NEW HAMPSHIRE RETIREMENT SYSTEM

Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance With *Government Auditing Standards*

Year Ended June 30, 2007

KPMG LLP
99 High Street
Boston, MA 02110-2371

Telephone 617 988 1000
Fax 617 507 8321
Internet www.us.kpmg.com

Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance With *Government Auditing Standards*

The Fiscal Committee of the General Court:

We have audited the financial statements of the New Hampshire Retirement System (the System), as of and for the year ended June 30, 2007, and have issued our report thereon dated August 11, 2008. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Internal Control Over Financial Reporting

In planning and performing our audit, we considered the System's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing an opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the System's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the System's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider collectively to be a significant deficiency.

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control over financial reporting. We consider the deficiencies described in Exhibit I (attached) collectively to be a significant deficiency in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control. Our consideration of the internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in the internal control that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we believe that the significant deficiency described above is not a material weakness.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the System's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations and contracts, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* and which are described in Exhibit I (attached).

The System's responses to the findings identified in our audit are described in Exhibit I (attached). We did not audit the System's responses and, accordingly, we express no opinion on them.

We noted certain matters that we reported to management of the System in a separate letter dated August 11, 2008.

This report is intended solely for the information and use of the management of the New Hampshire Retirement System and the Fiscal Committee of the General Court and is not intended to be and should not be used by another other than these specified parties.

KPMG LLP

August 11, 2008

Exhibit I

Observations Related to Internal Control Over Financial Reporting

Policies and Procedures

Cause:
Overall policies and procedures related to key areas of IT general controls are not documented. This documentation would include the following:

- IT Security Policy
- User Administration Procedures (i.e. new users, transfers, terminations)
- Change Management/Systems Development Policy and Procedures
- Computer Operation Monitoring Policies and Procedures

Effect:
The lack of documented and communicated policies and procedures related to security, change management, and computer operations results in an environment where governance is difficult and proper control procedures are either not implemented or not being effectively followed.

Recommendation:
Management should initiate an effort to document and communicate high-level policies to govern the proper implementation of IT security, change management, and computer operations monitoring processes.

High-level policies should be supplemented with detailed procedural documentation that includes control processes to address key risks related to each IT control area.

These policies and procedures should be periodically reviewed, updated and approved by management and should be communicated and made available to IT personnel and the user community as appropriate.

Management Response:
The System will update and document policies and procedures related to controls in the following areas:

- IT security policy
- User administration procedures
- Change management and systems development
- Computer operation monitoring

Administrative Access

Cause:
Administrative access to the database supporting the Pension Gold application is not adequately controlled and monitored due to the following:

- The generic default "sa" account is used to access the database with a shared password. The password is known by the IT Director, two technical specialists, and an outside contractor.

Actions performed at the database level are not logged and monitored.

Effect:
The use of a generic account with a shared password to administer the databases increases the risk that a password is compromised resulting in unauthorized and/or inappropriate direct access to production data and the potential for unauthorized and inappropriate modifications to data or database functionality. In addition, the use of generic accounts results in a lack of accountability for actions performed to the database as activity cannot be traced to the responsible individual.

Recommendation:
Management should require database administrators to access the database with accounts that are specific to those individuals. As default generic account ("sa") cannot be removed, administrators should be restricted from using this account to perform administrative functions. Activity performed with default generic account should be logged and monitored to detect potential inappropriate use. In addition, once specific database accounts are established for DBA's, their activity should be logged and monitored by supervisory personnel.

Management Response:
The System will require database administrators to access the database with accounts that are specific to those individuals and prohibit the administrators from using the default generic account to perform administrative functions. If possible, the default generic account will be eliminated.

Superuser Privileges

Cause:
Superuser privileges (i.e., ability to perform all functions) in all modules of the Pension Gold application is provided to the IT Director and outside IT consultant.

The Employer Services Supervisor has superuser level access to the Employer Reporting module. Logging of changes made to the system is configured; however there are not procedures in place to monitor logs to determine if any inappropriate transactions have occurred.

In addition, the activity logs in the system can be modified by the IT consultant.

Effect:
Providing personnel with superuser level access to the application results in a lack of adequate enforcement of segregation of duties and increases the risk that unauthorized and/or inappropriate transactions are processed. The lack of an effective process for monitoring the activity of users who have this level of access increases the risk that unauthorized and/or inappropriate transactions are not detected timely or at all.

If monitoring controls were in place, allowing the IT consultant the ability to modify those logs would result in the risk that those logs are modified inappropriately and unauthorized transactions would not be detected.

Recommendation:
Management should review all application level accounts within the Pension Gold application to ensure that access is commensurate with users' job responsibilities and take timely action to remediate exceptions.

Due to the small size of the organization, some superuser level access may be required. At a minimum, IT personnel should not have this level of access. Where personnel require this access to perform their job responsibilities, adequate logging and monitoring of activities should be performed by an individual who does not have superuser level access.

Activity/audit logs should only be modifiable by individuals who do not have superuser level access.

Management Response:
Due to the size of the Pension Gold system, superuser privileges are needed to maintain and update the database. All changes to the Pension Gold system are tracked within helpdesk software. Any changes are first made in the test environment. Prior to running the changes in production, NHRS staff reviews the changes first.

The IT Director superuser privileges are used for researching and testing in the test environment. Any change to the database made by the IT Director is recorded in the helpdesk software and changes are recorded in the audit trail.

In order to adequately enforce segregation of duties, the System will eliminate super user access for the IT consultant. As noted below, the System is in the process of transitioning the IT consultant's role to internal IT staff.

User Access Reviews

Cause:
A periodic review of user access to the Pension Gold application is not currently performed to determine that user access is commensurate with employee job responsibilities and that segregation of duties conflicts do not exist.

