Tailored Technologies LLC

685 Third Avenue
New York, NY 10017

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

Date: January 9, 2014

To: 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, 2013 Audit

---

HUGH L. CAREY BATTERY PARK CITY AUTHORITY
IN CONJUNCTION WITH THE FINANCIAL STATEMENT AUDIT FOR OCTOBER 31, 2013
INFORMATION TECHNOLOGY OBSERVATIONS AND RECOMMENDATIONS

OVERVIEW

On December 16, 2013, Marks Paneth's Tailored Technologies met with Director of IT, Deputy Director of IT, Network Administrator/Technical Unit Manager, and others. 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, 2013. We examined 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 MP 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 35 physical and virtual servers running Microsoft Windows Server 2000, 2003 and 2008. There is one Windows 2003 server at the Regatta and 3 Windows 2003 servers located in Albany backup location. The networks at their main location, the Regatta location, and Albany are protected from intrusion by a pair of SonicWall NAS 4500 clustered firewalls at each location. Symantec's Endpoint Protection version 12 and U.S. Internet Services is used to protect against SPAM. BPCA uses Microsoft's Dynamics GP (Great Plains) version 2010 as their accounting software and Paramount's Workplace version 11 for project accounting and procurement. Sage's ABRA version 9.1 is used as the Human Resources Information System and the ADP Online service is used to process payroll.

The following observations and recommendations are focused primarily on the need improve permissions to Great Plains access accounts, upgrade server and workstation operating systems, document the virtual servers and failover procedures, limit the Management Information Systems (MIS) department's access to financial and operational systems, improve the administration of system passwords, and improve the current data backup solution. Critical software applications which are out of date and no longer supported by the manufacturer are noted as is the lack of a formal ongoing IT Steering Committee. The lack of a comprehensive Business Continuity Plan for key financial and operational systems such as Dynamics GP (Great Plains), Paramount's Workplace application and Sage's Abra is noted and recommendations have been made accordingly.

TABLE OF CONTENTS

Exhibit I – Current Year Recommendations

1) Accounting System Permissions

Observation: 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.

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.

Management's Response: MIS management will review the permissions associated with accounts in Great Plains with the Finance department and will develop permissions that will address the concern raised.

2) Outdated Server Operating System

Observation: Many of BPCA's servers run the Microsoft Windows Server 2003 operating system. Windows Server 2003 is only covered by Microsoft's Extended Support. Under Extended Support, Microsoft support for Windows Server 2003 is limited. In addition, all support from Microsoft for Windows Server 2003 is scheduled to end entirely in July 2015. We were informed that projects plans are being created to ensure all servers are upgraded to Windows Server 2008 or 2012 by the end of 2014.

Recommendation: Management should consider allocating the necessary resources to ensure that all of the BPCA's servers are running an operating system which is covered by Microsoft Mainstream Support.

Management's Response: MIS recognizes the importance of keeping the Operating Systems up to date. MIS will be upgrading all Windows Server 2003 operating systems to either Windows Server 2008 or Windows Server 2012 depending on the compatibility and stability of other applications utilized on the servers. The upgrade is set to be completed by end of fiscal year 2014.

3) Outdated Workstation Operating System

Observation: While all of the workstations in the BPCA office are running the Microsoft Windows 7 operating system, half of the workstations in the Parks Conservancy office run Microsoft Windows XP. Windows XP is only covered by Microsoft's Extended Support. Under Extended Support, Microsoft support for Windows XP is limited and all support is scheduled to end entirely in April 2014. Microsoft has issued security warnings about continuing to run Windows XP after April 2014. The concern is that these unprotected workstations could easily become infected with malware (e.g. viruses, spyware, root kits) and transmit the infection to other workstations on the network.

Recommendation: Management should consider allocating the necessary resources to ensure that all of the BPCA's workstations are running an operating system which is covered by Microsoft Mainstream Support.

