# New York City School Construction Authority


## Management Letter Recommendations

(Resulting from the June 30, 2020 Audit)

MARKS PANETH

ACCOUNTANTS & ADVISORS

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

MARKS PANETH
ACCOUNTANTS & ADVISORS

December 23, 2020

The President and the Board of Trustees of the
New York City School Construction Authority

In planning and performing our audit of the financial statements of New York City School Construction Authority (the "Authority" or "SCA"), a component unit of The City of New York, as of and for the year ended June 30, 2020, in accordance with auditing standards generally accepted in the United States of America, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Our consideration of internal control was for the limited purpose described in the first paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses. Given these limitations during our audit, we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

In addition, we made recommendations and suggestions, which, if implemented, could further strengthen the internal controls and business practices (see attached Schedules). The Authority's responses to our observations and recommendations were not subjected to any auditing procedures and, accordingly, we express no opinion on the responses.

This report is intended solely for the information and use of the Authority's Board of Trustees, Audit Advisory Committee, management, others within the organization, and is not intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,

Marks Paneth LLP

MARKS PANETH LLP

Morison KSi
Independent member

## SCHEDULE 1 – FINANCIAL STATEMENT AUDIT OBSERVATIONS AND RECOMMENDATIONS

### OVERVIEW

There were no new observations and recommendations noted during our audit of the Authority's June 30, 2020 financial statements and no observations and recommendations from the prior year audit that require further attention.

In addition, we considered the internal controls within the information technology infrastructure and collected and evaluated evidence of the Authority's information systems, practices, and operations. The observations and recommendations related to information technology are located in Schedule II.

## SCHEDULE II – INFORMATION TECHNOLOGY OBSERVATIONS AND RECOMMENDATIONS

Exhibit I of this Schedule pertains to any new findings that were identified during our work in connection with the Authority's financial statement audit for the year ended June 30, 2020. Based upon our review of the IT General Controls, including obtaining information about Cyber Security controls and practices, two new observations were presented.

Exhibit II pertains to prior year recommendations that, based on our current procedures, appear to require further attention by management. There are three observations from the prior year that have been carried forward to this year.

Exhibit III are those observations and recommendations from the prior year that do not require further action.

## OVERVIEW

During the course of our review, Marks Paneth LLP's Audit Team spoke with the following individuals:

1. Emanuele Innamorato, Chief Information Officer
2. Steven Poon, Director of IT Operations, and Infrastructure

Our examination was performed in conjunction with the Authority's financial statement audit for the year ended June 30, 2020. We considered the internal controls within the Information Technology ("IT") infrastructure and collected and evaluated evidence of SCA's information systems, practices, and operations in order to 1) assist the Marks Paneth LLP 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 as to whether the use of automation is being optimally utilized and operating effectively and efficiently to contribute to SCA's goals and objectives.

Currently, SCA runs Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2016, Solaris 11, and VMware ESX 5.5/6. SCA uses:

1. Oracle's E-Business Suite (EBS) Financials as their accounting software
2. Workday's SaaS-based (Software as a Service) services for HR information management
3. Ultimate UKG Kronos Group SaaS-based services for payroll processing
4. Oracle's Primavera Contract Management for construction management tracking
5. Frontline Data Services co-location facility in Orangeburg, NY to host disaster recovery systems
6. Corus Group, LLC to provide disaster recovery support services

## CYBERSECURITY

We also considered SCA's Cyber Security protections and its ability to detect and prevent unauthorized internal and external access to SCA'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 SCA 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 the 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: *Are 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 SCA's information systems. We reviewed the Information Security Governance as well as other security policies that were developed to provide a foundation for which SCA manages its security risk.

Physical devices supporting SCA's technology environment are maintained in inventory. This practice of inventorying all information systems on the network reduces the risk that appropriate and adequate security controls may not be applied to the complete scope of SCA's information systems.

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

SCA 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 is commensurate with their job responsibilities at both the network and business application. The process is initiated by Human Resources and requires an employee ID for the account to be created. If the user requires access to financial systems, for example, the VP of Finance and Human Resources must approve access.

