Date: November 3, 2023

To: NY School Construction Authority

From: MHM IT Audit

Technology Observations and Recommendations Resulting From the 2023 IT Audit / Cybersecurity Review

OVERVIEW

MHM IT audit personnel conducted interviews with Steven Poon, Director of IT Operations and Infrastructure to walk through IT general controls and relevant cybersecurity controls.

Our review was specific to the following in-scope systems, including all levels of technology related to the system (e.g., network, application and database):

1. Oracle EBS
2. Primavera (Contract Management System)

CYBERSECURITY

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

As a method for review, CBIZ - 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*

Exhibit I – Current Year Recommendations

Observation 1: In alignment with Internal Audit's review dated May 20, 2022, and per our own inspection of current IT policies and procedures, MHM noted that multiple had not been reviewed or updated in an extended period. As policies and procedures was ranked the fifth highest risk to the organization in your FY24 Enterprise Risk Assessment, we would recommend that policies are revisited annually to ensure they are up-to-date and current business processes align with such policies.

Policies recommended immediate review would include:

1. Change Management Policy – last updated in March 2017
2. Personal Use of Work Resources (IT-007) – last updated in 2021
3. Internal Usage (IT-004) – last updated in 2019
4. Acceptable Use Policy for Electronic Email (IT-003) – last updated in 2019

FY23 Management Response:

A formal process has been established to review and update all IT policies and procedures annually. All IT policies and procedures will be updated by June 2024.

Observation 2: We recommend that management continue to work through open items on the most recent penetration test, and also continue to integrate changes and updates to the existing Business Continuity Plan.

The Internal Audit review from May-22 emphasized critical areas for addition to the Business Continuity Plan. Per our own independent inspection of the policy, it appeared that updates were still in progress with multiple notes/highlights throughout the document. We recommend that NYCSCA continue to work to finalize these changes.

In addition, NYCSCA should continue to work through remediation of high and critical findings from the most recent penetration test performed on September 30, 2022. Per discussion with management, approximately 75% of findings have been remediated. Continued focus and emphasis should be placed on resolution of high-risk items.

FY23 Management Response:

Throughout 2023, the Business Continuity Plan underwent updates and revisions through feedback and recovery test performed during remote work. The Business Continuity Plan is anticipated to be approved by end of March 2024, with training anticipated by end of June 2024.

In regard to the findings from the recent penetration test, all critical and high risk findings have been addressed, and the majority of the medium identified risk have also been resolved. The remaining open findings are anticipated to be remediated by March 2024.

Observation 3: We noted that no user access review had been performed to assess the appropriateness of access to Oracle EBS or Primavera during the past fiscal year. While quarterly reviews have been performed in the past, it was noted that the last reviews available were dated from October 2022. User access reviews provide an opportunity for validation that no former employees (or contractors/vendors) continue to have access to your systems, along with validating that permissions for existing employees aligns with their current roles and responsibilities.

FY23 Management Response:

The Oracle EBS user access review was completed in November 2023; the Primavera user access review is anticipated to be completed by end of February 2024.

Observation 4: MHM noted that no recent vendor risk assessments had been performed in the past fiscal year. In addition, we were unable to obtain evidence of the periodic review of vendor SOC reports.

We recommend that NYCSCA documents and reviews all key vendors on a periodic basis based upon the assessed level of risk of the vendor. As the organization relies on vendors to carry out processes, handle data, and sustain governance over parts the IT environment, management should carefully consider the effects this has on overall fluidity within the organization's IT infrastructure. Vendor assessments should be risk rated to maintain a level of pragmaticism in conducting and managing such reviews. Best practices would typically entail rating key vendors based upon overall level of assessed risk to the organization (high, medium and low) and then conducting reviews on a frequency in accordance with such risk (e.g., high = annually, medium = every 2 years, low = every 3 years).

We further recommend that NYCSCA performs a documented review of their vendor SOC reports annually. As these vendors handle important company processes and data, management should consider how this can affect the comfort and management of their own objectives and information. In addition to an overall assessment as to SOC compliance of third parties (evaluation of qualified/unqualified opinion and identified exceptions), we recommend that management consider formally documentation and evaluation of other key SOC risks (each of which would be "best practices"), including:

- an assessment of the reputation of the service auditor – Are they a known and/or reputable firm? This can typically be done via online research and ensuring the firm providing the opinion is registered with the AICPA. With more and more cybersecurity firms entering the SOC space, it is important to ensure you are getting comfort from a reputable firm,
- evaluating and documenting you have sufficient complementary user entity controls (CUECs) in place and are operating effectively – Any SOC report should spell out controls that your organization is responsible "in addition" to the controls of the service provider that must be in place. For example, the service provider may allow for you to manage your own access so it would be important to verify you have sufficient controls in this area to "complement" the service providers controls,
- verify that all subservice providers are detailed within the SOC report opinion by vendor name and not listed generically. For each subservice provider, confirm with your service provider as to their evaluation of the subservice provider which should include a similar SOC report evaluation.
- Review the duration of the period to issuance based upon the period of the report. If the issuance period is excessive after the report period end date (>90 days), inquire of the service provider as to the business reasons for the delay in demonstration of their compliance.
- Lastly, any exceptions identified should not only be assessed and considered if that will impact their environment – For example, if the service provider has exceptions around change management of their software, you may wish to inquire of them what the impact to your reliance on the system may be.

FY23 Management Response:

NYCSCA Information Technology and Internal Audit will collaborate to establish a formal program on vendor risk assessment and review of SOC. The program is anticipated to be established by the end of fiscal year 2024, with execution in fiscal year 2025. Upon execution of the program, Information Technology and Internal Audit will work with internal operations to implement procedures on risk and compliancy review, including SOC report review, for key vendors.