

Audit Committees:

State of New York Mortgage Agency,
New York State Housing Finance Agency
State of New York Municipal Bond Bank Agency, and
Tobacco Settlement Financing Corporation

In planning and performing our audit of the financial statements of the State of New York Mortgage Agency, the New York State Housing Finance Agency, the State of New York Municipal Bond Bank Agency and the Tobacco Settlement Financing Corporation, (collectively, the "Agencies") as of and for the year ended October 31, 2010, in accordance with auditing standards generally accepted in the United States, we considered its internal control over financial reporting ("internal control") as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Agency's internal control. Accordingly, we do not express an opinion on the effectiveness of the Agency's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

During our audit, we noted the following recommendations to enhance the internal controls and operations at the Agencies. None of the recommendations are considered to be instances of noncompliance with laws, regulations, contracts or agreements, but rather suggestions for improving existing systems and processes.

1. Accounting policies and procedures manual

Observation

The Accounting Department does not maintain a formal policies and procedures manual that documents the Agencies' various accounting policies that are applied in processing transactions related to the Agencies' financial statement accounts. The Accounting Department does have written policies for some of its transactions, but not a comprehensive manual that covers all of the significant financial statement accounts.

Recommendation

We suggest that the Agency develop and maintain a comprehensive accounting policies and procedures manual. A policies and procedures manual is an important tool that serves not only in training new employees but also facilitates the consistent processing, approval and reporting of transactions. This document should cover such items as the Agencies' financial reporting requirements, the timeline of the financial statement close process, review and approval of bank reconciliations and account analyses, estimation process for loan loss reserves, amortization of bond related accounts, etc. A policy and procedure manual will also serve to facilitate the cross-training of department personnel and help prevent potential financial reporting problems that could occur as a result of the unexpected absence of personnel.

Management's Response

We acknowledge the need for a more comprehensive policy and procedures manual. The Accounting Department's policy manual has not recently been updated, and our procedures are documented through

the use of flowcharts. In light of the integration of the housing agencies, we anticipate that there will be changes to our current processes and systems. Given that probability, we will evaluate how to proceed with the documentation of policies and procedures.

2. Accounting methodologies

Observation

We noted that the Agencies' accounting methodologies and practices are inconsistent across the various entities. For example, there are differences in the manner in which the statement of cash flows is prepared as well as the manner in which the amortization of bond-related costs and deferred mortgage acquisition costs are calculated.

Recommendation

We suggest the Agencies adopt a consistent methodology, across all entities, in accounting for the similar transactions and procedures. This will increase efficiencies in the preparation of the accounting analyses and also in cross-training of Agencies staff.

Management's Response

Management will review the individual accounting methodologies and practices across the Agencies. If appropriate, we will consider making these practices consistent across the entities. Some of the methodologies differ as a result of consistently applying each entity's original methodologies as adopted at inception, when the Agencies were not related.

3. Accounting for unamortized bond refunding costs

Observation

SONYMA currently accumulates bond refunding costs into one account and amortizes this amount over several years to interest expense. Although the difference is not material, generally accepted accounting principles (GAAP) requires that such costs be amortized over the shorter of the life of the old bonds or the new bonds.

Recommendation

In order to more closely follow GAAP, we suggest that the Agencies identify bond refunding costs by the applicable bond series to which they relate and amortize such cost over the shorter term of the old bond issue or the new.

Management's Response

SONYMA will consider implementing this recommendation during fiscal 2011. We note that the results of applying our current methodology are not materially different from that advanced by the recommendation.

4. Financial Accounting System

Observation

SONYMA currently uses Emphasys Solutions, Inc. for its mortgage application. This application has been used by SONYMA for over 20 years and has only had minor modifications in recent years. The system appears to lack certain significant functions such as the ability to generate historical reports, which is an

important function when performing certain data analyses. The system is also not fully integrated with the accounting general ledger system, thereby requiring the accounting staff to initiate the journal entries.

Recommendation

We suggest management investigate whether there exists the opportunity to enhance any of the accounting software features and options currently in place in order to provide system efficiencies. We also suggest management survey other state housing finance agencies to benchmark the capabilities of the systems used by the Agencies versus the systems used by other agencies.

Management's Response

SONYMA will look into ways to improve the functionality of this application.

Information Technology Section

Change Management

5. Mortgage Systems - Segregation of Duties

Observation

As the Mortgage Systems are supported by a third party provider, Emphasys Solutions, Inc., there are developer IDs that have access to migrate changes to production, these are 'AOD' and 'AOD Tech'. These IDs were found to have 24/7 access to the Agencies' Mortgage System with no monitoring of activities from management.

This poses a risk that unauthorized changes are made to the system without being detected, thus could affect the functionality of the system.