Additionally, SCA has deployed a formal Password Policy which leverages unique usernames and passwords (i.e., identities) for each user to ensure appropriate access and the ability to track interactions between users and systems. This policy also addresses password length requirements, complexity requirements and password duration/reset.

Recertifications of network and application accounts are performed to validate that users are still active employees and that the access levels are appropriate on an annual basis. Additionally, "Inactive Reports" are generated for users who have not signed on to the system in 45 days. If it is determined the user no longer exists, the user is removed from the system.

**Detect:**

There are various detection tools in place to monitor for and detect any unusual security patterns, events, and anomalies, including:

- Azure-hosted Cisco ASA and on-premise Checkpoint firewall devices deployed
- IronPort's SaaS-based services are used to filter spam
- Symantec's Endpoint Protection is used to defend against malware attacks on servers and workstations
- FireEye Intrusion Detection and Prevention (IDS/IPS) appliances monitor internal and external network connections
- Mobile device protection is provided by VMware's AirWatch mobile device management system, which includes the ability to delete ("wipe") data on the mobile devices issued by SCA. SCA does not allow employees to use their own personal devices to connect to SCA's email services and network/other information assets
- Microsoft's native BitLocker software is used to encrypt laptop hard drives

Additionally, SCA has engaged with EY to do penetration testing to determine and expose any potential vulnerabilities on the system. The next test is scheduled to be completed prior to the end of this calendar year. EY has also done a comprehensive review of SCA's cyber security program.

SCA is routinely providing training about cyber security. There is an active "Phishing" campaign to continually reinforce to end users not to open emails/attachments unless they are sure of the source.

**Respond:**

SCA has an Incident Response Plan in place to handle the response to a data breach in accordance with contractual, statutory, and/or regulatory obligations.

Additionally, should a new threat be introduced, Patch Management procedures are in place for "patching." Should there be a critical patch that needs to be installed immediately, it will be rolled out.

**Recover:**

A Disaster Recovery plan is in place. The plan should be expanded to address, and test scenarios related to cyber breach.

**Cyber Insurance:**

We were also informed that SCA is in the process of acquiring cyber insurance to mitigate losses from a variety of potential cyber incidents, including data breaches, business interruption, and network damage. We strongly recommend that SCA'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 SCA's business are addressed.

## Exhibit I – Current Year New Recommendations

***Observation 1 (FY20):*** Update existing information security program referencing compliance with European Union's GDPR (General Data Protection Regulation) & CCPA (California Consumer Privacy Act); amongst other upcoming similar privacy regulations.

***Recommendation:*** 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
    - Trade union memberships
    - Health or mortality
- 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 FY 2020 Response****:* Management agrees with this recommendation. IT will consult with SCA legal counsel to identify privacy regulations the agency is required to be in compliance with. The Data Classification policy and existing information security program will be updated to include the management of personal and sensitive data. The SCA will explore adding a Data Protection Officer.

***Observation 2 (FY20):*** We noted that the Authority did not perform a formal review of individual user access rights to the Network and the Oracle EBS application to ensure access changes were conducted in accordance with management's expectations during the fiscal year.

***Recommendation:*** 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 Oracle EBS 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 Oracle EBS 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 Oracle EBS 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 FY 2020 Response**:* Management agrees with this recommendation. SCA will review and modify its annual access procedure to include removal of terminated employees, verification of application roles based on current job responsibilities, and all generic accounts. This will be implemented in fourth quarter of FY 2021 as part of SCA's annual access review for Oracle EBS and network accounts. Privilege and administrative accounts will be reviewed every three months to ensure they are appropriate.

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

## Exhibit II – Prior Year Observations Requiring Further Attention

### 1. Cyber Insurance (Prior Year Observation #2)

***Prior Year Observation (FY 2017):*** We were informed that SCA has not purchased cyber insurance. Cyber insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruptions, and network damage. For further information regarding cyber insurance and its benefits, a good overview is provided by the U.S. Department of Homeland Security (DHS) at the following link:
( https://www.dhs.gov/cybersecurity-insurance )

***Initial Recommendation:*** Management should consider creating a risk profile in order to determine SCA's need for cyber insurance. Management should consider working with their insurance provider to provide an analysis of risk vs. cost. Cyber risk refers to any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber-attacks, fraud committed by misuse of data, any liability arising from data storage and the availability, integrity, and confidentiality of electronic information − be it related to individuals, companies or governments

The benefits of cyber insurance include, but are not limited to, the following:

1. Insurance places a dollar value on an organization's cyber risk.
2. The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement.
3. Many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools as well as significant incident response assistance following a cyber incident.

