The Metropolitan Transportation Authority

Report to Management

Year Ended December 31, 2020

Deloitte.

Deloitte & Touche LLP
30 Rockefeller Plaza
New York, NY 10112
USA
Tel: +1-212-492-4000
Fax: +1-212-489-1687
www.deloitte.com

May 28, 2021

The Audit Committee
Metropolitan Transportation Authority
New York, New York

And

The Management of the Metropolitan Transportation Authority
New York, New York

Dear Members of the Audit Committee and Management:

In connection with our audits of the financial statements of the Metropolitan Transportation Authority, First Mutual Transportation Assurance Company, Long Island Rail Road Company, Metro-North Commuter Railroad Company, MTA Bus Company, New York City Transit Authority, Staten Island Rapid Transit Operating Authority and the Triborough Bridge and Tunnel Authority (collectively the "MTA") as of and for the year ended December 31, 2020 (on which we have issued our reports dated May 28, 2021 which contain three explanatory paragraphs including subsidies from other governmental entities, the adoption of GASB 97, *Certain Component Unit Criteria and Accounting and Financial Reporting for Internal Revenue Code Section 457 Deferred Compensation Plans*, and the impact the novel coronavirus (COVID-19) outbreak on the Authority, performed in accordance with auditing standards generally accepted in the United States of America (generally accepted auditing standards), we considered the MTA's internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the MTA's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the MTA's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting. However, in connection with our audits, we have identified, and included in the attached Appendix A, deficiencies related to the MTA's internal control over financial reporting and other matters as of December 31, 2020, that we wish to bring to your attention.

We also plan to issue our Uniform Guidance Reports in accordance with *Government Auditing Standards* and the U.S. Office of Management and Budget ("OMB") audit requirements of Title 2 U.S. Code of Federal Regulations (CFR) Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* ("OMB Uniform Guidance") and compliance with the types of compliance requirements described in the *Part 43 of the New York State Codification of Rules and Regulations* which will include (1) Independent Auditors' Report (2) Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in accordance with *Government Auditing Standards* (3) Independent Auditors' Report on Compliance for Each Major Federal Program; and Report on Internal Control Over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by the Uniform Guidance, and (4) Independent Auditors' Report on Compliance for Each Major State of New York Department of Transportation Assistance Program; and Report on Internal

Controls over Compliance; and Report on Schedule of State of New York Department of Transportation Assistance expended Required by Part 43 of the New York State Codification of Rules and Regulations.

The definitions of a material weakness, significant deficiency and deficiency are also set forth in the attached Appendix B

Although we have included management's written response to our comments in the attached Appendix A, such responses have not been subjected to the auditing procedures applied in our audits of the financial statements and, accordingly, we do not express an opinion or provide any form of assurance on the appropriateness of the responses or the effectiveness of any corrective actions described therein.

A description of the responsibility of management for establishing and maintaining internal control over financial reporting and of the objectives of and inherent limitations of internal control over financial reporting, is set forth in the attached Appendix C and should be read in conjunction with this report.

This report is intended solely for the information and use of management, the Audit Committee, Federal and State awarding agencies or pass-through entities, and others within the organization and is not intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,

Deloitte & Touche LLP

THE METROPOLITAN TRANSPORTATION AUTHORITY
TABLE OF CONTENTS

Page

APPENDIX A

APPENDIX B

APPENDIX C

APPENDIX A

MTA CONSOLIDATED INFORMATION TECHNOLOGY (“IT”) DEPARTMENT

DEFICIENCIES

We identified, and included below, deficiencies involving the MTA Consolidated IT Department's internal control over financial reporting for the year ended December 31, 2020, that have not been previously communicated in writing or orally, by others within the MTA, or by us.

1. WCIS Oracle Database Password Parameters

Agency:
New York City Transit Authority

Criteria:
The identity of users should be authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
D&T noted that password settings for the DEFAULT profile (minimum length, expiration, lockout, history, & complexity) and the ADMIN_PROFILE profile (minimum length, expiration, history, & complexity) on the Oracle database supporting the WCIS application are not set in compliance with the company security policies. Given that both profiles have user accounts assigned to them, including individual database administrator accounts, these settings are inappropriate. There are individual user accounts assigned to the profile and therefore passwords for those individuals do not adhere to the policy for minimum length, expiration, lockout, history, & complexity.

Cause:
Although Management has a formal policy as it pertains to password parameters, they have not sufficiently reinforced the policy and haven't monitored adherence to the policy. D&T noted that the root cause was attributed to oversight on behalf of management.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access to the Oracle database supporting the WCIS application which could potentially lead to inappropriate changes to application data.