Effect:
Lack of adequate periodic review of logical access rights for the Pension Gold application increases the risk that access becomes inappropriate over time, as the environment evolves (i.e. users gain additional responsibilities, job transfers, etc.) and that inappropriate and/or unauthorized access is not detected and remediated timely.

Recommendation:
Management should implement a process that requires access rights to the application to be reviewed by appropriate personnel on a periodic basis. The review should be designed to detect access rights that are not commensurate with employee job responsibilities, specific segregation of duties conflicts, and accounts that belong to terminated employees.

Management Response:
Currently, the System is reviewing access to Pension Gold with managers to determine if access levels are appropriate for the work being performed by staff. In fiscal year 2008, the reviews will occur twice a year.

Password Configuration

Cause:
The following weaknesses exist regarding the password configuration for the Pension Gold application:

- For the overall application, there is no complexity requirement for passwords.
- For the overall application, there is no lockout configured after multiple successive unsuccessful login attempts.
- For the Employer Reporting module of the application minimum length and password expiration are not configured. In addition, users are not required to change their password upon initial login to the application.

Effect:
Lack of adequate password parameters increases the risk that a password is compromised, potentially resulting in unauthorized access to sensitive application functionality and data.

Recommendation:
Management should make the necessary modifications to the application configuration to require an adequate minimum length, password complexity, password expiration, and account lockout after unsuccessful attempts.

Where the functionality of the application does not allow for adequate passwords to be required, management should implement procedures to monitor passwords to ensure that users are establishing strong passwords and changing their passwords periodically.

Management Response:
The System will implement modifications to the password configuration within Pension Gold to require an adequate minimum length, password complexity, password expiration and account lockout after unsuccessful attempts.

Firewall Configuration

Cause:
Monitoring of modifications made to the firewall configuration is not performed.

Effect:
The lack of monitoring of the firewall configuration increases the risk that changes to the firewall configuration resulting in weaknesses in the external perimeter security.

Recommendation:
Managements should implement a process to monitor changes made to the firewall configuration and verify that those changes have been authorized, tested and approved.

Management Response:
The System will implement a process to monitor changes made to the firewall configuration and verify that those changes have been authorized, tested and approved.

Monitoring of Job Processing

Cause:
Monitoring of job processing is not currently performed by IT. IT relies on the user community to report problems that they encounter (e.g. jobs that end abruptly or are not run timely).

Effect:
The lack of proactive monitoring of the job schedule increases the risk that problems are not detected and resolved timely resulting in inefficiencies in processing and having an impact on the user community's ability to carry out their job responsibilities.

Recommendation:
Management should implement a process to monitor the job schedule to identify and detect problems in a timely manner and take appropriate action to resolve those problems prior to being notified by the user community.

Management Response:
The System will establish a proactive process to monitor the job schedule to detect problems in a timely manner.

Role of Outside IT Consultant

Cause:
There is a high level of reliance placed on an outside IT consultant in maintaining the IT environment. It does not appear that the activities of this consultant are adequately monitored to ensure that unauthorized and/or inappropriate activity does not occur. Specifically, the IT consultant has the ability to administer the Pension Gold application and database as well as the firewall. The consultant also has the ability to run scripts that modify data in the database supporting Pension Gold and there do not appear to be monitoring controls over this activity.

Effect:
Often external consultants are utilized to assist in maintaining IT environments where internal resource constraints exist. However, allowing an external consultant a high level of access to the IT environment without adequate monitoring of the individual's activities increases the risk that inappropriate actions are performed resulting in loss of data integrity, loss of system availability/stability, and/or the processing of inappropriate and unauthorized transactions.

Recommendation:
Management should review the level of access and level of reliance that they place on external IT consultants to verify that it is appropriate given the circumstances. IT consultants should be closely monitored to ensure that their actions are in the best interests of the organization. Where reliance is required to be placed on external consultants, procedures should be implemented to monitor their activities.

Management Response:
The System has entered into an agreement with its vendor for Pension Gold on-site support. The System is in the process of transitioning the IT consultant's role to internal IT staff. Hardware responsibilities have already occurred and a new position is planned to handle the database portion. As a result, reliance on on-site IT consultants will be eliminated. Nonetheless, the System will establish controls so that they will be in place should an independent consultant be engaged in the future.

In addition, the System will evaluate and determine whether an IT systems performance review should be conducted by an outside IT firm with expertise in public pension systems. The review would provide an independent assessment of the IT function from an industry perspective and allow a comprehensive approach for adopting improvements.

Observation Related to Compliance and Other Matters

IRS Voluntary Correction Program

During fiscal 2007, the System undertook a comprehensive review of its compliance with certain Internal Revenue Code (IRC) requirements. The review was overseen by the System's Board of Directors, its general counsel as well as an outside law firm specializing in IRC matters. The review was conducted to assist the System's general counsel in the preparation of a determination letter filing, and any related filings, concerning the qualification requirements under the IRC and to review the operation of the retiree health program in connection with those qualification requirements.

The outside law firm issued its conclusions and recommendations in its final report dated April 2, 2008. Consequently, in April 2008, the System made a filing with the Internal Revenue Service (IRS) as part of its voluntary correction program seeking IRS approval of the System's corrective action plan as well as relief from any fines or penalties resulting from the conclusions noted by the outside law firm.

We recommend that the System continue to work with its legal counsel and the Legislature to implement the changes necessary to fully comply with all statutory and regulatory compliance requirements.

Management Response:
The NHRS is dedicated to continuing to work with its legal counsel, the Legislature and the Internal Revenue Service to ensure that the voluntary compliance correction process is completed as expeditiously as possible. It is a primary goal of the NHRS that all changes necessary to comply with all statutory and regulatory compliance requirements be implemented and that the NHRS maintains statutory and regulatory compliance in the future.