Cyber insurance providers include, but are not limited to, the following:

1. American International Group (AIG)
   ( http://www.aig.com/business/insurance/cyber-insurance )
2. Chubb Limited
   ( https://www2.chubb.com/us-en/business-insurance/privacy-network-security.aspx )
3. XL Group Ltd.
   (http://xlcatlin.com/insurance/insurance-coverage/professional-insurance/cyber-and-technology)

***FY 2018 Update*:** We were informed that SCA is in the process of acquiring quotes for cyber insurance. We continue to recommend that management consider allocating the resources necessary to create a risk profile in order to determine SCA's need for cyber insurance

***Management's FY 2018 Response:*** SCA is in the process of acquiring cyber insurance quotes and completing its risk profile.

***FY 2019 Status Update:*** This process is partially remediated. SCA has engaged with a new insurance broker who is onboarding SCA to acquire cyber insurance. As SCA goes through this process of finalizing the cyber insurance coverage, we strongly recommend that SCA'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 SCA's business are addressed.

***Management's FY 2019 Response:*** The SCA agrees with the recommendation. In June 2019, the SCA retained the services of Marsh USA, Inc., as its new insurance broker. Recently, the SCA completed Marsh's cyber security self-assessment. The self-assessment, along with the cyber penetration testing, will be used to determine cyber insurance coverage options and quotes that align with SCA's business. The SCA anticipates finalizing cyber insurance coverage by the end of fiscal year 2020.

***Management's FY 2020 Response:*** The SCA is working with Marsh to obtain quotes from cyber insurance carriers, anticipating insurance coverage to start in fiscal year 2021.

**2. Business Continuity and Disaster Recovery (BCDR) Planning (Prior Year Observation #5)**

***Observation (FY 2015):*** We were provided with a copy of the SCA Emergency Management Plan and the renewal agreement with Corus Managed Services, LLC, SCA's provider of business continuity services. Further, we were informed SCA performs an annual disaster recovery test at the Corus site. We understand the deployment of the disaster recovery site is a work in progress; however, the documentation we were provided does not include detailed action plans documenting the disaster recovery procedures. In addition, while the functionality exists for staff to connect to the disaster recovery site, we were informed instructions for staff detailing how to connect to the disaster recovery servers have not been created.

***Initial Recommendation:*** Management should consider creating formal disaster recovery action plans for the activation of the disaster recovery site at Corus. We recommend creating the procedures to be used by people who are technically proficient but who may not have direct knowledge about SCA's operations, networks, and infrastructure. Include detailed instructions showing staff how to connect to the disaster recovery servers from workstations at SCA offices and from remote locations, such as from a home computer.

***FY 2018 Status:*** We were informed that SCA has completed its disaster recovery testing processes at the organization's designated warm site at Frontline Data Services in Orangeburg, NY. We were also informed that, as part of the BCDR plan, a Business Impact Analysis (BIA) has not yet been conducted. The concern is that the lack of a BIA will adversely affect recovery and, thus, the ability to perform business processes in the event of a severe business disruption. We continue to recommend that management consider allocating the resources necessary to conduct a BIA, so as to determine the critical functions at SCA, who performs them, and what resources would be needed in a business interruption; many of these may not be IT functions. As part of the BIA, the following should be performed:

1. Evaluate and document the Recovery Point Objective (RPO) for each critical function if applicable. *The RPO is the amount of time prior to a disruption for which the lack of data backup is acceptable.* For example, an RPO of two hours means that data lost up to two hours before a disruption will be restored by means other than a restore of a digital backup
2. Evaluate and document the Recovery Time Objective (RTO) for each of the critical functions identified in the Business Impact Analysis. *The RTO is the amount of time allowed for the restoration of a business process in order to avoid unacceptable consequences from a severe disruption.* Include in the evaluation "busier" times of year when determining the RTO

***Management's FY 2018 Response:*** SCA is nearing completion of a BIA, capturing the respective RTO and RPO for all essential business processes. In addition to IT considerations, the BIA identifies essential staff, assesses interdepartmental dependencies, and forecasts potential changes over a 12-month period.

