Tailored Technologies LLC

685 Third Avenue
New York, NY 10017

Tel: (212) 503-6300
Fax: (212) 503-6312

Date: January 20, 2016

To: John Tam, Director of IT

Cc: Robert Serpico, Chief Financial Officer
The Audit File of the Hugh L. Carey Battery Park City Authority

From: Tailored Technologies LLC

Technology Observations and Recommendations Resulting From the October 31, 2015 Audit

---

HUGH L. CAREY BATTERY PARK CITY AUTHORITY
IN CONJUNCTION WITH THE FINANCIAL STATEMENT AUDIT FOR OCTOBER 31, 2015
INFORMATION TECHNOLOGY OBSERVATIONS AND RECOMMENDATIONS

OVERVIEW

On January 6, 2016, Marks Paneth's Tailored Technologies met with:
Robert Serpico, Chief Financial Officer
Karl Koenig, Controller
John Tam, Director of IT
Robert Quon, Deputy Director of IT
Neresa Gordon, Network Security Manager
Su May Ng, Senior Programmer Analyst
Leandro Lafuente, Senior Systems Administrator

We also spoke with Benjamin Jones, VP of Administration, and Anthony Robinson, Office Manager.

Our procedures were performed in conjunction with Hugh L. Carey Battery Park City Authority's ("BPCA") financial statement audit for the year ended October 31, 2015. 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 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 whether the use of automation is being optimally utilized and operating effectively and efficiently to contribute to BPCA's goals and objectives.

BPCA has 19 physical and virtual servers running Microsoft Windows Server 2008 or 2012 or VMWare ESXi 5.5. There is one Windows Server 2008 server at the Regatta and 6 physical and virtual servers at the Battery Park City Parks Conservancy ("BPCPC") office running Windows Server 2012 or VMware ESXi 5.5. BPCA uses:

1. Microsoft's Dynamics GP (Great Plains) version 2013 as their accounting software
2. Paramount's WorkPlace version 12 for project accounting and procurement
3. Sage's Abra version 9.01 as the Human Resources Information System
4. ADP Online service to process payroll
5. CMA's LATS and ADP's eTime for time and attendance tracking
6. OpenText for document management

We also considered BPCA's cyber security protections and its ability to detect and prevent outsiders from gaining 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 offer a full cyber security review. Cyber security protections include deployment of:

1. A pair of SonicWall NAS 4500 clustered firewall devices at the main office and Regatta location
2. A pair of SonicWall NAS 3500 clustered firewall devices at the BPCPC offices
3. SonicWall TZ 215 firewall devices at all satellite locations
4. Symantec's Endpoint Protection version 12.5 to protect against viruses and malware
5. Spam filtering through U.S. Internet Services, BPCA's email provider
6. AirWatch mobile device management platform to for BYOD protection of BPCA-provided portable devices, which includes the ability to delete ("wipe") data on the mobile devices
7. Browser based only access to email using personal devices
8. Onsite and offsite backup of BPCA data and virtual services using QuorumLabs services
9. Penetration testing of the BPCA network performed monthly by New York State Office of Information Technology Services

The following observations and recommendations are focused on the need to:

1. Review the accounting system permissions for each user
2. Develop a complete Business Continuity and Disaster Recovery Plan

TABLE OF CONTENTS

Exhibit I – Current Year Recommendations

There are no new observations and recommendations for the current year.

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

Exhibit II – Prior Year Observations Requiring Further Attention

1) Accounting System Permissions (Prior Year Observation #1)

Observation (2013): We were provided documentation detailing account permissions within the Microsoft Dynamics GP (Great Plains) application. We note that all Finance Department (Fin1 and Fin2) accounts have permission which includes "all posting of the financial series", "the ability to post Payables Management checks", and "all posting of the purchasing series". The concern is that segregation of duties is not enforced within the application whereby staff can enter and post transactions without oversight. Over half of the accounts (26 out of 39) have permission to "post scheduled vendor payments" and "maintain vendors". Best practices dictate that the number of staff with access to post vendor payments and maintain vendor records should be limited in order to reduce the potential for fraud.

Initial Recommendation: Management should consider reviewing the permissions associated with the user accounts in Great Plains. Best practices dictate that posting transactions and maintaining vendors should be limited to senior accounting staff and accounts with permission to post should be restricted from entering transaction data.

2015 Status: There has been no change in the status of this comment in the past audit year. We remain concerned that the permissions granted to users does not align with the segregation of duties outlined in the BPCA financial procedures. A particular concern is all users in the BPCA_FIN1 and BPCPC_FIN1 groups have permissions to "Set up General Ledger" and "Set up Users and Security." Our review of documentation provided indicates:

1. 7 of the 14 staff at BPCA have BPCA_FIN1 permissions
2. 5 out of 6 staff at BPCPC have BPCPC_FIN1 permissions
3. 2 of the IT staff have BPCA_FIN1 permissions

All IT staff are also assigned POWERUSER permissions, which allow access to all Dynamics GP functions.

