

**MINUTES OF THE MEETING
OF
THE AUDIT COMMITTEE**

July 27, 2009

A meeting of the Audit Committee was held at the Authority's offices at the Clarence D. Rappleyea Building, 123 Main Street, White Plains, New York at approximately 7:15 p.m.

The following Members of the Audit Committee were present:

Trustee D. Patrick Curley (Chairman)
Trustee Elise M. Cusack
Trustee Jonathan F. Foster

Also in attendance were:

<i>Gil Quiniones</i>	<i>Chief Operating Officer</i>
<i>Terryl Brown Clemons</i>	<i>Executive Vice President and General Counsel</i>
<i>Joseph Del Sindaco</i>	<i>Executive Vice President and Chief Financial Officer</i>
<i>Joan Tursi</i>	<i>Senior Vice President – Enterprise Shared Services</i>
<i>Arnold Bellis</i>	<i>Vice President – Controller</i>
<i>Patricia Leto</i>	<i>Vice President – Procurement</i>
<i>Lesly Pardo</i>	<i>Vice President – Internal Audit</i>
<i>Karen Delince</i>	<i>Corporate Secretary</i>
<i>Brian McElroy</i>	<i>Treasurer</i>
<i>Angela Graves</i>	<i>Deputy Corporate Secretary</i>
<i>Thomas Concadoro</i>	<i>Director – Accounting</i>
<i>Michael Saltzman</i>	<i>Director – Media Relations</i>
<i>Dennis Eccleston</i>	<i>Chief Information Officer</i>
<i>Mary Jean Frank</i>	<i>Associate Corporate Secretary</i>
<i>Lorna Johnson</i>	<i>Assistant Corporate Secretary</i>
<i>David Milkosky</i>	<i>Partner, Ernst & Young</i>
<i>Louis Roberts</i>	<i>Audit Senior Manager, Ernst & Young</i>
<i>John Barile</i>	<i>Partner, Assurance and Advisory Business Services, Ernst & Young</i>
<i>Chuck Haddon</i>	<i>Managing Director, Navigant Consulting</i>
<i>Khai Nguyen</i>	<i>Director, Navigant Consulting</i>

1. **Minutes of the Regular Meeting of February 24, 2009**

The minutes of the Committee's Regular Meeting of February 24, 2009 were adopted.

2. Ernst & Young's Draft Management Letter

Mr. Thomas Concadoro presented an overview of Ernst & Young's ("E&Y") draft management letter for the year-end 2008 audit, saying that once it is finalized it will be forwarded to the Governor, the State Comptroller, New York State legislative leaders and the Authority Budget Office. In the letter, E&Y identified the following areas where the Authority could strengthen its general controls over information technology ("IT"). Mr. Dennis Eccleston then reviewed the comments for the Committee:

- **Enhance Segregation of Duties within the Change Management Process** – Segregating the ability to make program changes and the ability to migrate those changes into production is a primary control that companies traditionally rely on to prevent unauthorized updates of production programs. E&Y noted that a few Authority staff members were granted both capabilities in order to allow certain key systems personnel to stand in for other personnel should the primary functional user be unavailable. E&Y recommended that this dual access be eliminated, where feasible. In instances where management believes these duties cannot be segregated, E&Y recommended that the change management process be enhanced to include a formalized periodic post-implementation monitoring review of changes migrated to production by those users, with documentation retained for audit purposes. Authority management's response was that the current pre-implementation review by users significantly mitigates the risk of inappropriate changes and that only a select group of IT staff has the expanded capabilities. Management agreed to conduct quarterly reviews of these individuals' migration activities.
- **Use SAP to Enforce a Proper Segregation of Duties within the Accounts Receivable ("AR") and Accounts Payable ("AP") Processes** – Traditionally, companies running a core ERP application such as SAP use application security to enforce proper segregation of duties. E&Y noted several user accounts with access to process transactions that would normally be segregated. Specifically, E&Y noted that certain users have the following conflicting capabilities:
 - AR:** (1) Customer master maintenance and AR cash application
(2) Customer master maintenance and billing
(3) AR cash application and billing
 - AP:** (1) Vendor master maintenance and AP invoice processing
(2) Vendor master maintenance and AP payments
(3) AP invoice processing and AP payments

Apparently, the above access was granted during SAP implementation in order to provide users with the ability to perform specific required tasks that are part of their job responsibilities and are not inherently conflicting duties. The risk is that not using SAP to enforce proper segregation of duties may enable an employee to execute transactions that are not consistent with management's intentions. E&Y recommended that the Authority use SAP to enforce the proper segregation of AR and AP transactions. For situations where incompatible duties must be

granted to single users, E&Y recommended that management closely monitor the activities surrounding the accounts to confirm that inappropriate actions have not been performed. Authority management responded that it believed the duties referenced have been segregated appropriately through process and procedure, but also agreed to perform a full review of the referenced duties and modify security profiles where appropriate. These changes should be made by the end of 2009.

