Tailored Technologies LLC

622 Third Avenue
Seventh Floor
New York, NY 10017

Tel: (212) 503-6300
Fax: (212) 986-2461

Date: January 26, 2012

To: The Audit File of

From: Tailored Technologies LLC

Technology Observations and Recommendations Resulting From the October 31, 2011 Audit

---

HUGH L. CAREY BATTERY PARK CITY AUTHORITY
IN CONJUNCTION WITH THE FINANCIAL STATEMENT AUDIT FOR OCTOBER 31, 2011
INFORMATION TECHNOLOGY OBSERVATIONS AND RECOMMENDATIONS

OVERVIEW

In January 2012, Marks Paneth & Shron's Tailored Technologies met with Neresa Gordon, Network Administrator/Technical Unit Manager and Aijaz Khan, User Support Specialist. 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, 2011. We examined the controls within the Information Technology (IT) infrastructure and collected and evaluated evidence of BPCA's information systems, practices, and operations to ensure the optimal use of automation and reliance on computer controls for an effective and efficient audit process that eliminates the need for many time consuming manual audit procedures by effectively utilizing information system reliance. In addition, through our IT information gathering, we obtained evidence to determine that the information systems are safeguarding assets, maintaining data integrity, and operating effectively and efficiently to contribute to BPCA's goals and objectives.

BPCA has 21 servers running Windows Server 2000, 2003, and 2008 and an additional 16 virtual servers. The networks at their main location, the Regatta location, and the Albany backup location are each protected from intrusion by a pair of SonicWall NAS 4500 clustered firewalls. Symantec's Endpoint Protection version 11 and US Internet Services is used to protect against SPAM. BPCA uses Microsoft's Dynamics GP (Great Plains) version 9 as their accounting software and Paramount's Workplace version 10 for project accounting and procurement. Sage's Abra version 9 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 to document the virtual servers, document failover procedures, limit the Management Information Systems (MIS) department's access to financial and operational systems, improve MIS's approach to system's monitoring, improve the administration of system passwords, and improve the current data backup solution. Critical software applications which are out of date and, in some cases, no longer supported by the manufacturer are noted. 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) Virtual & Blade Server Documentation

Observation: 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.

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.

Management's Response: BPCA has Virtual and Blade server procedural documentation completed. See attached.

2) Internet Redundancy Documentation

Observation: There is a lack of procedural documentation covering the failover of Internet connectivity between the 24th Floor and Regatta locations. We were informed there are three 10 MB connections installed. One connects the 24th Floor to the Internet, a second connects the 24th Floor to the Regatta location, and the third connects Regatta to the Internet. While the same vendor provides the Internet connections from the 24th Floor and Regatta, the lines terminate in different central office locations which are a best practice. We were also informed the lines are supposed to be configured so that if one of the Internet connections fail, both sites can use the remaining connections. (For instance, if the connection to the 24th Floor fails, the router should direct Internet traffic to the connecting line to Regatta and from there out to the Internet over the Regatta's connection.) There is a fourth connection at Regatta provided by Time Warner Cable which is used for the security camera system but which could also provide a failover Internet connection if required. However, the Time Warner failover would require manual intervention and configuration. None of these configurations are documented. There is uncertainty whether the configurations have been properly deployed and what steps, if any, must be taken in the event of a failure. In addition, periodic testing of the failover procedures has not been performed.

Recommendation: Management should consider creating formal detailed documentation of the Internet connections, all failover configurations, and all procedures, particularly manual ones, necessary to ensure a smooth failover and a smooth failback in the event of a disruption of an Internet connection. Periodically connections should be purposely disrupted to test the failover configurations and staff training.

Management's Response: Verizon reconfigured the router at the Regatta which includes a new IP address and BGP capabilities. 24th Floor router has been updated with the new IP address of the Regatta and BPG configuration was verified in order to provide a seamless failover. BPCA recently did a test failover in collaboration with Verizon to make sure updated configuration is working properly.

Attached is the procedural documentation.

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

Exhibit II – Prior Year Observations Requiring Further Attention

3) MIS Rights to Financial and Operational Systems (Prior Year Observation #1)

Observation: 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. Stan Molinski 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.

Management's 2010 Response: BPCA agrees with this recommendation. Management will undertake a full review of the current practices in the MIS Department regarding access to the Authority's financial and operational systems to identify weaknesses and/or deficiencies. In response to the immediate concern regarding the MIS Department's "virtual administrative access" capability, BPCA will implement procedural safeguards to control access to the Authority's financial and administrative systems. Initial steps will include establishment of time and user access restrictions through individual instruction, written procedures, or other appropriate measures.

