Tailored Technologies LLC

685 Third Avenue
New York, NY 10017

Tel: (212) 503-6300

Date: January 19, 2017

To: To the file of Battery Park City

From: Tailored Technologies LLC

Technology Observations and Recommendations Resulting From the October 31, 2016 Audit

---

Marks Paneth LLP has issued a management letter under AU-C Section 265 indicating they did not observe any material weaknesses. The memo below represents our observations that are either minor in nature or represent best practices pertaining to technology. Matters in this memo are as of the date of this letter. If matters should arise between this date and the date of Marks Paneth LLP's audit report on the financial statements, we will update this memo.

Exhibit I of this memo lists new items that we noted during our work in connection with the Hugh L. Carey Battery Park City Authority's financial statement audit for the year ending October 31, 2016. Exhibit II pertains to prior year recommendations that, based on our current procedures, appear to require further attention by management. Exhibit III are those observations and recommendations from the prior year's letter that appear not to require further action.

It should be noted that we will review management's current year responses during Marks Paneth LLP's next audit cycle.

TABLE OF CONTENTS

OVERVIEW

On December 9, 2016, Marks Paneth LLP's Tailored Technologies met with the following individuals:

1. Robert Serpico, Chief Financial Officer
2. Karl Koenig, Controller
3. John Tam, Director of IT
4. Robert Quon, Deputy Director of IT
5. Neresa Gordon, Network Security Manager
6. Su May Ng, Senior Programmer Analyst
7. Leandro Lafuente, Senior Systems Administrator

Our examination was performed in conjunction with the Hugh L. Carey Battery Park City Authority (BPCA) financial statement audit for the year ended October 31, 2016. We considered the internal controls within the Information Technology (IT) infrastructure and collected and evaluated evidence of BPCA's information systems, practices, and operations in order to 1) assist the Marks Paneth LLP audit team to gain reliance on the computer controls for an effective and efficient audit process through the validation that information systems are safeguarding assets and maintaining data integrity and 2) provide recommendations as to whether the use of automation is being optimally utilized and operating effectively and efficiently to contribute to BPCA's goals and objectives.

Currently, BPCA has 28 physical and virtual servers running Microsoft Windows Server 2008 or 2012 or VMware ESXi 5.5. BPCA uses:

1. Microsoft's Dynamics GP (Great Plains) version 2013 as its accounting software
2. Paramount's WorkPlace version 12 for project accounting and procurement
3. Sage's Abra version 9.01 as its Human Resources Information System
4. ADP's online service to process payroll
5. ADP's eTIME version 8 for time and attendance tracking
6. OpenText eDOCS 5.3.1 for document management

The following observations and recommendations are focused on:

1. Data Restore Testing

CYBER SECURITY

We also considered BPCA's cyber security protections and its ability to detect and prevent unauthorized internal and external access to BPCA's network. We looked at the policies and procedures in place to ensure secure processes are maintained, and BPCA staff is informed of current, secure practices. It would be impractical as part of this IT audit process to provide a full cyber security review. Cyber security protections at BPCA include:

1. A pair of SonicWALL NSA 3500 clustered firewall devices at the BPCA offices
2. Symantec's Endpoint Protection version 12.5 to protect against viruses and malware
3. Spam filtering through US Internet, BPCA's email provider, as well as through their SonicWALL firewall devices
4. Onsite and offsite backup of BPCA data and virtual services using QuorumLabs' services
5. Penetration testing of the BPCA network performed twice a month by the New York State Office of Information Technology Services
6. VMware's AirWatch mobile device management platform for BYOD protection of BPCA-provided portable devices, which includes the ability to delete ("wipe") data on the mobile devices

Exhibit I – Current Year Recommendations

1) Data Restore Testing

Observation: We were informed BPCA does not perform periodic, scheduled test restores of backed up data. While user files are restored on an as-needed basis, the restored data, consisting of critical files and systems, is not formally tested. The concern is core financial and critical operational files could become unrecoverable, leaving the ability to restore and recover these files in doubt.

Recommendation: BPCA should consider creating formal policies and procedures requiring the periodic review and testing of backup processes. The policies and procedures should address, at minimum:

1. The review of documentation and backup job configurations to ensure the proper capture of all financial and operational data
2. The identification of the staff members who are authorized to approve the restore of data
3. The identification of staff members who are authorized to access the data backup storage
4. The identification of the backup data stores which must be encrypted
5. The schedule and scope of each test restore of both onsite and offsite data and verification steps to ensure the backup media is sound, and the data is correct and not corrupt

Files (such as Microsoft Word or Excel files): for testing the restore process and the integrity of backed up files and documents, we recommend:

1. Test restores of files occur at least once a quarter
2. IT, Finance, and operational staff prepare a list of critical files to be restored each quarter. We recommend a different list of files for each quarter
3. IT staff restore the identified files to a testing environment (either a separate directory or server) and have Finance and or operational staff open and inspect the files
4. The results of the test restores be documented and reported to senior management

Applications and Databases: Best practices dictate financial and critical operational applications and databases should be periodically restored to ensure the database can be properly restored should the production equipment fail. We recommend BPCA perform restore testing for all components of the Microsoft Dynamics GP system. Testing should include, at minimum:

1. Identification of a set of key reports by the business process owner; the reports should be generated by the production application immediately before backing up the application database
2. A restore of the application database from backup to a physical or virtual recovery server. This should be performed for both onsite and offsite backups
3. The business process owner should run a set of key reports from the restored database and compare with the production reports to ensure the accuracy of the backed up / recovered data

Management's Response: Management agrees with the recommendations and will develop a policy and procedure for restore testing that follows the requirements outlined in the above discussion. The first restore will be conducted before 7/1/17.

****END OF NEW RECOMMENDATIONS****

Exhibit II – Prior Year Observations Requiring Further Attention

There are no prior year observations and recommendations which require further attention.

**** END OF REPEAT RECOMMENDATIONS****

Exhibit III – Prior Year Recommendations That Appear Not to Require Further Action

2) Accounting System Permissions (Prior Year Observation #1)
3) Disaster Recovery Planning (Prior Year Observation #2)

****END****