- **Review Privileged Access Granted within the SAP Application** – SAP contains a number of sensitive system transactions that have powerful capabilities beyond what is needed in the ordinary course of day-to-day processing. Several user accounts were noted to have been granted excessive access to sensitive IT transaction codes. A listing of these codes and the associated users was provided to management under separate cover. Granting users the ability to execute privileged transactions beyond their normal job responsibilities increases the risk that inappropriate transactions may be executed within SAP. E&Y recommended that management (1) perform a detailed review of access granted to these sensitive system transactions and eliminate any access not required in the ordinary course of business and (2) consider implementing a manual or automated monitoring control to validate transactions executed by individuals assigned these key privileges. Authority management agreed to perform a detailed review of access to these transactions, noting that a number of the users with such access are IT staff and selected functional users who require access to these functions. Other functional staff members' profiles with these authorizations will be modified. The Authority will also explore acquiring a tool to monitor transactions assigned to individuals.
- **Enhance Segregation of Duties within the Logical Access Process** – Five employees have been granted privileged access to perform user administration functions within SAP, in addition to the responsibility of approving user requests for access to SAP. Leading practices suggest that authorization and execution of user provisioning requests be segregated. Allowing the same individual to authorize and administer user access increases the risk that inappropriate access may be granted to the production environment, which may not be detected and acted on in a timely manner. E&Y recommended that the user administration function in SAP be restricted to individuals who do not have the ability to authorize access. Authority management agreed with E&Y's recommendation and four of the five user accounts were modified by the end of June 2009. The remaining one is the Manager of SAP Support, who is required to perform administration functions as backup to the Security Administrator. Management will monitor transactions processed in this backup role on a quarterly basis.

Mr. Barile said that comments of this type were fairly typical for a company of the Authority's size and scope and that companies with larger IT staffs could more easily segregate these functions.

Vice Chairman Foster noted that management's response to the recommendations seemed somewhat defensive in certain cases and that this was probably not warranted. Responding to a question from Chairman Curley, Mr. Arnold Bellis said that while management generally agreed

with E&Y's findings, staff often finds alternative approaches to achieving the same objectives. He said that, as part of the process, Authority staff discusses these different approaches with E&Y.

Upon motion made and seconded, the members of the Committee voted unanimously to accept the management letter. Chairman Curley said that the minutes should reflect that the word "draft" will be removed from the management letter, which will be dated February 26, 2009 to be consistent with E&Y's audit opinion date.



Memorandum

June 30, 2009

To: Audit Committee Members
Chairman, D. Patrick Curley
Trustee, Elise M. Cusack
Trustee, Jonathan F. Foster

From: Thomas Concadoro *T Concadoro*
Director of Accounting

Subject: Ernst & Young- Draft Management Letter

Enclosed please find Ernst & Young's draft management letter for the year-end 2008 audit. We plan to review the draft recommendations and management responses at our next scheduled audit committee meeting. As required by generally accepted auditing standards, the effective date of the letter is February 26, 2009 which is the same as the audit opinion date. Please note that the draft was completed and issued to management much more recently. If you have any questions regarding this item, please call me on extension 3350 at the White Plains office.

Enclosed

cc: A. Bellis
J. Del Sindaco
D. Eccleston
K. Delince
A. Graves
L. Pardo

Audit Committee
Power Authority of the State of New York

In planning and performing our audit of the financial statements of Power Authority of the State of New York (the "Authority") as of and for the year ended December 31, 2008, 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 Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

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. 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 internal control was for the limited purpose described in the first paragraph and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control that we consider to be material weaknesses, as defined above.