Recommendation:
We recommend that MTA HQ management either align the password parameters for the DEFAULT and ADMIN_PROFILE profiles on the Oracle Database with MTA HQ security policies and industry best practices or restrict DEFAULT profile to system/generic accounts (i.e. removing the user accounts).

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: MTA will update the DEFAULT and ADMIN_PROFILE profiles on the Oracle Database to align with MTA password Standard. Estimated Completion Date 1st Quarter 2022.

2. WCIS Oracle Database Privileged Access

Agency:
New York City Transit Authority

Criteria:
Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.

Condition:
During our audit procedures, D&T noted that five users retained inappropriate access to the Oracle database supporting WCIS. Through inquiry with management, we noted that these users no longer work at the MTA, but their database accounts remained active.

Cause:
Although Management has a formal policy as it pertains to privileged access and the removal of access for terminated employees, they have not sufficiently reinforced the policy and haven't revoked accounts that no longer require elevated access.

Effect:
Given that privileged access has not been appropriately restricted, there is a risk of unauthorized user access modifications that would circumvent the provisioning and deprovisioning processes.

Recommendation:
We recommend that New York Transit Authority management appropriately restrict privileged access accounts when the access is no longer required.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: MTA will remove privileged access accounts who no longer need access. Estimated Completion Date 3rd Quarter 2021.

3. Change Management - Access to Production – WCIS Application

Agency:
New York City Transit Authority

Criteria:
Access to implement changes into the application production environment should be appropriately restricted to the IT Security Administrator and segregated from application developers.

Condition:
D&T noted that there is an insufficient segregation of duties as there are two developers with access to promote changes to the WCIS production environment. Additionally, D&T identified four accounts with inappropriate access to promote changes as they belong to terminated users.

As such, it is possible for a developer to migrate their own change into the WCIS production environment without appropriate change management testing and approvals.

Cause:
MTA IT has not appropriately segregated logical access for developers; they are granted access to both development and production environments without sufficient monitoring controls.

Effect:
Given that logical access has not been appropriately segregated, there is a risk of unauthorized changes being implemented into the production environment that would circumvent the change management process.

Recommendation:
We recommend that MTA IT restrict logical access to the developers such that they cannot move changes from the test environment into production.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by the following control:

- As changes are required to be tested and approved prior to implementation in production as a part of the control, D&T noted that an effective control would mitigate the risk of inappropriate changes to the application or supporting database.

Management Response (2020): Management Concurs: WCIS application will be replaced by Origami application in 7 business days. **Estimated Completion Date 3rd Quarter 2021.**

4. AFC Terminations

Agency:
New York City Transit Authority

Criteria:
Access for terminated and/or transferred users is removed or modified in a timely manner.

Condition:
During our audit procedures, D&T noted that access to the AFC application was not disabled in a timely manner for six out of twenty-five sampled terminated users.

Cause:
The root cause of this deficiency is that IT Management did not adhere to the user deprovisioning process when removing access for the terminated users identified in this finding.

Effect:
Given that these accounts remain enabled, there is a risk that the accounts could be compromised by other users and result in unauthorized access to the application, which may create improper segregation of duties.

Recommendation:
We recommend that New York Transit Authority management reinforce the termination process with end users and system administrators to ensure that access changes are appropriately communicated and removed in a timely manner when the access is no longer required.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management concur IAMS Identity Access Management System and People Soft and HR Human Resource feed works as design. However, HR termination process and HR feed needs to be strengthened so that IAMs can remove end users timely. **Estimated Completion Date 3rd Quarter 2021.**

5. Windows AD Network Privileged Access

Agency:
New York City Transit Authority

Criteria:
Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.

Condition:
During our audit procedures, D&T noted that there are two service accounts that are inappropriately granted privileged access to the Windows AD network supporting NYCT, as management is not aware of the purpose of the account and/or the users with access to each account.

Cause:
D&T noted the root cause of this deficiency is that IT Management does not perform a periodic review of service accounts to recertify their business purpose and the appropriateness of access.

Effect:
Given that privileged access has not been appropriately restricted, there is a risk of users with access to the noted service accounts have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.

Recommendation:
We recommend that management remove the inappropriate access and periodically recertify the appropriateness of service accounts.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management concurs; the 2 accounts access has been removed and is going through the standard decommission process. **Estimation Completion Date 3rd Quarter 2021**

6. TBTA Kronos Application Password Parameters

Agency:
Triborough Bridge and Tunnel Authority ("TBTA" and/or "company")

Criteria:
The identity of users should be authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
- The password parameters for the 'Never Expire' logon profile in the TBTA Kronos application are not set in line with the company password policy for the following parameters: password minimum length, password expiration, lockout threshold, password history and password complexity.