Management's Response: MIS recognizes the importance of keeping the Operating Systems covered by Microsoft Mainstream Support. BPCA's Windows XP machines are set to be removed after the upgrade of the dependent application, Opentext. Once Opentext is upgraded, all BPCA workstations will be running Windows 7. This is set to be completed by the end of the 2014 1st fiscal quarter. BPCPC is set to complete the replacements of their current Windows XP machines to Windows 7 by end of the 2014 2nd fiscal quarter.

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

Exhibit II – Prior Year Observations Requiring Further Attention

4) Virtual & Blade Server Documentation (Prior Year Observation #1)

Initial Observation (2011): There is a lack of procedural documentation covering the design and deployment of the virtual server environment and the blade servers at the 24th Floor and Albany locations. We were informed much of the internal BPCA knowledge about the virtual and blade environments was undocumented and not adequately transferred when previous MIS staff left the organization. As of the writing of this report, we had not received documentation we requested covering these two systems.

Initial Recommendation: Management should consider creating detailed design and deployment documentation covering the virtual server environment and the blade server environment. While preparing the documentation, management should consider a worst-case scenario and assume the documentation will be used by people who are technically proficient but who may not have direct knowledge about the organization's operations, networks, and infrastructure. Formal procedures should be created to ensure this critical documentation is reviewed and updated on an ongoing basis.

2013 Status: There has been no change in the status of this comment in the past audit year. We were informed that BPCA has terminated the blade server project referenced in our comment above. The newly hired Director of IT is creating a new project plan to provided disaster recovery capabilities in the Albany location. We continue to recommend BPCA document all redundant and recovery systems and create formal procedures to ensure the documentation is reviewed and updated.

Management's 2013 Response: MIS has documented procedures in the IT Strategic Plan on how the virtual system environment will be built and configured as part of the Windows operating system upgrade project slated to be completed end of the 3rd fiscal 2014 quarter. A formal procedure will be documented as part of the implementation of the new hardware and virtualized system environment.

5) MIS Rights to Financial and Operational Systems (Prior Year Observation #2)

Initial Observation (2010): The members of the MIS staff have full administrative access to the Dynamics GP and Workplace applications, including the ability to add and remove user accounts and modify database records. The Director of IT stated the IT department rarely accesses the Dynamics GP and Workplace applications. They do not have administrative access to the Abra and ADP systems.

2010 Recommendation: Management should consider performing a formal review of the procedures for the MIS Department to access the financial and operational systems. Best practices dictate the MIS Department should not have continual administrative access to these systems and there should be a documented procedure to give temporary access to the MIS Department as required. The management of user access within the financial and operational systems should be the responsibility of the individual

department managers for each system and not the MIS Department. To ensure the management of user accesses and passwords continues smoothly, the MIS Department should document the processes to add, update and remove accesses for each system. If, upon formal review, management concludes the MIS Department should have continual administrative access, then we recommend management create a documented set of formal procedures which detail the processes to follow in order to fully audit the data in the financial and operational systems and the network and application access accounts. The formal process of documenting the procedures will allow management the opportunity to analyze in detail the safeguards that need to be put in place and will provide an explicit checklist and schedule for the internal auditors to follow.

2013 Status: We were informed the MIS staff continues to have full administrative access to the Dynamics GP and Workplace databases and are responsible for setting up and managing user accounts in the Dynamics GP and Workplace applications. We continue to recommend:

- A senior member of the Finance staff should have control of the database access and management of user access accounts consistent with BPCA's established separation of duty controls and oversight.
- MIS continual administrative access to the databases and within the applications should be terminated and formal procedures should be implemented to provide temporary access as required.
- If, upon formal review, management concludes that the MIS staff should have continual administrative access, management should create formal policies and procedures for the full and periodic auditing of IT access and actions within the databases and applications.

Management's 2013 Response: Management has concluded that MIS staff will have continual administrative access to the financial and operational systems. A temporary control has been established to monitor the activities performed by MIS as required during user issue resolutions. The control output is automatically saved on a network drive on a continuing basis and is reviewed as necessary. BPCA is currently in the process of evaluating other forms of controls to address this recommendation.

