487-4370).

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.myflorida.com/audgen); by telephone (850-487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

OFFICE OF INSURANCE REGULATION

Financial Analysis and Monitoring Electronic Document Management System (FAME)

SUMMARY

This operational audit focused on selected general and application controls related to the Financial Analysis and Monitoring Electronic Document Management System (FAME) of the Office of Insurance Regulation (OIR). Our audit, covering the period March 2006 through February 2008, also included a follow-up on prior audit findings contained in audit report No. 2007-088, Viatical Settlement Regulation and Market Conduct Examinations. Our audit disclosed the following:

CHANGE MANAGEMENT

Finding No. 1: OIR change management controls should be enhanced. OIR staff could not always provide documentation to evidence program change requests and approvals, or subsequent user acceptance testing and approval.

USER ACCESS

Finding No. 2: OIR had not established written policies and procedures related to FAME user access. Additionally, OIR logical access controls over FAME needed improvement.

SCANNING AND INDEXING

Finding No. 3: OIR scanning and indexing procedures should be enhanced to better ensure that information is accurately and completely entered into FAME.

BACKGROUND

The Office of Insurance Regulation (OIR) is responsible for the enforcement of statutes and rules related to the business of insurance and the monitoring of industry markets. In connection with these responsibilities, OIR is to provide regulatory oversight of company solvency, policy forms and rates, market conduct performance, and new company entrants to the Florida market.

Upon licensure by OIR to do business in Florida, insurance companies are required to submit financial filings according to the methods and schedules prescribed by Chapter 624, Florida Statutes. OIR financial oversight business units, including Property and Casualty Financial Oversight, Life and Health Financial Oversight, and Specialty Product Administration, are responsible for reviewing financial filings and monitoring solvency of entities licensed to do business in the State of Florida. Collectively, these business units received 3,159 and 3,326 annual financial filings for the 2006 and 2007 calendar years, respectively.

The Market Research and Technology business unit of OIR is responsible for oversight of OIR information technology (IT) systems, including FAME. FAME supports the administration of OIR regulatory responsibilities relating to financial oversight. Specifically, electronically submitted financial filings are automatically uploaded to FAME and paper financial filings submitted via mail are scanned, indexed, and uploaded to FAME. Financial filings include insurance company contact information, annual financial statements, reinsurance and actuarial information, and certificates of compliance.

FAME also serves as a primary data source when OIR compiles information related to Florida's insurance markets. As financial filings are received and uploaded, FAME also provides for electronic management of financial examiner

work flow as it includes information related to the status, routing, correspondence, tracking, and supervisory review of each examiner's assignments.

During the audit period, OIR entered into a staff augmentation contract for programming services related to FAME as well as other OIR systems. The contracted programmer reported to the Market Research and Technology business unit.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Change Management

Effective change management controls should be in place over program changes to ensure that only authorized and properly functioning changes are implemented. Change management controls include procedures to ensure that all program changes are properly authorized, tested, and approved prior to their implementation.

DFS Administrative Policies and Procedures, Change Management and Control Policy 4-17, required OIR to follow DFS Division of Information Systems (Division) Change Management Procedures. These procedures required that all requests for program changes be processed through the Division Change Management System (CMS). CMS was designed to facilitate program changes including the documentation, notification, authorization, and review of all changes. Upon receipt of a request, a change management request number was automatically assigned by CMS.

In response to our request for a listing of FAME program changes made during the audit period, OIR staff identified 62 program changes. As required by the contract between OIR and the contracted programmer, to monitor the progress of requested program changes, OIR was to receive Project Status Reports[1] from the contracted programmer. Our review of OIR change management controls and selected Project Status Reports disclosed that:

- Project Status Reports did not contain a field for change management request numbers, information necessary to correlate the work reported on the Project Status Report to entries in CMS. Without the change management request number, OIR staff were unable to locate CMS records to provide documentation of change requests and approvals for 11 of 20 (55 percent) program changes we reviewed.
- Sound business practices for program changes include final user acceptance testing and approval prior to placing the change into production. Under OIR procedures, the contracted programmer required that users or requestors test and approve changes prior to moving the changes into production. Our audit disclosed that OIR staff were unable to provide documentation of user acceptance testing and approval for 18 of 20 (90 percent) program changes we reviewed. In response to our inquiry, OIR indicated that during user acceptance testing programmers and users or requestors primarily communicated by e-mail or telephone.

Absent sufficient documentation of program changes including requests, approvals, and user acceptance testing, the risk is increased that erroneous or unauthorized program changes may be placed in production.

Recommendation: To enhance change management controls, OIR should request that Project Status Reports include change management request numbers. OIR should also ensure that documentation of user acceptance testing and approval is maintained.