- In order to promote changes into production, the members of the TBTA Kronos application team use the username and password for a single shared account to access the Kronos Workforce Integration Manager tool. The password to this shared account is not being stored in a secure location such as password vaulting.

Cause:
Although Management has a formal policy as it pertains to password parameters, they have not sufficiently reinforced the policy and haven't monitored adherence to the policy. D&T noted that the root cause was attributed to oversight on behalf of management.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access to the Kronos application which could potentially lead to inappropriate changes to the application or underlying data.

Recommendation:
We recommend that MTA TBTA management update password parameters on the Kronos application network to align either to the MTA HQ security policies or industry best practices. We recommend that MTA TBTA management use a password vault or similar solution to secure the password for the shared account used to access the Kronos Workforce Integration Manager.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: The password criteria for all logon profiles is being updated to align with MTA policies. With the upgrade to the new Kronos application in the cloud, Single Sign On will be setup for all users. Any non-SSO accounts would be for the Production Support team, or for employees without network accounts. Each user will have a unique User ID. **Estimated Completion Date 1st Quarter 2022**

7. TBTA Kronos New Access Provisioning

Agency:
Triborough Bridge and Tunnel Authority ("TBTA")

Criteria:
Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties.

Condition:
During testing D&T noted that the request for access for the new hire sample did not specify the level of access the user should be granted in the TBTA Kronos application. As such, D&T was unable to validate that the type of access granted in the application matches the type of access requested for the new hire.

Cause:
The root cause of this deficiency is that IT Management did not adhere to the user provisioning process when requesting for new access for a user in the application.

Effect:
Without appropriate documentation related to the access provisioning process, there is a risk that users will be granted access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.

Recommendation:
We recommend that MTA TBTA management reinforce the access request process with end users and system administrators to ensure that access requests are appropriately documented.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: All user accounts (employee or manager) will be reviewed and approved by B&T controller office before they are assigned by IT We will be updating the access request process to accommodate any changes in the application due to our current Kronos upgrade.
Estimated Completion Date 1st Quarter 2022

8. TBTA Kronos and Oracle Database Terminations

Agency:
Triborough Bridge and Tunnel Authority ("TBTA")

Criteria:
Access for terminated and/or transferred users is removed or modified in a timely manner.

Condition:
During our audit procedures, D&T noted that there is not a process in place for the TBTA Kronos application team to be notified when users are terminated. As such, management is not disabling accounts belonging to terminated users in a timely manner.

Cause:
The root cause of this deficiency is that IT Management does not have a formal user deprovisioning process in place to remove access for terminated users on the application or supporting database.

Effect:
There is a risk that the accounts could be compromised and result in unauthorized access to the application, which may create improper segregation of duties.

Recommendation:
We recommend that TBTA management design a process to remove access from the Kronos application and supporting Oracle database when users are terminated from TBTA.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: The move to Single Sign On will create a de facto termination of the users access upon leaving the MTA. MTA IT will work on a report process to identify employee and manger accounts in Kronos that exist for employees that have been terminated so they can be addressed in a timely manner. **Estimated Completion Date 1st Quarter 2022**

9. Change Management - Access to Production – TBTA Kronos Application

Agency:
Triborough Bridge and Tunnel Authority ("TBTA")

Criteria:
Access to implement changes into the application production environment should be appropriately restricted to the IT Security Administrator and segregated from application developers.

Condition:
D&T noted the users with access to promote changes into production for the TBTA Kronos application are also the users who develop the changes. This is a segregation of duties risk. Management does not have a formal retrospective review in place where a full listing of changes promoted into production is exported and reviewed on an established frequency.

Cause:
The root cause of this deficiency is that the team managing the relevant application and its database is small and IT management is not able to appropriately segregate the users who are developing changes and the users who are promoting changes into production. Additionally, IT management has not recognized and addressed this risk by formalizing a monitoring review over changes promoted into production for the relevant application and database.

Effect:
Given that logical access has not been appropriately segregated, there is a risk of unauthorized changes being implemented into the production environment that would circumvent the change management process.