6) Administrator Password Management (Prior Year Observation #3)

Initial Observation (2010): We were informed that administrator passwords for the network, applications, and network devices are stored in a spreadsheet in the MIS directory on the network file system. The passwords are not stored offsite and senior management is not aware of the administrator login credentials. Best practices for Business Continuity dictate that a copy of the administrative password list is stored off site and management has access to the list.

Initial Recommendation: Management should consider implementing a procedure to maintain both a secure onsite and offsite copy of all network, application, and service login credentials in a secure location. Additionally, select members of senior management should have access to both copies. A secure offsite copy of administrator passwords provides access to this critical information in the event BPCA experiences a disruption to accessing the critical financial and operational software and hardware systems or the main location is not accessible. The procedure should include a process to update the onsite and offsite copies of the administrator passwords synchronized with BPCA's password policy. We recommend if the list of passwords is stored on the network, the list be maintained in a password safe application which uses either AES or Blowfish encryption.

2013 Status: We were informed the network administrative passwords continue to be kept in an encrypted file which is stored on site and off site that senior management knows how to access the file. Consistent with our recommendation in Comment #5, above, we continue to recommend complementary procedures should be established for the storage of administrative passwords to financial and critical operational systems. A member of senior management should know how to access

the application password lists and access to these lists should be consistent with roles, responsibilities, and the data contained in the system.

Management's 2013 Response: MIS recognizes the importance of securing network administrative passwords to financial and critical operational systems. A hardcopy of the administrative passwords in a sealed envelope has been given to senior management. Each person has signed a tracking sheet indicating they have received the sealed envelope and have set it for safe keeping in the event of a disaster. This is indicated in the MIS Policy 2013-2014 on section 6.6 (Administrator Password Management) of page 14.

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

Initial Observation (2010): There are no formal procedures for monitoring and auditing network and application accounts. The MIS staff reviews the security logs intermittently but does not have a proper checklist to audit accounts and access privileges.

Initial Recommendation: Management should consider creating formal policies and procedures to audit network and application access.

We recommend that, at a minimum, the network account audit should:

1. Compare active network accounts against the list of staff, temps, contractors, and consultants who have been approved for access; disable or purge all accounts that should not have access. This is usually handled by the Human Resources Department.
2. Review security logs to determine that all account status transactions match the record of additions and deletions based on the network account review. It should be determined whether any temporary or "ghost" accounts have been created.
3. Review the privilege level of all active accounts; making sure that all accounts have the proper and appropriate privileges.
4. Review remote access logs to determine if there has been any irregular activity.
5. Review server security logs to determine if there has been any irregular activity.

We recommend that, at a minimum, the application account audit should include:

1. Comparing active application accounts against the known list of application users.
2. Reviewing the privilege level of all active accounts to ensure all accounts have the proper and appropriate privileges based on user's responsibilities.
3. Reviewing the security matrix for unused temporary accounts regarding temps, contractors, and consultants who have been approved for access. All accounts that should not have access should be disabled or purged.

2013 Status: We were informed auditing of network access accounts is being performed in accordance with the BPCA MIS Policy which includes requirements for the periodic auditing of network, financial application, and critical operational system access accounts. However, BPCA has not developed formal procedures for the auditing of access accounts to the financial and critical operation systems. We continue to recommend management allocate the recourses necessary to create formal procedures for the formal periodic auditing of financial and critical operational application access accounts.

Management's 2013 Response: MIS recognizes the importance of monitoring and auditing of network accounts. The authority is in the process of establishing procedures which will be used to monitor and audit access accounts to the network and application accounts.

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

Initial Observation (2010): Data is backed up daily to magnetic tape. The daily tapes are transferred twice a week to an offsite repository managed by Iron Mountain. The daily tapes are saved for 4 weeks. A monthly tape is saved for a year, and an annual tape is saved for seven years. While this rotation of tapes is properly documented, the details of what data are backed up and how it is backed up is not documented.

