Marks Paneth LLP
685 Third Avenue
New York, NY 10017
P 212.503.8800
F 212.370.3759
markspaneth.com

MARKS PANETH
ACCOUNTANTS & ADVISORS

Date: January 30th, 2021

To: The File of the Hugh L. Carey Battery Park City Authority

From: Marks Paneth Information Technology Audit

Technology Observations and Recommendations Resulting from the October 31, 2021, Audit

---

Marks Paneth LLP has issued a management letter under AU-C Section 265 indicating we did not observe any material weaknesses. The memo below represents our observations that are either minor in nature or represent best practices pertaining to technology. Matters in this memo are as of the date of this letter. If matters should arise between this date and the date of Marks Paneth LLP's audit report on the financial statements, we will update this memo.

Exhibit I of this memo pertains to any new findings that were identified during our work in connection with Hugh L. Carey Battery Park City Authority's (BPCA) financial statement audit for the year ended October 31, 2021. Based upon our understanding of BPCA's IT General Controls which included a review of logical security, program change control, and system recovery and availability as well as obtaining information about Cyber Security controls and practices, 4 new recommendations were presented.

Exhibit II pertains to prior year recommendations that, based on our current procedures, appear to require further attention by management. Exhibit III pertains to the prior year recommendations that based upon current procedures, does not appear to require further attention by management.

It should be noted that we will review management's current year responses during Marks Paneth LLP's next audit cycle.

Table of Contents

Page

OVERVIEW 2

CYBERSECURITY 3

Exhibit I – Current Year Recommendations 5

Exhibit II – Prior Year Recommendations Requiring Further Action 6

Exhibit III – Prior Year Recommendations That Do Not Appear to Require Further Action 7

Morison KSi
Independent member

OVERVIEW

During the course of our review Marks Paneth LLP's audit team met with the following individuals:

1. Jason Rachnowitz, Director of Financial Reporting
2. Rodolfo 'Rudy' Machuca, Director of Technology
3. Robert Quon, Deputy Director of IT

Currently, BPCA's Microsoft Windows Servers are running on versions 2012 and 2016 and workstations have been upgraded to Windows10. BPCA uses the following business applications:

1. Microsoft's Dynamics GP (Great Plains) as its accounting software which was recently upgraded.
2. Paramount's WorkPlace for project accounting and procurement which was also recently upgraded.
3. ADP's SaaS-based (Software as a Service) iPayStatements and E-TIME for payroll processing and time and attendance tracking, respectively.
4. Microsoft's SaaS-based Office 365 SharePoint application for document management.

CYBERSECURITY

We also considered BPCA's Cyber Security protections and its ability to detect and prevent unauthorized internal and external access to BPCA's network, including review of policies and procedures in place to ensure secure processes are maintained. The review of Cyber Security Protections was focused on obtaining an understanding of the risk assessment and risk mitigation practices deployed at BPCA and did not include vulnerability scanning of network and penetration testing.

As a method for review, Marks Paneth referred to the NIST Cyber Security Framework which breaks down the assessment to following categories:

- Identify: *Is there a developed organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities*
- Protect: *Are there developed and implemented appropriate safeguards to ensure delivery of critical infrastructure services*
- Detect: *Are there developed and implemented activities to identify the occurrence of a cybersecurity event*
- Respond: *Are there developed and implemented activities to take action regarding a detected cybersecurity event*
- Recover: *Is there developed and implemented activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event*

Identify:

Organizational Cyber Security Policy is established and communicated throughout the organization with the intent to meet organizational goals which identify, measure, and control risk to BPCA's information systems.

BPCA utilizes an inventorying system to record and maintain IT assets so that it can properly manage and address both security risk as well as for provisioning in the event that disaster recovery is activated. This practice enables BPCA to be able to consistently apply security controls across the organization for existing and newly acquired IT equipment.

Protect: (Identify Access Management, Authentication and Access Control)

BPCA has processes in place for how Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes to govern access control so that users may be granted access to information systems that commensurate with their job responsibilities.

As defined in the MIS handbook and corroborated through interviews, the process to provision and deprovision users is initiated by Human Resources in the ticketing system. Network and application access are assigned once proper approvals are obtained. Within Great Plains, there are audit trails that exist to evidence any changes to the status of a user. Only a quarterly basis, recertification of accounts is performed by reconciling to active Human Resource employee listings. There are also policies and procedures around the access of the "Administrator" accounts on the system. Lastly there are policies and procedures for how termination of both MIS and non-MIS users is to be addressed.

The MIS handbook defines policy and procedure around Password Management for both users and "power" users of the system.

There are session management controls in place to mitigate risk of unauthorized access to an unattended terminal or workstation.

Detect:

There are various detection tools in place to monitor for and detect any unusual security patterns, events, and anomalies supporting the 200 Liberty Street office. Additionally, all other BPCA location networks have been adequately upgraded.

The following tools are currently utilized:

- Verizon manages BPCA's network, including addressing and monitoring firewalls and internet traffic.
- CISCO network switch to isolate network traffic to data and voice VLAN for all computers and phones at BPCA office.
- Fortinet and SonicWall firewalls limit the network traffic to and from the computers at BPCA office and the Internet.
- Symantec Endpoint Protection malware and antivirus software.
- Spam filters to log and evaluate any unusual patterns.
- Monthly vulnerability scans.
- Cyber Awareness training through phishing and spoofing tests to end users; and
- BYOD protection with the VMware's AirWatch Mobile Device Management (MDM) platform, which includes the ability to delete ("wipe") data on the mobile devices.

On an annual basis, there is Cyber Training embedded within required employee training.

Respond:

Verizon monitors the activity on the BPCA network and as such would be responsible to invoke Incident Response Procedures should unusual activity be detected. There are defined policies and procedures for communication and notification to BPCA.