Recommendation:
We recommend that MTA IT design and implement a review control to monitor changes promoted into the production environment.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: Due to the nature of the Kronos application and limited staff, developers need access to promote and duplicate their application changes to production. All production migrations are accompanied by tickets in ServiceNow and include user approvals. The current Kronos application will include separate User IDs for Application Support team members so that we can audit changes more effectively. **Estimated Completion Date 1st Quarter 2022**

10. ORT Application – User Access Recertification

Agency:
Triborough Bridge and Tunnel Authority ("TBTA")

Criteria:
User account recertifications / entitlement reviews are performed by the IT Department and application owners.

Condition:
D&T noted that for the ORT application, there is no periodic user account recertification / entitlement review performed by the IT Department or ORT application owners.

Cause:
The root cause of this deficiency is that IT Management does not have a formal user access review process in place to recertify access for the users who have access to the relevant application.

Effect:
Given that logical access is not periodically reviewed, there is a risk that users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.

Recommendation:
We recommend that MTA IT design and implement a review control to periodically recertify the appropriateness of users with access to ORT and their related system privileges.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: Management will recertify privilege users access annually **Estimation Completion Date 4th Quarter 2021.**

11. ManageEngine Tool Password Parameters

Agency:
Triborough Bridge and Tunnel Authority ("TBTA")

Criteria:
The identity of users should be authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
The ManageEngine Tool password parameters are not set in accordance with MTA policy for the following parameters: minimum password length, expiration, password history, and complexity. Weak password parameters could potentially result in users gaining unauthorized access the applications.

Cause:
Although Management has a formal policy as it pertains to password parameters, they have not sufficiently reinforced the policy and haven't monitored adherence to the policy. D&T noted that the root cause was attributed to oversight on behalf of management.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access to the ManageEngine tool which could potentially lead to inappropriate changes being implemented to the production environment (tool is used to implement ORT changes to production).

Recommendation:
We recommend that MTA TBTA management update password parameters on the ManageEngine tool to align either to the MTA HQ security policies or industry best practices.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concur: Management will research the feasibility of updating the Password Policy to align with MTA HQ security policy or industry best practice. **Estimated Completion Date 4th Quarter 2021.**

12. ORT Terminations

Agency:
Triborough Bridge and Tunnel Authority ("TBTA")

Criteria:
Access for terminated and/or transferred users is removed or modified in a timely manner.

Condition:
During our audit procedures, D&T noted that access to the ORT application was not disabled in a timely manner for three out of five sampled terminated users.

Cause:
The root cause of this deficiency is that IT Management did not adhere to the user deprovisioning process when removing access for the terminated users identified in this finding.

Effect:
Given that these accounts remain enabled, there is a risk that the accounts could be compromised by other users and result in unauthorized access to the application, which may create improper segregation of duties.

Recommendation:
We recommend that TBTA management reinforce the termination process with end users and system administrators to ensure that access changes are appropriately communicated and removed in a timely manner when the access is no longer required.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: Management will reinforce the termination process with end users and system administrators to ensure that access changes are appropriately communicated and removed in a timely. **Estimated Completion Date 4th quarter 2021.**

13. ORT Batch Job Monitoring

Agency:
Triborough Bridge and Tunnel Authority ("TBTA")

Criteria:
Automated scheduling tools have been implemented for the completeness of the flow of processing and are monitored by the IT Department.

Condition:
During our audit procedures, D&T noted that management does not maintain documentation related to batch job monitoring. As such, we were unable to validate that management performs appropriate monitoring procedures around the completion of the relevant batch jobs and resolution of job errors.

Cause:
The root cause of this deficiency is that Management does not maintain documentation around the monitoring of batch jobs, specifically error resolution.

Effect:
There is a risk that production systems, programs, and/or jobs result in inaccurate, incomplete, or unauthorized processing of data.

Recommendation:
We recommend that TBTA management retain documentation related to monitoring of batch job status and the resolution of any noted errors.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: Management will create procedures for monitoring of batch job status and Resolution of any noted errors. **Estimated Completion Date 1st Quarter 2022**

14. CSS Application, MNR Kronos Application, & Oracle Database Password Parameters

Agency:
Metro-North Railroad Commuter Railroad Company ("MNR" and/or "company")

Criteria:
The identity of users should be authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
CSS Application: The CSS password parameters do not have a lockout threshold set, whereas the company policy requires a lockout threshold of at least five attempts. Additionally, the password history is only three, while the company policy requires twenty-four. As such, the password parameters are not set in accordance with MTA security policies/industry best practices. Weak password parameters could potentially result in users gaining unauthorized access the applications.

MNR Kronos Application:

1. The password parameters for the &SUPER_USER_LOGON Logon Profile in the MNR Kronos application are not in line with the company password policy for the following parameters: password expiration, lockout threshold, password history and password complexity.