The BCP also will address facilities, personnel, and business processes not governed by IT systems. BCP triggering scenarios will provide clear guidelines by informing the content of recovery action plans. The BCP will align with Disaster Recovery operations. The BIA and BCP will be completed by end of fiscal year 2019. Staff training on Business Continuity will commence subsequent to completion of the BCP.

***FY 2019 Status Update:*** The COO's office has responsibility to drive the BCDR initiative. We were informed that the BIA process is completed which will be used to drive recovery strategies and plans.

From a technical recovery perspective, Disaster Recovery (DR) procedures are documented. The datacenter backup site is in Orangeburg, New York. SCA is utilizing their own equipment for DR versus renting the equipment.

Our recommendations include the following:

Based upon the results of the BIA, business continuity plans should be developed based upon the agreed-to strategies for people, process, and technology. The technical DR plans should be reviewed to validate that the technical recovery will support the business requirements agreed to in the BIA results.

BCDR plans are built on scenarios and assumptions of availability of systems, people, and processes. It is through testing as well as training and awareness that plans can be tested and challenged to ensure their viability should they need to be activated at a time of incident. Given the current landscape of threats and risks that could impact operations, from an isolated incident, such as fire impacting a single floor, to a system outage caused by malware incident, it is essential that testing of the components of the business continuity plans are conducted. Many organizations similar in size to SCA have put in place a "maturity model" for how they address their testing program.

For example, organizations may initiate their testing by doing basic walkthroughs of the plans so that resources understand their role and responsibility. Each test, thereafter, becomes more sophisticated to test capabilities and "prove" that assumptions and strategies will work as intended. We, therefore, recommend that SCA test current plans in place to assess their capabilities and use the outcome of testing to further drive and refine their overall business continuity program.

***Management's FY 2019 Response:*** Based on the data derived from the BIA, the SCA drafted a business continuity plan ("BCP") describing the allocation of personnel and equipment during disruptive incidents lasting greater than 24 hours. These incidents encompass scenarios that negatively impact the state of the SCA's headquarters, the efficacy of IT systems, and the ability of staff to mobilize. The BCP is anticipated to be delivered by the end of March 2020.

The SCA is creating a resiliency strategy that integrates business continuity, emergency management, information technology disaster recovery, and cyber security. Implementing mechanisms for business continuity testing will be facilitated through the procurement of an appropriately credentialed vendor that will assist in developing and executing training that will result in adoption of the recommended maturity model. Development of testing mechanisms and implementation for a maturity model is anticipated by December 2020.

***Management's FY 2020 Response:*** The SCA approved a Business Continuity Plan (BCP) in the first quarter of calendar year 2020. While the COVID-19 Pandemic has delayed in-person BCP training for leadership and staff until 2021, actual Business Continuity Plan implementation has taken place since mid-March 2020. The BCP has informed the assignment and dissemination of IT equipment needs to affected staff—successfully transitioning the SCA to a remote workforce. Operational roles in the BCP have provided a framework for quickly developing policies and strategies on emerging issues during the Pandemic, including dissemination of PPE, IT implementation for daily health screenings for all employees, teleworking and other Pandemic-specific policies and operating guidelines, and staff training for both an interim and eventual full-staff return to the SCA's main office. The BCP requires an annual update which is facilitated via a Business Impact Assessment (BIA). That update to the BIA will be completed January 2021. The BIA update and the lessons learned from the COVID-19 Pandemic will be incorporated into the 2021 version of the BCP. The 2021 BCP is scheduled for leadership approval by March 2021.

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

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

3. **Outdated Server Operating System (Prior Year Observation #1)**
4. **Laptop and Portable Device Security (Prior Year Observation #3)**
5. **IT Rights to Financial and Operational Systems (Prior Year Observation #4)**

****END****