Recover:

Defined backup and restore procedures as well as a formal and tested Disaster Recovery Plan exists for BPCA.

Cyber Insurance:

We were also informed that BPCA has purchased cyber insurance to mitigate losses from a variety of potential cyber incidents, including data breaches, business interruption, and network damage. As a best practice, we recommend that BPCA's Audit Committee, Legal or other appropriate Board Committee members, review the summary of policy provisions to confirm coverage and ensure all necessary precautions for BPCA's business is addressed.

Exhibit I – Current Year Recommendations

Observation 1: We noted that a network penetration test was not performed in FY21. Such a study identifies weaknesses within the technology environment and categorizes risks into 'high', 'medium' and 'low. At a minimum, management should consider performing an informal risk assessment of IT functions at least annually to help identify potential risks to critical systems, IT infrastructure, and the achievement of business objectives. Formal documentation of such a review should be retained by IT.

Managements FY21 Response: A penetration test of our environment was conducted in FY21 (November 2020) by the Authority's internal audit, Crowe. Since that testing, we have implemented a Phishing Alert software package, as well as educated our team members on how to recognize suspicious email messages. We have also given them the capability to mark messages as potential phishing email messages and the MIS department then investigates and clears the message if it is deemed safe. Additionally, we have conducted several training sessions on cybersecurity issues that can affect our environment.

Observation 2: We were unable to obtain evidence of management reviewing the user control considerations listed within associated vendor SOC reports.

We recommend that management obtain and review the SOC reports annually to ensure that the controls tested in the report are operating and designed effectively. As the Organization relies on the vendor for change management procedures, management should carefully consider the potential effects this may have on the application's overall stability and availability. All SOC reports should be maintained for future reference and audit necessities. Evidence of a review of the report should be formalized and retained.

Management FY21 Response: We will require that the technology vendors that we work with provide a SOC report annually that shows that they are following the same best practices as BPCA. We will verify that they are compliant with security regulations that match or exceed our security requirements. The report will provide detailed information and assurance about the service organization's security, availability, processing integrity, confidentiality, and/or privacy controls.

Observation 3: Update the existing information security program referencing compliance with the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act, European Union's GDPR (General Data Protection Regulation) & CCPA (California Consumer Privacy Act); amongst other upcoming similar privacy regulations.

Management should consider updating their existing information security program with natural language that is easy to understand, with specificity around:

- How users' personal data is handled, including any third parties that you share data with.
- Identifying a DPO (Data Protection Officer) who is a knowledgeable expert who can answer questions, be on the lookout for policy breaches, and ensures that data privacy laws are being followed.
- Categorize sensitive data, including but not limited to
    - Race or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union memberships
    - Genetic or biometric data
    - Health or mortality
    - Sex life or sexual orientation

- Expand on data classification or retention procedures; as any information stored is public information; classifying institutional data based on its level of sensitivity, value, and criticality. Classification of data will aid in determining baseline security controls for the protection of data. We recommend considering the following:
    - Is the information in question critical for business operations?
    - Would the information be considered a permanent document of any kind?
    - Is the data considered proprietary intellectual property?
    - Does the data reflect current, legitimate, and useful business information or needs?

Management's FY21 Response: We will update the existing information security program to reference our compliance with NYSHIELD using natural language. All of our current personal data including the categories mentioned above are maintained by ADP.

Observation 4: We noted that the Organization did not perform a formal review of individual user access rights to the Network and Great Plains to ensure access changes were conducted in accordance with management's expectations during the fiscal year.

We recommend management perform a comprehensive review of user access entitlements for all in-scope applications on a regular basis (e.g., annually). The review should be performed by department heads and/or business owners based on system reports provided by system administrators and include the following:

- Review of Network and Great Plains account listings to ensure generic/group IDs are appropriate (use of such is strongly discouraged and should be minimized to the extent possible)
- Review of Network and Great Plains account listings to ensure accounts for terminated employees have been disabled or removed
- Review individual user access to ensure access is restricted to appropriate functions based on current job responsibilities
- Review access to powerful privileges, system resources and administrative access to ensure access is restricted to a very limited number of authorized personnel

The access review for the Network and Great Plains should be formally documented by each department head and/or data owner and evidence should be retained. Any identified conflicts in access rights should be followed up and resolved in a timely manner.

Management's FY21 Response: The MIS department has made the necessary changes to restrict individual user access rights to the network and Great Plains. We have removed stale or inactive accounts as well as increased the number of characters required for our passwords. We have also set expiration dates on our passwords that force all of our team members to change their passwords every 90 days. The MIS department has also audited our usernames and removed administrative rights to every team member except for those who need it (MIS team only).

Exhibit II – Prior Year Recommendations Requiring Further Action

Observation 1 (FY20): We noted that a formalized and approved Disaster Recovery Plan exists, however associated testing was not conducted in FY20.

To work toward a more resilient environment, we recommend that management reaffirm their Disaster Recovery/Business Continuity plan to enable business processes to operate manually and uninterrupted in the event of unforeseen circumstances. Furthermore, we recommend the Disaster Recovery plan be tested at least annually to ensure that, in the event of an emergency, the plan is effective. Being prepared in the event of a breach is the best defensive action an organization can take to minimize the risk posed by a potential cyber security attack.

Management's FY20 Response: Due to the pandemic this was not completed for FY20. We will accomplish in FY21.

Management's FY21 Response: Unfortunately, the MIS team's Senior Network Manager and Senior Systems Administrator left the Authority this past year, preventing the short-staffed team to conduct a successful test. We are in the process of re-hiring staff and with this new staff, we will be conducting a Disaster Recovery test in Fiscal Year 2022.

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

1. *Outdated Firewall Device*