2011 Status: There has been no change in status for this comment in the 2011 audit year. We were informed MIS staff members' rights remain the same and no additional control procedures have been implemented. We were also informed the MIS Coordinator for the Battery Park City Park Conservancy (BPCPC) has full access to the Human Resources database maintained by BPCPC. We continue to recommend management either rescind the administrative privileges for the MIS staff to all financial and critical operational systems or create documented audit and oversight procedures.

Management's 2011 Response: With the new upgrade of our Financial Systems, completed the week of May 7th, MIS no longer has admin access to the Financial Systems. Finance department has the ability to change their own passwords. Financial Applications especially GP and Workplace force the user to change the password for security purposes which allows Finance to manage their passwords while the MIS dept. has only temporary access to the systems as required. BPCA believes that if continual administrative access to these systems were to lie solely with the Finance Department with no ability to audit access or template overrides it would constitute an internal control violation.

Access procedures for both Finance and MIS have been created which will allow for the data in the financial and operational systems and the network application access accounts to be audited. We are in the process of documenting the new upgrade as well.

Additionally, management has confirmed that the MIS coordinator in BPCPC (Parks Conservancy) does not have any access to the HR database.

4) Administrator Password Management (Prior Year Observation #2)

Observation: 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.

2010 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.

Management's 2010 Response: BPCA agrees with this recommendation. BPCA has now begun to encrypt the passwords onsite. As to offsite storage of passwords, BPCA currently stores and has always stored its passwords offsite in a secure location. However, those passwords are not immediately retrievable. BPCA will now have access to the passwords in real time. In addition to the Director of IT, the President & CEO, the Executive Vice President/Chief Administrative Officer will have copies of the passwords.

2011 Status: We were informed only MIS staff has access to a list of administrative passwords and a copy of the list is not kept offsite. We continue to recommend management implement a documented procedure to maintain a full list of all administrator passwords in one location. The procedure should address:

1. What should be stored on the list, such as the Administrator passwords for network, critical network devices (e.g. firewalls, routers), encryption keys, and Internet record keepers (e.g. domain name registrar(s), MX record holder).
2. Provisions for maintaining separate lists for passwords to financial and critical operational systems.
3. How to store the lists (e.g. paper, digital). If a list is printed out, it should be stored in a sealed envelope in a fire rated safe. Digital copies should be encrypted using a 256-bit encryption key.
4. Where to store a list. At a minimum, one copy should be stored onsite and another copy stored offsite so the passwords are available in the event the main office is inaccessible.
5. Requirements to keep the lists up to date.

In addition, designated members of senior management should be provided directions on how to access these password lists in the event of an emergency. The procedures should include:

1. Who in senior management should know how to access the network password list. Access to the list should be consistent with roles, responsibilities, and network resources available.
2. Who in senior management should know how to access to the application password lists. Access to these lists should be consistent with roles, responsibilities, and the data contained in the system.

Management's 2011 Response: Management agrees with this recommendation. BPCA always stored its passwords offsite in a secure location; however, BPCA also now has access to the offsite passwords

in real time through the BPCA FTP site. The passwords have also been encrypted onsite as well as off-site with Sophos-Utimaco Safeguard Private Crypto file. BPCA's President/CEO and Executive VP/CAO/General Counsel have access to both copies of passwords.

5) Oversight and Auditing of Network and Application Accounts (Prior Year Observation #3)

Observation: 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.

2010 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.

Management's 2010 Response: BPCA agrees with this recommendation. BPCA will implement the recommendation and will draft procedures consistent with the recommendation.

2011 Status: BPCA's *Management Information System Policy* was updated to include Section 7.15 which covers monthly audits of network and Dynamic GP user accounts. However, we were informed only informal network account auditing was being performed. Formal, periodic account auditing as outline in Section 7.5 is not being performed. We continue to recommend account auditing as outlined in Section 7.5 for all financial and critical operational systems, also including Sage ABRA, Paramount's Workplace, and the BPCPC Human Resources database, be performed.

Management's 2011 Response: Management agrees with this recommendation. A formal audit of the network was performed after 19 staff left in an effort to ensure all access was disabled to the network and to deactivate access to all financial applications. Ongoing monitoring will now take place monthly and a checklist has been created in the network drive. See below.

6) Systems Monitoring (Prior Year Observation #4)

Observation: We were informed the MIS Department does not take a proactive approach to monitoring and auditing the hardware and software environment at BPCA. The server inventory documentation is created manually and inventory documentation does not exist for the workstations. This can potentially lead to additional IT costs as well as potential business disruptions.