We continue to recommend BPCA:

1. Review the permissions assigned to each user account and restrict user permissions based on their roles, responsibilities, and segregation of duties
2. While we understand IT staff and vendors require administrative access to perform maintenance and upgrade tasks, BPCA should create policies and procedures for the Controller to enable the IT accounts only when work is performed and disable them when the task is complete

There is an additional concern relating to the permissions granted to the Chief Financial Officer's access account. We were informed the Chief Financial Officer does not perform any data entry or transactional tasks with Dynamics GP. However, his account gives him the broad permissions of the BPCA_FIN1 group. We recommend the Chief Financial Officer's account be restricted to read-only access to the Dynamics GP system.

Management's 2015 Response: Management agrees with the recommendation. The user roles and permissions, including those for IT staff, are already being reviewed on a quarterly basis (with a ticket in Track-IT as a reminder) and adjusted as needed. The Chief Financial Officer's account will be set as read-only.

2) Disaster Recovery Planning (Prior Year Observation #6)

Initial Observation (2010): While BPCA does have data backup procedures in place, it lacks a comprehensive Business Continuity Plan for key financial and operational systems such as Dynamics GP (Great Plains), Workplace, and Abra. A comprehensive assessment of the potential impacts, acceptable down times, and an actionable recovery plan for operations at BPCA has not been developed. A complete plan will assist management in understanding the organization's risks and options with respect to managing unforeseen disruptions. In addition, the Business Continuity Plan should be updated on a regular basis to reflect changes in the operational and computer infrastructures.

We note the MIS Department is in the process of constructing mirrored server environments in both the One World Financial Center and Albany locations. The plan is to replicate applications and data from One World Financial Center to Albany at regular intervals throughout the day. Under this plan, the Albany location will be used as a remote data back up facility and a failover site.

Initial Recommendation: Management should consider developing a comprehensive Business Continuity Plan listing procedures, personnel and contact information. Please note that any recommendations made with respect to Business Continuity planning are for outline purposes only. It would be impractical as part of this IT audit process to offer all the necessary components of a fully operational plan.

1. Create an organization wide business continuity plan covering all mission critical aspects of the organization including, but not limited to, technology.
2. Conduct a Business Impact Analysis to determine what the mission critical functions at BPCA are, who performs them and what resources would be needed in a business interruption. These critical functions and the corresponding procedures should be fully documented and included as part of a comprehensive Business Continuity Plan.
3. As part of a Business Impact Analysis, evaluate and document the "Recovery Time Objective" for mission critical functions. Include in your evaluation "busier" times of the year (or month) and decide upon a suitable course of action for these time periods.
4. Management should prioritize the completion of the mirrored server environments between the One World Financial Center and Albany locations. Include full testing, documentation and periodic updates of the remote access procedures to the Albany servers and distribute to staff.
5. Create and document a formal data backup and restore procedure.
6. Make sure physical copies of all installation media for operating systems and applications are stored off site. Include a full list of registration and licensing information.
7. Ensure all BPCA's vendor contact information, including the IT vendors, is documented and periodically updated in the Business Continuity Plan.
8. Make sure management has access to administrative network security rights in the event that the MIS staff or outside consultants become unavailable in a disruption.
9. Develop and document emergency procedures and distribute to each employee.
10. Keep a copy of the Plan stored in an off-site location. Consider requiring key staff to keep a copy of the Plan stored on a secure USB drive so that the Plan is available to them at all times.
11. Determine an alternate meeting place in the event your current location becomes inaccessible, as part of an overall disaster recovery plan.
12. Document the procedures to migrate back to a normal production environment after the emergency situation has been resolved.

2015 Status: BPCA has made progress in its disaster preparedness in the past audit year. Most notably, BPCA has engaged the services of QuorumLabs to provide onsite and offsite redundancy of its virtual servers. Should one of BPCA's physical server's fail, BPCA can use the QuorumLabs onsite appliance to host virtual servers; should the data center at the main location become unavailable, QuorumLabs can deploy the virtual servers in its offsite data center. BPCA is also in the process of:

1. Creating a formal Business Impact Analysis of all systems and departments
2. Preparing the Regatta location as a disaster recovery site for staff
3. Preparing formal Action Plan documentation for IT and office staff
4. Testing the disaster recovery capabilities of the onsite appliance and offsite data center

We continue to recommend management allocate the resources necessary to complete the disaster recovery preparedness and create a formal Business Continuity and Disaster Recovery Plan.

Management's 2015 Response: Management agrees with the recommendation. A disaster recovery preparedness plan along with a formal Business Continuity Plan is in the process of being created and will be finalized once final testing of the system is complete.

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

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

3) Outdated Server Operating System (Prior Year Observation #2)

4) MIS Rights to Financial and Operational Systems (Prior Year Observation #3)

5) Oversight and Auditing of Network and Application Accounts (Prior Year Observation #4)

6) Data Backup and Restore Procedures (Prior Year Observation #5)

**** END ****