Finding No. 2: User Access

Effective security administration procedures reduce the risk of unauthorized access to a system by ensuring that:

- Appropriate and timely action is taken to request, approve, assign, and remove user access accounts;

[1] Project Status Reports were designed by DFS, Division of Information Systems Project Management Office, and were to be completed electronically.

- User access privileges are periodically reviewed; and
- Necessary logical access controls relating to the management of access privileges are in place.

OIR did not have written policies and procedures in place for FAME that addressed these matters. In response to our inquiries, OIR staff stated that while procedures have not been reduced to writing, in practice, a series of steps were taken when establishing and removing FAME user access. However, our review of FAME user access disclosed the following deficiencies:

- For 15 of 20 (75 percent) users' access tested, OIR staff could not provide documentation to evidence approval of user access accounts.
- For 3 of 7 (42.9 percent) users who had terminated employment during the audit period, user access was not timely removed. For the 3 employees, removal of user access occurred 4 days, 111 days, and 365 days, respectively, from the date the employee terminated.
- OIR staff did not periodically review user access privileges to ensure that access privileges remained appropriate.
- Certain other logical access controls relating to the management of access privileges needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising OIR data and IT resources. However, appropriate OIR personnel have been notified of these issues.

Unauthorized access to IT resources increases the potential for malicious or unintentional disclosure, modification, or destruction of data and IT resources. Documenting and periodically reviewing the approval and assignment of user access accounts, timely revoking the access of terminated employees, and properly managing access privileges are effective procedures that decrease the risk of unauthorized access.

Recommendation: To minimize the risk of compromising OIR data and IT resources, OIR should establish and implement written procedures that address requesting, approving, assigning, reviewing, and removing user access accounts. OIR should ensure that these procedures require the revocation of access privileges immediately upon employee termination. Further, OIR should strengthen its IT security controls related to the management of access privileges.

Finding No. 3: Scanning and Indexing

Effective data input controls, such as data verification through supervisory or independent review and approval, ensure the accuracy, completeness, and timeliness of data during its conversion from its original source into computer data or entry into a computer application.

OIR used scanning and indexing to convert paper documents sent from insurance companies into electronic formats to be stored in FAME. Our audit disclosed OIR scanning and indexing guidelines did not include provisions for supervisory or independent review of information scanned and stored in FAME.

In response to our inquiry, OIR staff confirmed that there was no review and approval process in place for document scanning and indexing. OIR staff suggested that a financial examiner could identify inaccurate or incomplete financial documentation within FAME during a company's regularly scheduled financial examination. However, we noted that such examinations may occur months after documents are scanned and, therefore, may not adequately compensate for the lack of review at the time information is scanned.

In response to our request for a listing of financial filings processed through the scanning and indexing system, OIR staff stated that over 700 scanned documents were processed during the audit period. However, OIR staff stated that company files containing scanned documents could not be identified and that scanned documents could not be made available for our review without manually searching through each company's electronic financial filing. As OIR was

unable to identify those financial filings that were processed through the scanning and indexing system, it was not practicable for us on audit to compare scanned documents to originals for accuracy, completeness, and timeliness.

Without proper scanning and indexing procedures that include supervisory or independent review and approval, there is an increased risk that FAME could contain erroneous information, thereby jeopardizing the effectiveness and timeliness of OIR's financial oversight of insurance companies.

Recommendation: OIR should enhance its scanning and indexing process to ensure that information is recorded accurately, completely, and timely in FAME through appropriate data verification procedures, including supervisory or independent review and approval.

PRIOR AUDIT FOLLOW-UP

As part of our audit, we determined that the Department had corrected, or was in the process of correcting, the findings included in audit report No. 2007-088.

OBJECTIVES, SCOPE, AND METHODOLOGY

This operational audit focused on general and application controls related to the OIR FAME and included a follow-up on prior audit findings disclosed in audit report No. 2007-088 relating to OIR regulation of Viaticals and OIR performance of Market Conduct Examinations. The objectives of this audit were:

- To evaluate the effectiveness of established internal controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the economic, efficient, and effective operation of State government; the validity and reliability of records and reports; and the safeguarding of assets.
- To evaluate management's performance in achieving compliance with controlling laws, administrative rules, and other guidelines; the economic, efficient, and effective operation of State government; the validity and reliability of records and reports; and the safeguarding of assets.
- To determine whether the management had corrected, or was in the process of correcting, all deficiencies disclosed in the prior audit report No. 2007-088.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

We conducted this operational audit in accordance with applicable 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.