During our review of general controls over information technology, we identified certain areas where the Authority could strengthen its internal controls as follows:

1. Enhance Segregation of Duties within the Change Management Process

Observation

The segregation of the ability to make program changes and the ability to migrate those changes into production is a primary control that companies traditionally rely upon to prevent unauthorized update to production programs. During our testing, we noted that there were a few individuals within the Authority that were granted both capabilities. Per discussion, these capabilities were granted to allow certain key

systems personnel to stand in for other personnel should the primary functional user be unavailable.

Risk

There is an increased risk that inappropriate changes may be migrated into production if incompatible duties are not segregated (i.e. development and migration).

Recommendation

We recommend that the access granted to key individuals to both develop and migrate program changes be eliminated, where feasible. In instances where management believes these duties cannot be segregated, we recommend that the change management process be enhanced to include a formalized post-implementation monitoring review of changes migrated to production by those users. This review should be performed on a periodic basis (i.e. monthly) to assess whether changes migrated into production were appropriate and authorized, and documentation should be retained for audit purposes.

Management Response

Management believes that the current pre-implementation review by users significantly mitigates the risk of inappropriate changes. It should be noted that only a select group of IT staff were granted expanded capabilities to facilitate expanded coverage for SAP maintenance activities. Management agrees to conduct periodic reviews of these individuals' migration activities to ensure changes are implemented appropriately.

2. Utilize SAP to Enforce a Proper Segregation of Duties within the Accounts Receivable (AR) and Accounts Payable (AP) Processes

Observation

Traditionally, companies running a core ERP application such as SAP utilize application security to enforce a proper segregation of duties. During testing of key transactions, we noted several user accounts with access to process transactions that would normally be segregated. Specifically, we noted certain users having the ability to execute the following conflicting capabilities:

Accounts Receivable:

1. Customer Master Maintenance and AR Cash Application
2. Customer Master Maintenance and. Billing
3. AR Cash Application and Billing

Accounts Payable:

1. Vendor Master Maintenance and AP Invoice Processing
2. Vendor Master Maintenance and AP Payments
3. AP Invoice Processing and. AP Payments

It appears that the above access was granted during the SAP implementation in order to provide users with the ability to perform specific required tasks which are part of

their job responsibilities. These tasks were not conflicting duties in and of themselves, but were inherent in the broader profiles they were assigned to.

Risk

Not utilizing the SAP application to enforce a proper segregation of duties increases the risk that an employee may execute transactions that are not consistent with management's intentions.

Recommendation

We recommend that the Authority use SAP to enforce the proper segregation of transactions within the Accounts Payable and Accounts Receivable processes. This may necessitate redesigning security profiles to make them more specific to job functions. For situations where incompatible duties must be granted to single users, we recommend that management closely monitor the activities surrounding the accounts to confirm that inappropriate actions have not been performed.

Management's Response

Management believes that the duties referenced have been segregated appropriately through process and procedure and the delineation of departmental responsibilities. Management agrees that SAP should be utilized where possible, to enforce the procedural segregation of transactions. Accordingly, we will perform a full review of the referenced duties and will modify security profiles where appropriate. (In addition, it should be noted, that the billing transactions that were identified as incompatible were used prior to the implementation of SAP Billing and cannot currently be used to generate customer invoices or other billing transactions).

3. Review Privileged Access Granted within the SAP Application

Observation

The SAP application contains a number of sensitive system transactions that have powerful capabilities beyond what is needed in the ordinary course of day to day processing. During testing of these key transactions, several user accounts were noted to have been granted excessive access to sensitive IT transaction codes. A listing of these codes and the associated users was provided to management under separate cover.

Risk

Granting users the ability to execute privileged transactions beyond their normal job responsibilities increases the risk that inappropriate transactions may be executed within the SAP system.

Recommendation

We recommend that management perform a detailed review of access granted to these sensitive system transactions and eliminate any access not required in the ordinary course of business. Further, we recommend that management consider implementing a monitoring control (manual or automated) to validate the transactions executed by individuals assigned with these key privileges.

Management's Response

Management agrees and will perform a detailed review of access to these transactions. A number of the users with such access are IT staff and selected functional users who require access to these functions. Other functional staff members' profiles with these authorizations will be modified. The Authority will also explore acquiring a tool to monitor transactions assigned to individuals.

4. Enhance Segregation of Duties within the Logical Access Process

Observation

There are five employees who have been granted privileged access to perform user administration functions within SAP, in addition to the responsibility of approving user requests for access to SAP. Leading practices suggest that the authorization and the execution of user provisioning requests be segregated.