The process of restoring data is undocumented. In addition, there are no formal procedures to test the data restore process on an ongoing basis and to test the viability of tapes in the rotation. While there is a procedure for authorizing the restoration of data it is also undocumented.

Initial Recommendation: Management should consider documenting all backup policies and procedures as well as periodically reviewing these policies to verify the contents and appropriateness of each. This can result in the consolidation of backup jobs and related hardware, leading to potential cost savings. We recommend the documentation include, at minimum:

1. A description of the data retention requirements for both short term operational needs and the long term compliance requirements.
2. A full description of each backup job including the intended scope of the job, the server, the drive, the directory structure and to which storage device the backup is directed.
3. A description of the configuration and schedule for each backup job including the automated status notifications to be delivered to the designated MIS staff.

Management should also consider re-evaluating BPCA's current data tape backup solution. Data tape backups are becoming increasingly obsolete as other more reliant data backup solutions have become less costly. Additionally, compared to new data backup technologies, tapes are not as reliable, are not as durable, are slower, have a smaller data capacity, require continual replacement, require more administration and require human intervention to load and rotate the tapes. We recommend the following potential data backup options, as costs allow:

1. Deploy a Storage Area Network (SAN) backup solution with versioning technology at the One World Financial Center and the Albany locations. The devices should be configured to copy the data from One World Financial Center to Albany so each site has a complete copy of the data. (We were informed the MIS Department is addressing this by creating a failover site in Albany where data will be replicated from One World Financial Center. This project is scheduled to complete the first quarter of 2011.)
2. An Internet based backup solution that will backup network data to an Internet based on-line service in a secure fashion. This option provides for additional contingency and disaster recovery planning options. We recommend this solution in combination with either the existing tape backup or SAN solution. Providers include, but are not limited to:
    i. Iron Mountain (http://ironmountain.com/dataprotection)
    ii. Seagate's i365 (http://www.i365.com/data-backups/index.html)
    iii. AmeriVault's VenYu (http://www.venyu.com/)
3. If the use tape based backup is continued, we recommend the following:
    i. Securely store all onsite and offsite tapes in data rated fireproof safes.
    ii. Replace the actual data tapes at least every 6-9 months.
    iii. Clean the recording heads on the tape drives according to the drive manufacturer's maintenance recommendations.
4. The backup policy should include a procedure to perform test restores on the tape media on a regular basis. Implementation of a policy to perform test restores on a periodic basis ensures the backup media is in good condition, the intended data is being backed up, and the restored data is correct and not corrupted.
5. The backup policy should include the procedures detailing who is authorized to request a data restore and what data they are authorized to request. Special consideration should be given to the procedures for requesting the restoration of financial or confidential information.

2013 Status: There has been no change in the status of this comment in the past audit year. We continue to recommend management allocate the resources necessary to ensure:

- Magnetic tapes are replaced as the primary media for daily data backups.
- A copy of the backed up data is taken off site daily and senior management has authorized access to all data backups.
- There is full documentation of data being backed up which is reviewed periodically by management to ensure all critical data is backed up and the Data Retention Policy is followed.
- Formal data test restore policies and procedures are implemented.

Management's 2013 Response: MIS is currently investigating switching backups from tapes to hard drives formats or Internet backup solutions. Backup tapes are already actively rotated offsite for storage and senior management has authorized access to backups. Documentation on all tape backup sessions (job name, server, drives, folders, files, target source, date and time) are currently maintained on the backup system. On a quarterly basis, management reviews the tape backup procedures. A formal data test restore is also performed and on a quarterly basis. This is indicated in the MIS Policy 2013-2014 on section 8.1 and 8.2 (Backup and Restore, respectively) of page 20.