Our audit included examination of various records and transactions (as well as events and conditions) occurring during the period March 2006 through February 2008. In conducting our audit, we:

- Interviewed selected OIR personnel.
- Obtained an understanding of internal controls and tested the effectiveness of key processes and procedures related to FAME. In testing the effectiveness of those processes and procedures we:
  - Tested 20 program changes from the population of 62 program changes to determine the adequacy of IT general controls over systems development and maintenance.
  - Tested 20 user accounts from the population of 137 user accounts to determine the adequacy of IT general controls over user access.

- Tested logical access controls for the 137 user accounts.
- Reviewed the *FAME User's Guide*.

➢ Evaluated OIR actions taken to correct the deficiencies disclosed in audit report No. 2007-088. Specifically, to determine the sufficiency of OIR corrective actions, we obtained and reviewed applicable OIR policy and procedure revisions and documentation evidencing the use of conflict of interest forms. We also reviewed the examination and investigation checklists and evaluated the related supervisory review and approval process.

➢ Performed various other audit procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a biennial basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated October 27, 2008, the Commissioner of Insurance Regulation provided a response to our preliminary and tentative audit findings. The letter is included at the end of this report as APPENDIX A.

APPENDIX A
MANAGEMENT RESPONSE

OFFICE OF INSURANCE REGULATION

KEVIN M. MCCARTY
COMMISSIONER

FINANCIAL SERVICES COMMISSION

CHARLIE CRIST
GOVERNOR

ALEX SINK
CHIEF FINANCIAL OFFICER

BILL MCCOLLUM
ATTORNEY GENERAL

CHARLES BRONSON
COMMISSIONER OF AGRICULTURE

October 27, 2008

Mr. David W. Martin, CPA
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Re: Auditor General letter dated September 30, 2008 – Preliminary and Tentative Audit Findings and Recommendations – Office of Insurance Regulation's **Financial Analysis and Monitoring Electronic Document Management System (FAME)**

Dear Mr. Martin:

This letter is being forwarded to you in response to referenced preliminary and tentative audit findings and related recommendations.

The Office of Insurance Regulation (the Office) has reviewed the summary, background information, findings and related recommendations that were forwarded to this agency in an enclosure to referenced letter. This Office's responses to the findings and related recommendations are included in the enclosure to this letter.

I appreciate the opportunity to review and respond to referenced preliminary and tentative audit findings and related recommendations.

Sincerely,

Kevin M. McCarty

AC/aec

Enclosure

KEVIN M. MCCARTY • COMMISSIONER
200 EAST GAINES STREET • TALLAHASSEE, FLORIDA 32399-0305 • (850) 413-5914 • FAX (850) 488-3334
WEBSITE: WWW.FLOIR.COM • EMAIL: KEVIN.MCCARTY@FLDFS.COM

APPENDIX A
MANAGEMENT RESPONSE (Continued)

October 27, 2008
Auditor General Operational Audit
Page 1 of 2

Management Responses to the Auditor General's Preliminary and Tentative Audit Findings and related Recommendations – Office of Insurance Regulation's Financial Analysis and Monitoring Electronic Document Management System (FAME)

Change Management

Finding No. 1: OIR change management controls should be enhanced. OIR staff could not always provide documentation to evidence program change requests and approvals or subsequent user acceptance testing and approval.

Recommendation: To enhance change management controls, OIR should request that Project Status Reports include change management request numbers. OIR should also ensure that documentation of user acceptance testing and approval is maintained.

Response: The Office concurs with Finding No. 1 and related recommendations. An updated OIR Administrative Policy and Procedure (AP&P) will be developed and implemented to reflect this finding and recommendations within the next 90 calendar days.

User Access

Finding No. 2: OIR had not established written policies and procedures related to FAME user access. Additionally, OIR logical access controls over FAME needed improvement.

Recommendation: To minimize the risk of compromising OIR data and IT resources, OIR should establish and implement written procedures that address requesting, approving, assigning, reviewing and removing access accounts. OIR should ensure that these procedures require the revocation of access privileges immediately upon employee termination. Further, OIR should strengthen its IT security controls related to management of access privileges.

Response: The Office concurs with Finding No. 2 and related recommendations. Accordingly, an OIR Administrative Policy and Procedure (AP&P) will be developed and implemented to reflect this finding and related recommendations within the next 90 calendar days.

Scanning and Indexing

Finding No. 3: OIR scanning and indexing procedures should be enhanced to better ensure that information is accurately and completely entered into FAME.

APPENDIX A
MANAGEMENT RESPONSE (Continued)

October 27, 2008
Auditor General Operational Audit
Page 2 of 2

Recommendation: OIR should enhance its scanning and indexing to ensure that information is recorded accurately, completely and timely in FAME through appropriate data verification procedures, including supervisory or independent review and approval.

Response: The Office concurs with Finding No. 3 and related recommendations. Accordingly, a formal OIR internal procedure has been developed and implemented to reflect this finding and related recommendations.