Tailored Technologies LLC

685 Third Avenue
New York, NY 10017

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

Date: January 15, 2015

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, 2014 Audit

---

HUGH L. CAREY BATTERY PARK CITY AUTHORITY
IN CONJUNCTION WITH THE FINANCIAL STATEMENT AUDIT FOR OCTOBER 31, 2014
INFORMATION TECHNOLOGY OBSERVATIONS AND RECOMMENDATIONS

OVERVIEW

On January 14, 2015, Marks Paneth's Tailored Technologies met with Robert Serpico, Chief Financial Officer, Karl Koenig, Controller, Daniel Curiale, Director Financial Reporting, John Tam, Director of IT, Neresa Gordon, Network Administrator/Technical Unit Manager, Siu Ng, Senior Programmer Analyst, and Benjamin Jones, VP of Administration. 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, 2014. 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 20 physical and virtual servers running Microsoft Windows Server 2003, 2008, or 2012 or VMWare ESXi 5.5. There is one Windows 2003 server at the Regatta and 2 Windows 2003 servers located at the Battery Park City Parks Conservancy ("BPCPC") office. The networks at their main location, the Regatta location, and BPCPC are protected from intrusion by a pair of SonicWall NAS 4500 clustered firewalls at each location. BPCA has decommissioned the servers previously deployed in Albany NY. 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 operating systems, 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. 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.

A central component of our IT audit procedures is to review the cyber security defenses deployed to protect the organization's information and infrastructure. Specific cyber security concerns we have identified are the need to improve permissions to Great Plains access accounts, limit the Management Information Systems (MIS) department's access to financial and operational systems, improve the current data backup solution, and create a comprehensive Business Continuity 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.

2014 Status: We reviewed the security permissions of user accounts within the Microsoft Dynamics GP application. While improvements have been made 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". We continue to recommend BPCA review the permissions assigned to each user account and restrict user permissions based on their roles, responsibilities, and segregation of duties.

An additional concern relates to the permissions granted to the Chief Financial Officer's access account. We were informed the Chief Financial Officer does not perform 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 2014 Response: MIS continues to recognize the importance of security controls on permission of user accounts. Further evaluation of BPCA_FIN1 and BPCPC_FIN1 groups will be conducted for identify tighter controls that can be implemented. In addition, the Chief Financial Officer will have read-only access as recommended.

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

Observation (2013): 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.

Initial 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.

2014 Status: We were provided documentation indicating many of the BPCA servers run either the Microsoft Windows Server 2008 or Server 2012 operating system. Both operating systems are covered by Microsoft Mainstream Support. We were informed the remaining servers running the Server 2003 operating system will be upgraded by the July 2015 deadline.

Management's 2014 Response: MIS continues to recognize the importance of keeping our system updated. MIS agrees to decommission Server 2003 by July 2015.

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

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.

Initial 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.

2014 Status: The MIS staff continues to have full administrative access to the Dynamics GP and Workplace applications and databases. We were informed BPCA has recently deployed FastPath's Audit Trail to monitor and track access activities within Dynamics GP and is formalizing oversight review procedures between the Financial and IT departments. We continue to recommend management remove IT administrative access rights within the financial systems or create formal policies and procedures for oversight of IT administrative access in addition to deployment of the FastPath's Audit Trail.

Control: Best practices dictate removing IT administrative access within the financial and operational systems. Our recommendations include:

1. Management of user access within the financial systems should be performed by the business process owner, such as the Chief Financial Officer or designate. The Director of IT or designate should document the processes to add, update, and remove accesses to ensure that the management of user accesses and passwords continues smoothly.
2. A documented procedure for the business process owner or designate to give temporary access to the IT department only as required. All IT access events within the financial and operational systems should be logged in a central ticketing system. Each log entry should indicate the reason for accessing the system.

