Long Island Power Authority

(A Component Unit of the State of New York)

Management Letters for year ended December 31, 2015

Introduction

On March 21, 2016, KPMG LLP, the Long Island Power Authority's (the Authority) independent accountants, completed its annual audit of the Authority for the year ended December 31, 2015. The audit is performed in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States.

In planning and performing the audit, KPMG LLP considers the Authority's internal control over financial reporting (internal control) to determine the appropriate audit procedures, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control.

The Management Letters presented in the attachment to this letter contain comments and recommendations related to the Authority's internal control over financial reporting. KPMG LLP's observations and recommendations, and management's responses regarding such matters are presented in the attachments.

These Management Letters should be read in conjunction with KPMG LLP's Independent 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*, which was issued on March 21, 2016, and is included in the Long Island Power Authority's 2015 Annual Report.

KPMG LLP
345 Park Avenue
New York, NY 10154-0102

July 27, 2016

Finance and Audit Committee
Long Island Power Authority
Uniondale, New York

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the Long Island Power Authority (the Authority), as of and for the year ended December 31, 2015, in accordance with auditing standards generally accepted in the United States of America, we considered the Authority's 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.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized as follows:

Finding #1: Non – Compliance of Active Directory (Network) and Mainframe (RACF) Password Parameters supporting the CAS/EBO applications

Background

PSEG Long Island is a third party service provider that manages the Authority's transmission and distribution system. Through various management agreements with the Authority, PSEG Long Island provides customer support (billing, cash collections and services) to the Authority's electric customers. Furthermore, PSEG Long Island manages the Authority's in-scope applications (CAS & EBO), which are hosted at PSEG Long Island's Data Center located in Garden City, New York. CAS and EBO applications are supported by the Mainframe environment, which is supported by the RACF security management structure. Network passwords are supported by the Windows Active Directory framework. In order to log into the CAS and EBO applications end users have to utilize the RACF security structure.

Observation

KPMG inspected the Information Technology (IT) Security Policy titled Information Systems and Infrastructure Security (ISIS) Instruction provided by PSEG Long Island and compared the password requirements to the Active Directory and RACF password configuration settings and noted that they

do not meet the minimum requirements as outlined in the IT Security Policy. The following password parameters did not adhere to the Password Management Standards:

1) New user accounts created on the Active Directory are not required to change the default password at initial log-on.
2) Password complexity is not enabled on the Mainframe.
3) Maximum password age for system administrators is not set to 30 days and is instead set to 60 days on the Mainframe.

Risk

Without strong password parameters configured in the key applications and systems, there is an increased risk that unauthorized users may obtain access to financially relevant information.

Recommendation

KPMG recommends that PSEG Long Island make appropriate changes to the Active Directory and RACF password standards to meet the minimum password management standards outlined in the PSEG Long Island IT Security Policy or PSEG Long Island should update their password policies and standards to appropriately reflect the current mainframe standards and their system limitations.

Management Response

New accounts are created through two different methods. Employee accounts are created through an automated process and for accounts created using the automated process password change requirement is enforced on first log-on. Contractor accounts are manually created. The manual creation process requires the administrator to explicitly select the option to enforce password change on first log-on. When the process was demonstrated this step was missed. Normal password expiration and change policy is in effect for all accounts. All accounts are disabled after 60 days of inactivity. All contractor accounts are deleted at expiration date or December 31st of each year.

At National Grid, the Authority's previous service provider, the standard was set to 8 characters, allowing for special characters and numbers. This requirement was transitioned to PSEG Long Island. In the past, this was listed as an exception to the audit. Extensive investigation, modifications, and testing would need to be performed in the CICS CAS/EBO subsystems, all mainframe web interfaces, MDT's, Agent Desktop password storage feature, TSO, etc. This is a global change that would affect all mainframe applications at once and could present an extreme risk to daily business operations.

PSEG Long Island has updated its password governance to document the mainframe configuration is the standard for mainframe passwords. The standard was updated April 30, 2015 and published to the repository of PSEG Long Island Information Technology Internal Controls.

The mainframe does not support multiple password expiration policies. PSEG Long Island proposes a waiver to the corporate password expiration policy for mainframe administrators.