2010 Recommendation: Management should consider directing the MIS Department to take a more proactive approach towards monitoring and documenting the IT environment. The MIS Department could utilize the asset and change tracking modules of the existing Track-IT help desk application to monitor and audit the hardware and systems on the network. Other alternatives include, but are not limited to:

1. Lansweeper Pro (http://www.lansweeper.com)
2. Belarc Belmanage (http://www.belarc.com)

Management's 2010 Response: BPCA agrees with this recommendation. BPCA currently has several software packages which have been implemented to a limited degree, including "TrackIT" and the GP "fixed assets" module. BPCA management is assessing the recommended software including its budget impact. Staff will submit several options to the IT Steering Committee for consideration.

2011 Status: We were informed an appliance for network monitoring was purchased by the former Director of IT. However, MIS staff is not using it or any other application to actively monitor the BPCA network. We continue to recommend a more proactive approach to monitoring and documenting the IT environment.

Management's 2011 Response: BPCA does not agree with this finding.

BPCA network is actively monitored through penetration by MS-ISAC NYS Cyber Security every 3rd Wednesday of the month through Qualys Guard Enterprise Security suite. Please find attached the Jan 2012 monthly report as well as our access to the application.

BPCA also has "IP Switch What's up Gold" which is a network management and monitoring solution which is also used for monitoring and was in place prior to the audit. MIS always had alert turned on each system so that whenever there is a system issue an email alert is sent to MIS staff. Attached is the report of 'IP Switch.'

BPCA did not purchase a network monitor appliance. The office of Managed Security Services (MSS) NYS Cyber security provided a Dell PER610 server through a federal grant. The Dell PER610 server was returned to make it available to another State agency as the equipment was duplicating the current monitoring provided by the NYS Cyber Security.

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

Observation: 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.

2010 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.

Management's 2010 Response: BPCA agrees full review of with this recommendation. Management will begin a full review of existing back-up policies and procedures, including relevant documentation. As part of that review, staff will assess the current data tape back-up solution and suggest more up to date solutions to the IT Steering Committee for consideration.

2011 Status: There has been no change in the status of this comment in the 2011 audit year. We continue to recommend BPCA increase the frequency backups are taken off site, eliminate magnetic tapes as the primary backup media, and fully document all backup procedures.

Management's 2011 Response: Management agrees with this recommendation. BPCA will increase the frequency of the backups taken offsite and has talked to our present provider, Iron Mountain, about providing online Backup. BPCA is also analyzing additional storage solutions including an 'Exagrid Disk" based backup system as well as Cloud Computing.

Our current procedure is attached.

8) Critical Applications Versions (Prior Year Observation #7)

Observation: 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.

2010 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.

Management's 2010 Response: BPCA agrees with this recommendation. The upgrade of Microsoft Dynamics was budgeted for in Fiscal Year 2011 and an RFP will be issued in March. This GP upgrade RFP will also include updates for Crystal and FRX reports. An upgrade for Sage's Abra was completed two weeks ago.

2011 Status: We were informed Sage's ABRA was upgraded at the end of the 2011 audit year and Microsoft Dynamics GP 2010 is scheduled to go live in March 2012. Management should continue to support the Dynamics GP upgrade given the lack of software manufacturer support for the currently installed version.

Management's 2011 Response: Financial Applications have been upgraded and completed and went live on May 7th 2012.

9) Steering Committee (Prior Year Observation #8)

Observation: 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.

2010 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.

Management's 2010 Response: BPCA agrees with this recommendation. The IT Steering Committee has met twice in response to the IT audit and will be meeting regularly to update the MIS policies as well as work on a Business Impact Analysis for the entire organization (both BPCA and the BPCPC) as the first step to a global Business Continuity plan.

2011 Status: We were informed an IT working group convened on an as-needed basis to oversee the upgrade of Microsoft Dynamics GP from version 9 to version 2010. 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 2011 Response: BPCA has a formal IT steering Committee which convened on regular basis during FY 2011. Please see attached PDF.

10) Disaster Recovery Planning (Prior Year Observation #9)

Observation: 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.

2010 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.

Management's 2010 Response: BPCA agrees with this recommendation. The IT Steering Committee will conduct a Business Impact Analysis as a first step in developing a comprehensive Business Continuity Plan. In the interim, completion of the mirrored environment in Albany will continue in order to ensure that remote back-up and fail-over systems are in place while a more comprehensive plan is developed.

2011 Status: There has been no change in the status of this comment in the 2011 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 Response: Management agrees with this recommendation. Completion of the mirrored environment in Albany was completed. However, a more comprehensive plan is required.

**** END OF REPEAT COMMENTS ****

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

11) Redundant Communications Infrastructure (Prior Year Observation #6)

**** END ****