3. Procedures for the business process owner or designate to confirm that no unauthorized changes were made during access by the IT department.
4. The Director of IT or designate and the business process owner or designate should together periodically review the records in the ticketing system, the access audit report generated by the system, and the FastPath audit reports. If there are discrepancies between the tickets and the audit logs such as an access event without a supporting ticket, the event should be researched and resolved to ensure IT is accessing the system for required purposes only.
5. Procedures to ensure that all development work and report writing is performed in a separate non-production environment. Once tested and accepted by the business process owner, IT is provided temporary access to upload the approved changes to the production environment.
6. Procedures for IT to create "scripts" to transfer production data to the development environment to be run by the business process owner. Along with transferring data from production to development, the script should randomize sensitive data such as social security numbers.

Oversight: In the event management concludes operational effectiveness requires IT to maintain administrative access to any or all of the financial systems, policies and procedures should be created for the oversight of IT access and activities within the systems. Our recommendations include:

1. Management should identify the business process owner for the financial systems, such as the Chief Financial Officer or designate.
2. The business process owner or designate should also have full administrative access to the system as a way to distribute control and mitigate risk.
3. All IT access events within the financial and operational systems should be logged in a central ticketing system. Each log entry should indicate the reason for accessing the system.
4. The Director of IT or designate and the business process owner or designate should together periodically review the records in the ticketing system, the access audit report generated by the system under review, and the FastPath audit reports. If there are discrepancies between the tickets and the audit logs such as an access event without a supporting ticket, the event should be researched and resolved to ensure IT is accessing the system for required purposes only.
5. Procedures for the business process owner or designate to confirm that no unauthorized changes were made during access by the IT department.
6. Procedures to ensure that all development work and report writing is performed in a separate non-production environment. Once tested and accepted by the business process owner, IT is provided temporary access to upload the approved changes to the production environment.
7. Procedures for IT to create "scripts" to transfer production data to the development environment to be run by the business process owner. Along with transferring data from production to development, the script should randomize sensitive data such as social security numbers.

Management's 2014 Response: MIS recognizes the importance of securing access to the financial systems. We agree to the controls and oversights as indicated above. Formal procedures are expected to be generated and documented by end of 2nd Fiscal Qtr.

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

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.

2014 Status: 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 2014 Response: Formal procedures on periodic auditing of network and application accounts will be established by July 2015. MIS currently uses their ticketing system, Track-IT, to auto-generate and monitor tickets for auditing of accounts. Further controls will be set in place with the various departments to solidify the auditing processes of network and application accounts.

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

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.

2014 Status: While there has been no change in the status of this comment in the past audit year, we were informed BPCA is currently deploying redundant servers in the BPCPC office to improve data backup procedures and improve disaster recovery capabilities. Servers in the BPCA office will replicate at least daily with the servers in the BPCPC office ensuring both sites have a full copy of all data generated by BPCA and BPCPC. In addition, the servers will be replicated daily to an online service to provide both redundant data backup and disaster recovery capabilities. This project is scheduled to be completed by mid-2015.

Management's 2014 Response: MIS agrees that the implementation of the disaster recovery capabilities underway will significantly improve the backup procedures for both BPCA and BPCP. We agree that this project will be completed mid-2015.

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

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.

2014 Status: While there has been no change in the status of this comment in the past audit year, the deployment of IT disaster recovery capabilities is in progress. The servers at the BPCA office will be replicated daily to an online service providing BPCA the ability to access business critical applications and data remotely in the event of an emergency. This project is scheduled to be completed mid-2015. In addition, we were informed business continuity planning for the entire organization is in progress and actionable plans and documentation are scheduled to be completed by the end of 2015.

Management's 2014 Response: MIS continues to recognize the importance of disaster recovery and is scheduled to have a system implemented by the end of 2015 for both BPCA and BPCP.

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

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

7) **Outdated Workstation Operating System (Prior Year Observation #3)**

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

9) **Administrator Password Management (Prior Year Observation #6)**

10) **Critical Applications Versions (Prior Year Observation #9)**

11) **Steering Committee (Prior Year Observation #10)**

**** END ****