Finding #2: Access Recertification over Network, CAS and EBO Applications, and Mainframe Operating System

Observation

KPMG inspected the High Level Access Review report and noted this quarterly review was only of high level administrator access accounts to the network and mainframe. We were informed a periodic review is performed on user access to the Active Directory, CAS and EBO applications and the RACF but were unable to obtain evidence a review was performed.

Risk

Without periodic access reviews, terminated or transferred user accounts may exist in financially relevant applications. This may lead to inappropriate or unauthorized access to financially significant data and may impact the financial reporting process.

Recommendation

KPMG recommends PSEG Long Island perform periodic access review of all user access to the Active Directory, CAS and EBO applications, and the Mainframe Operating System. This will enable application administrators to remove inappropriate/inactive IDs in a timely manner and will reduce the possibility of malicious activity by unauthorized users.

Management Response

In 2015, during a Customer Data Protection Audit, PSEG Long Island Internal Audit had identified an observation in which a CAS entitlement review was not being performed by the Customer Services Group. As a result of that observation management implemented a formal process to perform the required annual review for customer PII user entitlements to ensure user access is appropriately granted. PSEG Long Island Internal Audit performed a follow up review and noted that Customer Service had completed the entitlement reviews for CAS, using a tool created by IT that shows the transaction types for each user in CAS. These listings were provided to the Managers of each department to review and approve the access, based on the transaction type associated to the user and their job functionality.

For 2016, PSEG Long Island will add an entitlement review for EBO access modeled on the CAS approach that was implemented in 2015. For RACF, an entitlement review for all TSO accounts will also be added which will address accounts that are not already covered by the Quarterly High Level Access Review.

There is an automated process that creates and removes employee accounts in Active Directory based on a daily data feed from the SAP Human Resources system. IT performs periodic reviews of all Active Directory users to verify that the automation that deactivates an AD account upon leaving the company is working properly. All active employees are entitled to Active Directory access as normal part of employment. Contractor accounts are setup to expire in the current calendar year. Upon

renewal of the contractor account, the responsible manager submits a request to extend the account which also recertifies the entitlement.

Finding #3: Unauthorized Access to EBO Database Privileged Group

Background

PSEG Long Island manages the Authority's in scope applications (CAS & EBO), which are hosted at PSEG Long Island's Data Center located in Garden City, New York. CAS and EBO applications are supported by the Mainframe environment, which is supported by the RACF security management structure. The EBO backend database is DB2. The access is role based and the following roles exist for DB2 database access:

1) Role 700 - Allows limited updates

2) Role 701 - Allows to make changes.

3) Role 702 - Super User/Privileged Access

4) Role 766 - IT Personnel (Simulation Mode)

Observation

KPMG inspected the EBO database privileged listing, group 702, and upon inquiry with management and inspection, determined that access does not follow the least privileged concept. Specifically we noted the following weaknesses with regard to EBO database access to the privileged access group 702:

- Twenty two users inappropriately retained access to the privileged group 702 in DB2. Upon inquiry with management and inspection, we noted the super user access privilege is not requested when access is authorized and is not required for the Customer Operations personnel to perform their job responsibilities.
- Twenty three (23) accounts were identified as needing to be removed. Of these 21 accounts belonged to former National Grid personnel. KPMG noted these accounts did not have an active network or mainframe accounts.

Risk

Not properly enforcing least privilege access rights increases the risk of users accessing and modifying information within the system that is not authorized by management. These changes could adversely affect the, confidentiality, availability, and integrity of EBO data.

Recommendation

KPMG recommends that management enforce the least privilege concept and assign access to commensurate with job responsibilities.

Management Response

The twenty two user accounts reported as inappropriately retaining access had already been revoked from RACF and did not have any access to DB2 or EBO and was explained to KPMG during the audit.

IT grants access to EBO based upon authorization and approval from the business. The business makes the determination of the appropriate access level based upon the role.

Authorization is provided using the security access request form which is attached to a Service Now access request ticket. The request ticket is routed to IT where it is reviewed to determine that no inappropriate high level access is requested. Effective July 1, 2016, the review will be documented in the Work Notes section of the Service Now ticket by the IT Administrator who fulfills the request.

The security of EBO access is controlled through RACF. As noted in the finding, the RACF accounts were disabled, so access to EBO would not be possible for any of the twenty three accounts. The procedure for EBO accounts has been modified so when RACF accounts are removed, the EBO accounts are also removed.