Risk

Allowing the same individual to authorize and administer user access increases the risk that inappropriate access may be granted to the production environment, which may not be detected and acted upon in a timely manner.

Recommendation

We recommend that the user administration function in SAP be restricted to individual(s) that do not have the ability to authorize access. The administration capabilities should be segregated from the application business end-users.

Management Response

Management agrees. Four of the five user accounts will be modified by end of June 2009. The remaining one is the Manager of SAP Support who is required to perform administration functions as backup to the Security Administrator. Management will monitor transactions processed in this backup role.

* * * * *

This communication is intended solely for the information and use of the Audit Committee, management, members of the Authority, and the Office of the State Comptroller of the State of New York and is not intended to be and should not be used by anyone other than these specified parties.

We would be pleased to discuss the above matters or to respond to any questions, at your convenience.

February 26, 2009

3. **Motion to Conduct an Executive Session**

“Mr. Chairman, I move that the Authority conduct an executive session pursuant to Section 105 of the Public Officers Law of the State of New York to discuss matters leading to the appointment, employment, promotion, discipline, suspension, dismissal or removal of a particular person or corporation.” Upon motion made and seconded, an Executive Session was held.

4. **Motion to Resume Meeting in Open Session**

“Mr. Chairman, I move to resume the meeting in Open Session.” Upon motion made and seconded, the meeting resumed in open session.

5. Recommendation to the Board of Trustees on the Selection of External Auditors for the Ensuing Five Years

Chairman Curley presented the highlights of the Audit Committee's recommendation to the Board of Trustees. He said that the members of the Committee had participated in lively discussions with Authority staff regarding the selection.

Upon motion made and seconded, the Audit Committee voted to recommend to the full Board of Trustees that KPMG be selected as the Authority's external auditor for the period 2009-2014. The vote was as follows: Chairman Curley – no; Vice Chairman Foster – yes and Trustee Cusack – yes.

6. Internal Audit Activity Report

Mr. Lesly Pardo presented an overview of Internal Audit's ("IA") activity for the first half of 2009. He said that as of June 30, 14 audits had been completed, including seven financial/internal control; three information technology and four operational. Seven audits were in progress as of June 30. Approximately 49% of the audits included in the 2009 Audit Plan have been completed or are in progress. Mr. Pardo said that 10 audit reports containing 18 recommendations had been issued and that four reports were under review as of June 30. All of the recommendations in the audit reports had been accepted by management and the accepted recommendations are being actively tracked. To ensure that issues raised in the audits are properly addressed, implementation of critical recommendations is being verified by observation and testing rather than reliance on verbal confirmation. Mr. Pardo also said that IA had received full cooperation and support from management and that IA staff were given full and unrestricted access to all documents, records and personnel necessary to perform their work.

In response to a question from Chairman Curley, Mr. Pardo said that the criteria for audits being selected for the 2009 Audit Plan were arrived at by analyzing the audit universe and developing priorities based on risk factors. He said that the Audit Committee had approved the 2009 Audit Plan at its February 24 meeting.

Mr. Pardo said that an open-position requisition has been made for a Manager of Special Audit Services who would be responsible for planning, executing and directing all fraud prevention/detection IA activities within the Authority, including special investigations into instances of fraud, waste, abuse and ethical/regulatory violations. He said that periodic reports would be provided to executive management and the Audit Committee on these investigations and their results.

AUDIT COMMITTEE

**INTERNAL AUDIT
ACTIVITY REPORT**

JUNE 30, 2009

**2009 INTERNAL AUDIT PLAN
ACTIVITY REPORT
6/30/09**

Summary

- Completed 14 audits including 7 financial, 4 operational and 3 information technology.
- Seven (7) audits in progress as of 6/30/09.
- Approximately 49% of the audits in the original Audit Plan have been completed or in progress.
- Issued 10 audit reports. Four (4) reports under review as of 6/30/09.
- Eighteen (18) recommendations were made to improve internal controls/operational efficiency.
- All recommendations have been accepted by management. Accepted recommendations are being actively tracked and critical recommendations implemented are being verified.
- We are receiving management's full cooperation and support.