9) Critical Applications Versions (Prior Year Observation #6)

Initial Observation (2010): We understand some critical applications are out of date. The Dynamics GP version 9 is no longer supported by Microsoft as of January 11, 2011. While management is already aware of this we understand the current Dynamics GP vendor is capable of supporting the current version on a time and material basis. Both Crystal Reports, used for financial reporting, and Sage's Abra human resources system are two full versions behind. The concern is if there are problems with these applications, resources would be either limited or unavailable to help mitigate any issues. Best practices dictate the core financial and operational systems of an organization be hosted on the software manufacturer's currently supported version.

Initial Recommendation: Management should consider immediately beginning the process to either select new systems or upgrade the current applications given their criticality. We recommend BPCA pursue a formal software selection process to ensure the new applications will meet the current and future needs of the organization.

2013 Status: While Sage's ABRA was upgraded at the end of the 2011 audit year and Microsoft Dynamics GP was upgraded to version 2010 in May 2012, important components of the financial management and reporting software system remain out of date and or unsupported. Crystal Reports 11 is hosted on a server running Microsoft Windows 2000, and operating system which Microsoft no longer supports and the sole developer for the DLOC inventory system is no longer available. We were also informed the Microsoft FRx reporting system has not been fully integrated with the upgraded Dynamics GP 2010. We continue to recommend management allocate the resources necessary to bring all components of the financial management and reporting systems up to date.

Management's 2013 Response: MIS recognizes the importance of keeping critical systems up to date. Crystal Reports is set to move to Windows Server 2012 as part of the project to upgrade of all the server operating systems which is slated to be complete at the end of fiscal 2014. FRx is set to be upgraded to Microsoft Management Reporter in the end of the 2014 3rd fiscal quarter. Even though the sole developer is no longer available for DLOC, they have other developers for the DLOC application within the company. These developers recently performed work in the upgrade to the DLOCs application for BPCPC.

10) Steering Committee (Prior Year Observation #7)

Initial Observation (2010): We were informed that while there is an IT Steering Committee at BPCA it has not been convened for at least 6 months. We were told that this Steering Committee used to meet at least once a quarter.

Initial Recommendation: Management should consider scheduling these meetings on a rotation consistent with the technology needs of BPCA. We recommend these meetings be held at least every 6 months to review and approve IT plans and priorities as well as assess and address risks related to technology deployed throughout the organization.

2013 Status: We were informed there has been no change in the status of this comment in the past audit year. We continue to recommend a formal IT Steering Committee, with members from all major operational groups, meet at least every 6 months to review and approve IT plans and priorities as well as assess and address risks related to technology deployed.

Management's 2013 Response: MIS recognizes the importance of the IT Steering Committee meetings. BPCA has held 2 formal IT Steering Committee meetings. The 1st formal IT Steering Committee meeting was held on September 26 at 2:30pm and the 2nd formal IT Steering Committee was held on December 19 at 2:30pm. MIS will continue to hold the IT Steering Committee meetings on a quarterly basis. Information about IT plans and departmental plans were discussed during these meetings. This is indicated in the MIS Policy 2013-2014 on section 2.8 (IT Steering Committee) of page 6. MIS expects to have this issue removed from the next year's audit.

11) Disaster Recovery Planning (Prior Year Observation #8)

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.

2013 Status: There has been no change in the status of this comment in the past audit year. We continue to recommend BPCA conduct a Business Impact Analysis and develop a full Business Continuity Plan. There are a number of Business Continuity and Disaster Recovery Planning template guides, including those produced by government agencies, to guide the process. Providers of template guides include, but are not limited to:

- Janco – http://e-janco.com/DRP.htm
- Info-Tech – http://www.infotech.com/research/disaster-recovery-plan-template

Management's 2013 Response: MIS recognizes the importance of disaster recovery plan. BPCA management will conduct a full business continuity plan in reference to the MIS disaster recovery/business continuity project plan as indicated in the IT Strategic Plan slated for completion at the end of 2014 fiscal year.

**** END ****