Finding #4: Changes to programs are not tested and approved to production

Background

PSEG Long Island manages the Authority's in scope applications (CAS & EBO), which are hosted at PSEG Long Island's Data Center located in Garden City, New York. CAS and EBO applications are supported by the Mainframe environment, which is supported by the RACF security management structure. Access to the network is managed by the Windows Active Directory framework. Changes to CAS, EBO, EBO database DB2, RACF (mainframe) and Active Directory must be tested and approved prior to their move to production.

Observation

Inspected the change documentation for a selection of CAS, EBO, EBO database DB2, RACF mainframe changes and Active Directory changes and noted the following weaknesses:

- Documentation on successful testing could not be evidenced for 2 EBO changes out of a selection of 25 CAS and EBO changes. Additionally, change documentation to evidence testing and approval to migrate to production could not be evidenced for 5 (3 CAS and 2 EBO) out of the selection of 25 changes.
- Documentation to evidence testing and approval to migrate the change to production could not be evidenced for 1 out of a selection of 2 DB2 changes.
- Documentation on successful testing could not be evidenced for 1 out of a selection of 8 Mainframe changes. Additionally, documentation to evidence testing and approval to migrate

the change to production could not be evidenced for 3 out of a selection of 8 Mainframe changes.

- Documentation to evidence testing and approval to migrate the change to production could not be evidenced for 1 out of a selection of 3 Active Directory changes.

Risk

Change control process is not effective if documentation is not maintained to evidence the changes were tested and approved by the relevant parties to be migrated to production and increases the likelihood for unauthorized changes to the production environment. Changes that are implemented without testing or inadequate testing increases the risk of the system failure or inaccurate processing of financial data.

Recommendation

KPMG recommends that PSEG Long Island enforce the change control process and require documentation of testing and approval of the change for migration to production be retained.

Management Response

Based on a review of the CAS/EBO Change Requests that were identified PSEG Long Island had located and provided to KPMG the requested evidence for the following for the 5 CAS changes:

- CHG0000037928 – There was an e-mail from Richard Maklary attached to the change that provides his approval based on his verification as the user.
- CHG0000036140 – There was an e-mail from Jenna Hanley attached to the change that provides her approval based on her verification as the user.
- CHG0000035496 – There was an e-mail from Patricia Faltings attached to the change that provides her approval based on her verification as the user.
- CHG0000037708 – This change was only a change to the EBO database (DB2) to include two new users. There was no change to the code or design of the system. Note that this was not a CAS change.
- CHG0000036223 – There was an e-mail from Jeffrey Sills attached to the change that provides his approval based on his verification as the user.

Regarding the two EBO changes identified, PSEG Long Island had identified and have located the following:

- CHG0000036938 – This change was only a change to the EBO database (DB2) to include two new users. There was no change to the code or design of the system.
- CHG0000035576 – This ticket was for an update to the COTS product VeriMove from Pitney Bowes which is performed on a periodic basis. As described in the test plan section of the ticket the software will be tested on the Development server first.

PSEG Long Island will continue to reinforce the need for including CAS/EBO application test results with Change Requests with the IT team. PSEG Long Island will not approve the change request until CAS/EBO application test results and approval are attached to the change ticket.

Finding #5: Lack of Access authorizations forms

Background

PSEG Long Island is a third party service provider that manages the Authority's power producing facilities and transmissions. Through various management agreements with the Authority, PSEG Long Island provides customer support (billing, cash collections and services) to the Authority's electric customers. Furthermore, PSEG Long Island manages the Authority's in scope applications (CAS & EBO), which are hosted at PSEG Long Island's Data Center located in Garden City, New York. CAS and EBO applications are supported by the Mainframe environment, which is supported by the RACF security management structure. Access to the network is managed by the Windows Active Directory framework.

Observation

Inspected the access authorization forms for a selection of new users and determined the following:

- Approval for access to be granted could not be evidenced for 4 out of a selection of 25 Active Directory accounts.
- Approval for access to be granted could not be evidence for 1 out of a selection of 25 CAS accounts.

Risk

Weak access controls increases the risk of unauthorized access to the system environment.

Recommendation

KPMG recommends PSEG Long Island require documented approval to grant access to the systems and these authorizations are retained.