**2009 INTERNAL AUDIT PLAN
ACTIVITY REPORT
6/30/09**

Completed Audits**Report Date****Financial/Internal Control Audits**

Long-Term Debt/Interest Rate Risk Management	6/30/09
Headquarters Accounts Payable	5/28/09
Real Estate Management	3/31/09
AECOM USA Inc. (Contract)	3/31/09
Clark Energy Center Finance & Administration	6/30/09
Power for Jobs Rebates	Reviewing
Niagara Power Project Finance, Purchasing & Warehousing	Reviewing

Operational Audits

Capital Planning/Budgeting	5/05/09
Blenheim-Gilboa Life Extension and Modernization Project	3/13/09
Energy Services Programs	Reviewing
Ethics and Employee Awareness	Reviewing

Information Technology Audits

IT Legal/Regulatory Compliance	2/27/09
NERC Critical Infrastructure Protection Compliance - Poletti, Flynn, 500 MW	3/31/09
Change Control – SAP	5/29/09

**2009 INTERNAL AUDIT PLAN
ACTIVITY REPORT
6/30/09**

Audits In-Progress

Purchased Power/Energy Hedging Transactions
Stimulus Audit and Reporting Project
Health and Safety Programs
NERC-CIP Technical St. Lawrence
NERC-CIP Technical Niagara
NERC-CIP Technical Blenheim-Gilboa
NERC-CIP Technical Clark Energy Center
NYPA Network Security

2009 INTERNAL AUDIT PLAN ACTIVITY REPORT 6/30/09

Internal Audit Plan – July through December 2009

1. **Internal Audit/Special Investigations Activities** – An open position requisition has been made for the Internal Audit Manager of Special Audit Services. This individual is responsible for planning, executing and directing all fraud prevention/detection internal audit activities within the organization; including the execution of special investigations involving cases and instances of fraud, wastes, abuses and ethical/regulatory complaints.

Periodic reports will be provided to executive management and the Audit Committee on the cases received during the period and the resolution of the related investigation procedures.

2. **Enterprise Risk Management Infrastructure** – NYPA is in the process of implementing an Enterprise Risk Management program. The audit will independently report on the Authority's progress in implementing the program and assess the effectiveness of the program's timely identification of business objectives and corresponding risks. Primary objectives of the audits are to assess the effectiveness of the risk management methodology; the completeness of the risk assessment activities; effectiveness of management's reporting/monitoring process; and degree in which identified risks are being mitigated.
3. **Energy Hedging Transactions** – Assess the adequacy of the Authority's power hedging and trading policy in (1) the establishment of acceptable levels of energy pricing risk (expressed in terms of the impact changing energy prices will have on NYPA's net income and customer pricing) and how risks will be measured. Scope of the audit will include (1) evaluating the effectiveness of the process used in providing management with timely and accurate energy risk information and positions; (2) incorporation of pricing factors including those relating to the NYS Economic Development Program requiring subsidize energy prices; and (3) conducting detailed testing of financial and energy hedging transactions to verify that established energy hedging requirements are being complied with.

Internal Audit Plan – July through December 2009 (Continued)

4. **Fuel Operations/Fuel Hedging Transactions** – Evaluate the effectiveness of the forecasting and reporting tools used to make fuel purchasing and hedging decisions. We will evaluate how the tools provide management with timely information that is in line with established risk levels. Detailed testing will be conducted on financial transactions such as (1) procurement/payments of fuel oil and natural gas; and (2) fuel hedging transactions to verify compliance with NYPA established policies and procedures.
5. **NYPA Counterparty Credit Risk** – Determine and evaluate the effectiveness of management's process for monitoring, assessing and managing counterparty risks in relation to its trading operations. Detailed testing will be conducted on a sample of "in the money" positions to determine the adequacy of collateral positions and compliance with trading agreements.
6. **Succession Planning** – Assess the completeness and adequacy of the Human Resource Department's succession planning for the Authority. Key areas of focus consist of (1) determining the comprehensiveness of critical NYPA positions within the HR succession planning scope; (2) identifying critical skills/knowledge requirements for NYPA; and (2) evaluating the adequacy of the established succession plan (identification of individuals to fill key positions in case of turnover) for each of the identified critically NYPA positions.
7. **NYPA Global Physical Security Programs** – Entity wide evaluation of NYPA's physical security policies and procedures in ensuring effective physical security over all of the Authority's business sites and energy production facilities. Specific focus will be to evaluate the effectiveness of the Authority's coordinated physical security monitoring program and anti-terrorism specific measures. Detailed testing procedures will be conducted to determine the effectiveness of NYPA's personnel execution of the required security polices and procedures.
8. **NERC Critical Infrastructure Protection (CIP) Compliance** – Evaluate the effectiveness of the Authority's coordinated compliance monitoring process and self examination procedures utilized by management in ensuring compliance with the North American Electric Reliability Corporation CIP standards as it relates to the protection of critical assets and cyber-security. This integrated information technology and operational audit will include all NYPA power generation facilities and will include independent testing and validation to assess the Authority's compliance with its own established policies and procedures as it relates to asset protection and cyber-security.

