FINAL DRAFT

THE TRUSTEES OF THE PUBLIC LIBRARY OF THE CITY OF BOSTON

MANAGEMENT LETTER

JUNE 30, 2016

FINAL DRAFT

CliftonLarsonAllen LLP
CLAconnect.com

To the Honorable Board of Trustees
The Public Library of the City of Boston, Massachusetts

In planning and performing our audit of the financial statements of The Trustees of the Public Library of the City of Boston (Library), a component unit of the City of Boston, Massachusetts, as of and for the year ended June 30, 2016, 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, we considered the Library's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Library's internal control. Accordingly, we do not express an opinion on the effectiveness of the Library's internal control.

However, during our audit we became aware of several matters that are opportunities for strengthening internal controls and operating efficiency. The memorandum that accompanies this letter summarizes our comments and recommendations regarding those matters. This letter does not affect our report dated November 11, 2016, on the financial statements of the Library.

We will review the status of these comments during our next audit engagement. We have already discussed many of these comments and suggestions with various Library personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

The Library's written responses to the matters identified in our audit were prepared by the Library's Chief Financial Officer. The responses have not been subjected to the audit procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

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

CliftonLarsonAllen LLP

Boston, MA
May 5, 2017

FINAL DRAFT

THE TRUSTEES OF THE PUBLIC LIBRARY OF THE CITY OF BOSTON

MANAGEMENT LETTER

JUNE 30, 2016

TABLE OF CONTENTS

Comments and Recommendations

Information Technology

Comment

We evaluated the Library's computer processing environments and general controls over information technology related to business and financial systems. The evaluation was not intended to be a full scope network security review of the Library's information technology infrastructure. The scope was limited to internal controls and security features related to the integrity of transactions and data that could impact financial reporting.

The following is a summary of the deficiencies we identified that were also reported in the prior year Management Letter:

- During the fiscal year under audit, there were no periodic reviews of permissions and security roles assigned to users in the Polaris application to validate employees and approved business partners continue to have appropriate access based on job responsibilities. It is our understanding that the Library intends to do this during fiscal year 2017.

- During the fiscal year under audit, there was not a regular schedule to test the restoration of backed up data for the PeopleSoft and Polaris applications to verify data would be recoverable and readable should an incident or disaster occur. It is our understanding that the Library intends to do this during fiscal year 2017.

- Full-scale security assessments are not periodically conducted, which would include an internal vulnerability assessment, external penetration test, social engineering assessment, and/or phishing assessment

- A full set of policies and procedures have not been formally documented. At the time of our evaluation, the Library had started drafting network and server security policies.

The following is a summary of additional deficiencies we identified:

- The Library has three Windows 2000 and five Windows 2003 servers active on its network. These servers are no longer supported by the vendor and have known vulnerabilities. An attacker could exploit these known vulnerabilities to access the network.

- The Library does not have a documented IT Strategic Plan, nor does it have a formal Information Technology Committee. Currently the IT managers meet on a weekly basis, discuss, prioritize, and assign projects. However, formal documentation of the discussions and projects is not maintained.

Recommendations and Management's Responses

We recommend the following:

- **Recommendation # 1:** Perform periodic reviews (i.e. annual) of all permissions and user roles in Polaris to ensure permissions are consist with job responsibilities and user roles are assigned appropriately to employees and approved business partners. The review should be documented, including any changes made as a result of the review. In addition, implement detective controls such as reviewing of user access logs in Polaris to ensure no activity appears inappropriate.

- **Management's Response:** This audit was completed in September 2016. The Library's applications manager also makes these changes on a regular basis each time there is a position update initiated through HR. Starting in FY17 and continuing in future fiscal years, the IT Department will conduct this audit on an annual basis, and file a report with Library's Human Resources Department and Chief Financial Officer by June 30th.

- **Recommendation # 2:** Develop a schedule for PeopleSoft and Polaris to perform data backup restore testing on a semi-annual basis to verify data would be recoverable and readable should an incident or disaster occur. The restores should be documented to provide evidence that the restore took place, the restore was successful, and the data was readable.

  - **Management's Response:** Innovative/Polaris conducts regular audits and generates reports and contacts the Library's IT Department when there is unusual activity on the server level. For the client level, sample testing will be completed during the upcoming upgrade. The Polaris testing will be completed during this upgrade which is scheduled for the end of May. In future fiscal years, BPL IT will repeat this test on a Bi Annual basis, and include in a report to the Library's Chief Financial Officer by June 30th.

    The PeopleSoft system is maintained by the City of Boston Department of Innovation & Technology. Therefore, the Library BPL does not have the authority or responsibility to perform testing on these systems. However, the City has tested a restoration of backed up data within the past year.

- **Recommendation # 3:** Perform periodic reviews to assess the security and configuration weaknesses of the internal network

  - **Management's Response:** A full slate of security testing was conducted by an external entity in 2014. The Library is in the process of contracting with a provider to perform this work again, which will allow the Library to conduct this assessment of a periodic basis. This assessment will be included in a report to the Library's Chief Financial Officer by June 30th of each year.

- **Recommendation # 4:** Formally document policies and procedures, obtain management approval and perform periodic reviews of policies and procedures

  - **Management's Response:** The Library is reviewing what policies and procedures already exist to determine the status of this recommendation. While the process did begin in FY17, it will likely not be concluded until FY18.

- **Recommendation # 5:** Upgrade the Windows 2000 and five Windows 2003 servers

  - **Management's Response:** These windows servers are scheduled to be decommissioned upon launch of the new bpl.org website. A series of launch milestone events are anticipated to commence in FY18.

- **Recommendation # 6:** Establish a formal Information Technology Committee, which should include IT leaders and stakeholders from other departments. This committee would provide direction and oversight to the IT environment. Minutes from Committee meetings should be maintained. Additionally, an overall project sheet IT Strategic Plan should be kept and maintained where all appropriate staff has access.

- **Management's Response:** The Library's most recent technology plan covered the period 2013-2016. The specific external requirements to maintain such a plan no longer apply. With anticipated hiring of a new Chief Technology Officer, the library will develop a new strategic Digital, Online and Technology Service plan and form an Emerging Technology committee during Fiscal Year 2018 to study new technologies and vet strategic plans. Also, there is a weekly IT managers committee which works on policy, projects and operations. Currently capital IT projects are tracked through the Project Management Offices project tracking process. Moving forward, smaller projects will be tracked here as well.