Management Response

Active Directory has been remediated. Employee accounts are created through the SAP interface. Contractor accounts are now requested through the Service Now application. All documentation will be retained as evidence.

CAS Accounts are only created based upon approved requests in Service Now from the Customer Business unit.

Finding #6: Data restorations are not performed

Background

PSEG Long Island manages the Authority's in scope applications (CAS & EBO), which are hosted at PSEG Long Island's Data Center located in Garden City, New York. CAS and EBO applications are supported by the Mainframe environment, which is supported by the RACF security management structure. Access to the network is managed by the Windows Active Directory framework. PSEG Long Island data are mirrored to an offsite location to serve as the backup.

Observation

KPMG inquired of management and inspected relevant documentation regarding data restorations and were informed that data restoration tests are not performed annually due to resource constraints.

Risk

If backups are not periodically checked to help ensure they are accessible, the risk exists that if there was an interruption to PSEG Long Island's system environment, financially relevant data, relied upon to generate reports, could be lost and not be recoverable.

Recommendation

KPMG recommends that formal data restoration procedures should be put in place and restoration testing should occur on at least an annual basis.

Management Response

Evidence of multiple occurrences of actual successful restores was provided to KPMG during the audit. However, there is no documented procedure to test restores from the backup on a periodic basis.

PSEG Long Island will develop a process and procedure for testing viability of data backups by performing restore of a data sample on a periodic basis.

In addition, we identified a deficiency in internal control that we consider to be a significant deficiency, and communicated that in writing to management and those charged with governance on March 21, 2016.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Authority's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of management, the Finance and Audit Committee, and others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

KPMG LLP
345 Park Avenue
New York, NY 10154-0102

June 28, 2016

Finance and Audit Committee
Long Island Power Authority
Uniondale, New York

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the Long Island Power Authority (the Authority), as of and for the year ended December 31, 2015, in accordance with auditing standards generally accepted in the United States of America, we considered the Authority's 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.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized as follows:

Finding #1: No procedures in place over data restoration – Data Restoration

Background
Epicor is an application used by the Authority for cash & investments, accounts payable, accrual, and expenses. The application is managed by the Authority and the source code is owned by the vendor. Epicor's operating system is Windows 2003 and is supported by an SQL 2005 Server. A formally documented Disaster Recovery process is in place at the organization.

Observation
KPMG noted that there are no written procedures in place over data restoration. Furthermore, the Disaster Recovery plan does not cover Epicor application within its scope. Per conversation with the Authority, data recovery is performed sporadically throughout the year for employees needing restoration of deleted files.

Risk
Financially relevant data, relied upon to generate reports, could be lost and not be recovered. This is especially important with tape media because tapes wear out and tape drives get dirty over time.

Recommendation
KPMG recommends that formal data restoration procedures should be put in place and restoration testing should occur on at least an annual basis. Epicor should be added to the formal disaster recovery plan process testing.

Management Response

Restores of the entire Epicor database are done in the test environment several times per year. In addition, backups are first completed to hard disk based virtual libraries followed by migration to tape. In extreme situations, only the latest backup would be required and that would only be a tape that is that is no more than a week old. Those tape drives are automatically cleaned and tested by our automated tape library. Tapes are not reused, but shipped for safe environmentally appropriate storage to a third-party vendor.

The observation on Epicor is noted, and will be added to the formal disaster recovery plan during 2016.

Finding #2: No System Development Life Cycle (SDLC) procedures are in place at the Authority – Program development

Background
Epicor is an application used by the Authority for cash & investments, accounts payable, accrual, and expenses. The application is managed by the Authority and the source code is owned by the vendor. Epicor's operating system is Windows 2003 and it is supported by an SQL 2005 Server.

Observation
KPMG noted that there are no SDLC procedures in place at the Authority for system upgrades. KPMG noted that SDLC procedures existed, but since the change in service provider, those SDLC procedures are no longer relevant.

Risk
If there are no formal procedures in place for program development there is a risk of failed implementation of programs that could lead to incorrect information in financial reports.

Recommendation
KPMG recommends that the Authority have formal SDLC procedures in place for new program and infrastructure development, which includes all major phases of program development and implementation.

Management Response

The platform used is Windows 2012R2 and SQL 2012.