Recommendation

Management should introduce a process for routinely/periodically (eg: monthly) monitoring changes that have been made to the production environment to verify that those changes made were authorized.

Additionally, a control must be placed on the request for activation and deactivation of the vendor IDs. Such IDs must only be activated when there is an authorized change that needs to be migrated. Active access of the third party IDs must only be limited up to a reasonable time.

Management's Response

A new procedure has been created so that the Emphasys Remote Access VPN accounts are disabled at all times except when a documented request for access has been granted for a limited period of time. This procedure has been in place as of November 4, 2010. Management will consider implementing file system auditing software to track changes.

6. Network (Active Directory) - Privilege Access

Observation

The Agencies has recently upgraded its network infrastructure from Novell to Active Directory, however, one ID, 'NDS' was found to have been assigned to consultants that continued to be active even after

implementation of the new infrastructure.

This poses a risk that unauthorized users can use this ID to process unauthorized activities in the system.

Recommendation

'NDS' ID must be disabled as it is no longer being used.

Management's Response

Management agrees with the findings and recommendations and has remediated this on September 10, 2010.

7. SONYMA Visual Basic (VB) - Authorization

Observation

There is no formal approval of changes before they are moved to the production environment. All approvals are done prior to development.

This poses a risk that changes made to the production environment did not go through the change management process, thus could impact system functionality.

Recommendation

We recommend that management places a control for approval of the change prior to moving the change to production.

Management's Response

Management agrees with the findings and recommendation. The VP of Development will approve the changes before they are migrated to production.

8. Mortgage System - User Acceptance Tests

Observation

For two applications within the Mortgage System, program changes do not go through a proper user acceptance test, these are:

- Bond Service
- Foreclosure

This poses a risk that changes made to the production environment did not pass the user requirements.

Recommendation

We recommend that management strictly enforces user acceptance test controls over all systems.

Management's Response

Management agrees with the findings and recommendations.

LOGICAL ACCESS KEY FINDINGS AND RECOMMENDATIONS

9. Password Controls & Settings (Network, SONYMA VB and Mortgage Systems)

Observation

The Agencies maintain two levels of password security for the majority of applications. The first is network level passwords, which provide access to the Agencies' network. The second level is application specific passwords, which allow access to specified applications.

There are certain password settings that are not set based on leading practices:

Complexity: Passwords can be made more complex through methods such as requiring a minimum password length, excluding easily guessed passwords and requiring combination of character types (capitals, numbers, and special characters)

Account Lockout: Allowing a specified number of password entry errors before locking the account;

Recommendation

We recommend that management improve the network password security. We suggest the following password parameters be put in place:

Complexity: Passwords should contain a combination of letters, numbers and special characters;

Minimum Length: Passwords should contain a minimum of 6-8 characters;

History: Users may not reuse their last 5 passwords;

Account Lockout: User accounts are permanently deactivated after three unsuccessful tries (until a security administrator provides access again).

Idle Session Timeout: User accounts are automatically logged out after 15 minutes of inactivity

Management's Response

The Agencies are in compliance with our guideline which covers all of the listed items, except for "Complexity". There are other compensating controls in place which reduces the need for password complexity. These controls include 2 factor authentications for remote access, user awareness training, and password expiration. It is the opinion of Management that our policy is sufficient.

10. All Systems - User Access Recertification

Observation

The Agencies has no policy over user access recertification, as such, for the fiscal year; as such no user access recertification was performed.

Without a periodic user access recertification review, current and existing users may continue to have excessive access rights or inappropriate access rights especially when they have moved from one department to another, or promotions have taken place and they no longer need certain access.

Recommendation

We recommend that management establish a formal process for periodically (e.g.: bi-weekly or monthly) reviewing user access to verify the appropriateness and validity of access.

Management's Response

A new system has been put in place to extract user access report, the report is then sent to all departmental



head who re-certify departmental user access. An initial report was sent out in December 2010, and the results were exercised. Ongoing, a bi-annual user re-certification will be exercised.

11. All Systems - Data Restore

Observation

No data restore test was performed during the year on any of the applications. Not regularly testing backups may lead to discovering at a later time that backups are not restorable.

Recommendation

Management should establish a control in place that regularly tests backup restores.

Management's Response

A restore was indeed successfully performed on October 28, 2010 off of the main file server. The restore demonstrated successful operation of the software and hardware components of our backup & restore infrastructure. Ongoing, a quarterly restore test will be exercised.

This letter is intended solely for the information and use of the Board of Members and Directors and management of the Agencies and is not intended to be and should not be used by anyone other than these specified parties.

We are pleased to submit the above comments for your review and consideration. We are prepared to discuss any of the points noted and to respond to any questions or comments, at your convenience. We would also be pleased to assist you in implementing any of the above recommendations.

Ernst + Young LLP

January 27, 2011