Internal Audit Plan – July through December 2009 (Continued)

9. **NYPA Corporate Compliance Program** – NYPA is in the process of defining its Corporate Compliance program/function. The audit will independently report on the Authority's progress in implementing the program. We will also evaluate the effectiveness of the Authority's coordinated compliance monitoring process and self examination procedures utilized by management in ensuring compliance with all applicable laws and regulations. Primary focus will be determining how effective the oversight functions (i.e., Compliance & General Counsel) work with the business functions to (1) identify compliance requirements; (2) develop applicable policies and procedures to ensure compliance; (3) process for assessing and monitoring compliance; and (4) the filing of required reports.
10. **B-G Operations & Maintenance** – Assess the effectiveness of the procedures used in the day-to-day monitoring and maintenance of the B-G operations. Detailed testing to verify compliance with established procedures will primarily focus on the following areas: (1) interface with ECC and ERM; (2) plant performance management; (3) maintenance resource management program; (4) reliability and outage management; and (5) overall budgeting and cost control.
11. **500 MW Operations & Maintenance** – Assess the effectiveness of the procedures used in the day-to-day monitoring and maintenance of the 500 MW operations. Detailed testing to verify compliance with established procedures will primarily focus on the following areas: (1) interface with ECC and ERM; (2) plant performance management; (3) maintenance resource management program; (4) reliability and outage management; and (5) overall budgeting and cost control.
12. **NYISO Energy Settlements (Load Serving Transactions)** – Conduct an integrated information technology and operational based review of the systems, reports and processes utilized in the billing and settlement of load serving transactions with the NYISO. Detail testing on settlement reports, rebills and reconciliations will be performed to assess the completeness and accuracy of the settlement transactions.
13. **NYPA Network Security** – Evaluate the effectiveness of the information technology security controls utilized by the Authority in protecting its computer network from unauthorized access. Such controls and process in scope includes: assigning and termination of user access; hard-ware and network configurations; and utilization of firewalls. We will be utilizing the Information Systems Audit and Control Association (ISACA) framework for network security in conducting our evaluation.

14. **Power System Operations/Energy Management Systems** – Conduct an integrated information technology and operational based review of the systems and processes utilized within the ECC operations and transmission systems. Specific areas of focus include: (1) ECC control room operations; (2) coordination with NYPA generation and transmission managers; (3) performance monitoring tools and procedures; and (4) interaction with the NYISO.
15. **Monthly Internal Management Reporting** – Review and determine the adequacy, timeliness, completeness and accuracy of the Authority’s monthly internal financial reporting. We will conduct detailed review over the monthly financial reporting close process and will conducted detail transaction to verify the completeness and accuracy of reported figures/numbers.
16. **Follow-up on Audit Recommendations/Findings** – Conduct audit assignments and detailed testing procedures to verify the effectiveness of management’s action plans in response to reported internal audit recommendations and findings. Results of the follow-up activities provide the basis for the accurate reporting to the Audit Committee of remediated control deficiencies by management.
17. **External Audit Support** – Under the supervision and direction of the external auditors, conduct financial audit procedures consisting of both control documentation and detailed transaction testing over defined financial reporting cycles. Results are reported directly to the external auditors.

**2009 INTERNAL AUDIT PLAN
ACTIVITY REPORT
6/30/09**

REPORT RECAP*

FINANCIAL/INTERNAL CONTROL AUDITS

An audit of **Long-Term Debt and Interest Rate Risk Management** covering Interest Rate Hedging Activities, Issuance of Long and Short Term Debt, Debt Portfolio Management System (PORTIA), and Interest Accrual and Payment resulted in recommendations to strengthen controls over the reporting and monitoring of interest rate hedging activities.