The observations and recommendation are accurate; however, the Authority believes this risk is very low. If a new system would be put in place financial information is verified and a backup to the old system is always provided for. Even during upgrades preformed to Epicor in 2015, all financial control reports were produced prior to upgrade and subsequent to upgrade to ensure the accuracy of data during transition. Such documentation was provided and a formal procedure document will be completed during 2016.

Finding #3: User Acceptance Testing (UAT) was not appropriately performed for Epicor upgrade – Program development

Background
Epicor is an application used by the Authority for cash & investments, accounts payable, accrual, and expenses. The application is managed by the Authority and the source code is owned by the vendor. Epicor's operating system is Windows 2003 and it is supported by an SQL 2005 Server. During the current audit period under review, a major version upgrade of the application was undertaken and defined as a project by the Authority. The Authority performed a version upgrade in 2015 per vendor requirements and guidance.

Observation
While UAT testing was conducted within the current audit period under review, it was informal and ad hoc and did not include testing scripts. KPMG further noted that UAT documentation that was provided all appears to have been conducted after the first phase of the project concluded and as such no UAT documentation appears to have been retained and provided for the first phase. KPMG recommends that formal UAT procedures as defined by industry best practices be followed for the UAT and appropriate approvals be retained for project implementation.

Risk
If testing, review and approval by appropriate individuals within the organization is not documented and conducted for program development, there is a risk of failed implementation of programs that could lead to incorrect information in financial reports.

Recommendation
KPMG recommends that the Authority have a formal process of requirements documentation as outlined by industry best practices for new program and infrastructure development, which includes all major phases of program development and implementation such as UAT testing and approval by appropriate members of IT and business staff.

Management Response

A review of all financial reports was completed before and after in the test system to verify accuracy prior to going live with new system. Evidence of all reports were provided to KPMG.

A formal procedure document will be completed during 2016.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Authority's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of management, the Finance and Audit Committee, and others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

KPMG LLP
345 Park Avenue
New York, NY 10154-0102

Management and Finance & Audit Committee
Long Island Power Authority
Uniondale, New York

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the Long Island Power Authority (the "Authority") as of and for the year ended December 31, 2015, in accordance with auditing standards generally accepted in the United States of America, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances 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.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses and/or significant deficiencies and therefore, material weaknesses and/or significant deficiencies may exist that were not identified. However, as discussed below, we identified a deficiency in internal control that we consider to be a *significant deficiency*.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

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 a 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. None of the identified significant deficiencies described below are considered to be material weaknesses.

A significant deficiency is a deficiency, or a 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. We consider the following deficiency in the Authority's internal control to be a significant deficiency:

PSEG – Long Island (PSEG-LI) manages and hosts the Authority's billing and customer information technology systems (CAS & EBO). A significant deficiency was identified over the monitoring controls of access to the development and production environments resulting in the risk that certain individuals could develop changes to the system configuration and put those changes into production without appropriate monitoring or detective controls in place.

Management's Response:

During KPMG's audit, a separation of duties deficiency was identified. It is PSEG Long Island's position that the current System Administrator access is a standard practice and required to perform maintenance activities in CAS/EBO. Entitlement reviews within Customer Operations control all CAS/EBO access and validates each user's need with appropriate management. In addition, there are mitigating financial controls that PSEG Long Island's Finance team performs including analytical reviews of monthly revenue variances by customer segment to review variances to plan as well as reviews of customer usage and revenue within Customer Operations.

PSEG Long Island did internally review and confirm that all file access and changes performed by the System Administrators who do have access to both development and production environments are being logged. PSEG Long Island already monitors the daily "RACF Violation" and "Special Access" reports which are captured in the PageCenter tool. Also, all moves from development to production are approved and tracked through the PSEG change management process.

As a result of the above limited exposure, Information Technology monitoring, and mitigating financial controls, PSEG Long Island views this control deficiency as a low risk to the Authority, however PSEG Long Island has agreed to institute an additional control to monitor System Administrator activity. Our Mainframe security team is in the process of documenting a procedure for further monitoring and we are estimating that it will take 30-60 days to have the custom security report in place to support the monitoring of System Administrator activities.

The Authority's written response to the significant deficiency identified in our audit was not subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on it.

This communication is intended solely for the information and use of management, the Finance and Audit Committee, and others within the organization, and is not intended to be, and should not be, used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

New York, New York
March 21, 2016