



FINANCIAL SERVICES
COMMISSION

CHARLIE CRIST
GOVERNOR

ALEX SINK
CHIEF FINANCIAL OFFICER

BILL MCCOLLUM
ATTORNEY GENERAL

CHARLES BRONSON
COMMISSIONER OF
AGRICULTURE

OFFICE OF INSURANCE REGULATION

KEVIN M. MCCARTY
COMMISSIONER

May 8, 2009

Mr. Kevin M. McCarty
Commissioner of Insurance
Office of Insurance Regulation
200 E. Gaines Street
Tallahassee, FL 32399

Re: Auditor General Operational Audit -- **Report No. 2009-032 dated November 2008** --
Office of Insurance Regulation's Financial Analysis and Monitoring Electronic
Document Management System (FAME)

Dear Commissioner McCarty:

Status information concerning corrective actions that have been taken in response to the findings that were documented in referenced report is provided in the attached documentation pursuant to Section 20.055(5) (h), Florida Statutes. Corrective actions are keyed to the findings in the referenced report.

Sincerely,


A.E. Callahan

AEC/aec

Attachment

Cc: Audrey Brown, Chief of Staff
Rebecca McCarley, Deputy Chief of Staff
Belinda Miller, Deputy Commissioner, P&C, Office of Insurance Regulation
Mary Beth Senkewicz, Deputy Commissioner, L&H/Specialty, Office of Insurance
Regulation
Joint Legislative Audit Committee

Follow up to the Auditor General's Operational Audit – Report No. 2009-032 – Office of Insurance Regulation (the Office) 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.

Follow up: The Office concurred with Finding No. 1 and related recommendations. Each program change is currently:

- Numbered using change management numbers;
- Developed in a development environment
- Tested in a test environment;
- Tested in a production environment;
- Approved by sign-off of system owners in both test and production environments; and
- Implemented following approval by the affected application system owner.

This agency determined that, inasmuch as the current change management procedures described above are in compliance with the Office's Change Management Administrative Policy and Procedure (AP&P) – OIR AP&P 1-1 and the Department of Financial Service (DFS) Division of Information Systems (DIS) Operating Procedure governing change management -- DIS 015 -- there is no need to update OIR AP&P 1-1 at this time.

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.

Follow Up: The Office concurred with Finding No. 2 and related recommendations. A revised AP&P that addresses Application Access Control -- DFS AP&P 4-05 -- is currently under review in draft form that has been found to be acceptable for implementation by the Office. Accordingly, it has been determined by this agency that development of an AP&P by this agency that addresses Application Access Control is no longer necessary. In addition to adopting DFS AP&P 4-05, the Office will develop an internal administrative procedure which will be applicable to all of the Office's application system owners and which will ensure compliance with DFS AP&P 4-05.

Access Control for the Office includes:

- Appropriate and timely action for requesting, approving, assigning and removing user access accounts;
- Periodic review of user access privileges; and
- The use of controls that assure effective administration, management and control of application system access privileges.

Action has recently been taken to complete a risk assessment of all of the office's application systems. Additionally, action has been taken to identify and document the owners of each of the office's application systems. This information, together with information and guidance provided by DFS AP&P 4-05 and the Office's internal procedure that is described above will help assure that effective application system access controls are employed by all organizational elements within this agency.

Finally, we have recently learned that data security will be further enhanced within the Office by use of Active Directory in such a manner that password control will be enforced, including requirements for ensuring periodic password change, for major application systems such as CORE.

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.

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.

Follow Up: The Office concurred 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.