An audit of **Headquarters Accounts Payable** showed that controls are in place and functioning effectively. Recommendations were made dealing with procedures for processing vendor payments based on approved purchase orders and receipt of goods and services.

An audit of **Clark Energy Center Finance and Administration** which covered budgetary controls, payroll, accounts payable, property records, travel and living expenses and SAP access found controls to be adequate and effective.

An audit of **Real Estate Management** resulted in recommendations to improve controls over Real Estate documentation for land conveyances and tree removal, and procurement credit card procedures.

A contract audit of **AECOM Inc.** (total contract value of \$130 million) which provides program management and implementation services for SENY Energy Efficiency projects resulted in recommendations concerning subcontractor contract awards and contractor's schedule of services.

**2009 INTERNAL AUDIT PLAN
ACTIVITY REPORT
6/30/09**

**REPORT RECAP*
(CONTINUED)**

OPERATIONAL AUDITS

An audit of NYPA's **Capital Planning/Budgeting** functions resulted in recommendations concerning Budget Department procedures, capital authorization limits, post completion assessment guidelines, and detailed budget variance analysis of Fleet's capital purchases.

An audit of the **Blenheim-Gilboa Life Extension and Modernization (LEM) Construction Project Audit** covering Project Management, Financial Management, Reporting and Quality Assurance concluded that the process and related internal controls were adequate and effective. Recommendations were made dealing with additional work request, review of project costs, and LEM Quality Plan.

INFORMATION SYSTEMS AUDITS

An audit of **IT Legal & Regulatory Compliance** resulted in a recommendation to develop written procedures for portable devices (Blackberries, laptops).

An audit of **Change Control – SAP** covering changes, maintenance, and upgrades to the SAP System found controls over the SAP Change Control procedures and processes to be adequate.

An audit of the identification of critical assets and critical cyber assets as required by **NERC at the Poletti, Flynn and 500 MW Plants** concluded that the methodology and process performed in complying with NERC requirements were effective.

7. Amendments to Audit Committee Charter

Mr. Pardo presented the highlights of staff's recommendations to the members of the Audit Committee. He said that as part of the Internal Audit Transformation Initiative, Navigant Consulting ("Navigant") reviewed the Audit Committee's roles and responsibilities as delineated in the Audit Committee Charter ("Charter") to ensure that it complies with best practices and the requirements of the Public Authority Accountability Act of 2005. The Audit Committee is currently responsible for oversight of the Authority's relationship with its independent accountants and the Internal Audit process. To enhance the Audit Committee's roles and responsibilities, Navigant prepared a draft revised Audit Committee Charter. The most significant of the revisions to the Charter are the following:

- **(1) Section C2 – Accounting/Financial Reporting and Oversight of the Independent Accountants:** (b) review and approve the annual audited financial statements, including the external auditor's management letter, and all other independent communications; (c) oversee the establishment of procedures for the effective receipt and treatment of complaints regarding auditing, internal accounting and accounting matters and (g) approve any non-audit work by the independent accountants.
- **(2) Section C3 – Risk Management/Internal Controls and Oversight of Internal Audit:** (d) provide guidance to the Authority's Chief Risk Officer ("CRO") and Enterprise-Wide Risk Management Program with regard to critical business objectives, risks and philosophy/tolerance for risk mitigation, as well as reporting requirements of the CRO to the Committee.
- **(3) Section C4 – Ethics, Legal/Regulatory Compliance and Oversight of the Ethics and Compliance Office:** (a) provide oversight and guidance to the Authority's Chief Ethics and Compliance Officer with regard to the programs and policies of the Authority designed to ensure compliance with applicable laws and regulations; (b) meet at least three times a year with the Authority's Chief Ethics and Compliance Officer to discuss the effectiveness of the overall compliance program and reported instances of Code of Conduct violations and (c) authorize investigations into any matters within the Audit Committee's scope and responsibilities.

The members of the Audit Committee reviewed the draft revised Charter prepared by Navigant and will discuss a further revised draft at their next meeting.

8. Other Business

In response to a question from Vice Chairman Foster, Mr. Joseph Del Sindaco said that staff would make a hedging presentation to the Trustees at their September meeting.

9. Next Meeting

The next regular meeting of the Committee would be determined. Upon motion made and seconded, the meeting was adjourned at approximately 8:30 p.m.