HUGH L. CAREY
BATTERY PARK
CITY AUTHORITY

MIS 2011 Audit items

In January 2011, Tailored Technologies LLC ("TT"), acting on behalf of Marks Paneth & Shron LLP completed an Information Technology ("IT") audit of Battery Park City Authority's ("BPCA") management information systems ("MIS") in conjunction with the fiscal year 2010 audit of the financial statements. TT examined the controls within the IT infrastructure and collected and evaluated 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. The following are TT's recommendations and BPCA's responses.

1) MIS Rights to Financial and Operational Systems

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

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 that the management of user access and passwords continues smoothly, the MIS Department should document the processes to add, update and remove access 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 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.**

2) Administrator Password Management

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 should be stored off-site and management has access to the list.

Recommendation: Management should consider implementing a procedure to maintain both a secure onsite and off-site 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 off-site 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 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.**

3) Oversight and Auditing of Network and Application Accounts

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.

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 Response: **BPCA agrees with this recommendation. BPCA will implement the recommendation and will draft procedures consistent with the recommendation.**

4) Systems Monitoring

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.

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 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.**

5) Data Backup and Restore Procedures

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.

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 Response: **BPCA agrees 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.**

6) Redundant Communications Infrastructure

Observation: There is a lack of redundancy in the data communications infrastructure as well as a lack of documentation. The One World Financial Center, Regatta, and Albany locations only have a single router and firewall device installed. There are key connections between One World Financial Center and Regatta and between One World Financial Center and Albany that do not have backup or failover devices in place.

Recommendation: Management should consider, given the importance of Internet connectivity to business continuity planning, having on-hand an extra preconfigured and updated firewall and router at each site to be used in the event the existing hardware fails. This will enable a quicker recovery from firewall or router hardware failure. As the Albany site becomes operational, consider reviewing the data connections between all sites and modifying as necessary. Consider provisioning a redundant, auto-failover connection between the One World Financial Center, Regatta, and Albany sites.

Management's Response: **BPCA agrees with this recommendation. Staff will assess the existing infrastructure and cost impact of this recommendation to ensure sound auto failover connections.**

7) Critical Applications Versions

Observation: We understand some critical applications are out of date. The Microsoft Dynamics version 9 is no longer supported by Microsoft as of January 11, 2011. While management is already aware of this we understand the current Microsoft 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.

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

8) Steering Committee

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.

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 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.**

9) Disaster Recovery Planning

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 Microsoft Dynamics GP, 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.

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 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.**