2. In order to promote changes into production, the members of the MNR Kronos application team use the username and password for a single shared account to access the Kronos Workforce Integration Manager tool. The password to this shared account is not being stored in a secure location such as password vaulting.

MNR Kronos Database: For the DEFAULT profile in the Oracle database supporting the MNR Kronos application, there is a user account assigned to this profile and the password parameters on this profile are not in line with the company password policy or industry standards for the following parameters: minimum password length, complexity, password history, password expiration and lockout attempts.

Cause:
Although Management has a formal policy as it pertains to password parameters, they have not sufficiently reinforced the policy and haven't monitored adherence to the policy. D&T noted that the root cause was attributed to oversight on behalf of management.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access to the CSS application, Kronos application, and Oracle database supporting the Kronos application, which could potentially lead to inappropriate changes to the application or underlying data.

Recommendation:
We recommend that MNR management align the password parameters for the CSS application and Kronos application with the MNR security policies and industry best practices. We recommend that MNR

management use a password vault or similar solution to secure the password for the shared account used to access the Kronos Workforce Integration Manager. We recommend that MNR management either align the password parameters for the DEFAULT profile on the Oracle database with MTA HQ security policies and industry best practices or restrict DEFAULT profile to system/generic accounts (i.e. removing the user accounts).

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs, password history will be updated to align with CSS application and Kronos application with the MNR security policies. **Estimated Completion Date 3rd Quarter 2021**

15. Change Management - Access to Production – CSS Application & MNR Kronos Application

Agency:
Metro-North Railroad Commuter Railroad Company ("MNR" and/or "company")

Criteria:
Access to implement changes into the application production environment should be appropriately restricted to the IT Security Administrator and segregated from application developers.

Condition:
CSS Application: Programmers, who are users that have access to develop changes to the CSS application, have access to promote changes into the CSS production environment.

MNR Kronos Application and Database: The users with access to promote changes into production for the MNR Kronos application are also the users who develop the changes. This is a segregation of duties risk. Management does not have a formal retrospective review in place where a full listing of changes promoted into production is exported and reviewed on an established frequency.

Cause:
The root cause of this deficiency is that the team managing the relevant application and its database is small and IT management is not able to appropriately segregate the users who are developing changes and the users who are promoting changes into production. Additionally, IT management has not recognized and addressed this risk by formalizing a monitoring review over changes promoted into production for the relevant application and database.

Effect:
Given that logical access has not been appropriately segregated, there is a risk of unauthorized changes being implemented into the production environment that would circumvent the change management process.

Recommendation:
We recommend that MTA IT design and implement a review control to monitor changes promoted into the production environment for both the CSS and Kronos applications.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020)*:* Management Concurs: Due to the nature of the Kronos application and limited staff, developers need access to promote and duplicate their application changes to production. All production migrations are accompanied by tickets in ServiceNow and include user approvals. The current Kronos application will include separate User IDs for Application Support team members so that we can audit changes more effectively. **Estimated Completion Date 1st Quarter 2022**

16. MNR Kronos Application and Oracle Database Terminations

Agency:
Metro-North Railroad Commuter Railroad Company ("MNR" and/or "company")

Criteria:
Access for terminated and/or transferred users is removed or modified in a timely manner.

Condition:
During our audit procedures, D&T noted that there is not a process in place for the MNR Kronos application team to be notified when users are terminated. As such, management is not disabling accounts belonging to terminated users in a timely manner.

Cause:
The root cause of this deficiency is that IT Management does not have a formal user deprovisioning process in place to remove access for terminated users on the application or supporting database.

Effect:
There is a risk that the accounts could be compromised and result in unauthorized access to the application, which may create improper segregation of duties.

Recommendation:
We recommend that MNR management design a process to remove access from the Kronos application and supporting Oracle database when users are terminated from MNR.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: The move to Single Sign On will create a de facto termination of the user's access upon leaving the MTA. MTA IT will work on a report process to identify employee and manger accounts in Kronos that exist for employees that have been terminated so they can be addressed in a timely manner. **Estimated Completion Date 1st Quarter 2022**

17. LIRR Kronos Application Password Parameters

Agency:
Long Island Railroad Company ("LIRR" and/or "company")

Criteria:
The identity of users should be authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
LIRR Kronos Application:

1. The password parameters for the &SUPER_USER_LOGON Logon Profile in the LIRR Kronos application are not in line with the company password policy for the following parameters: password minimum length, password expiration, lockout threshold, password history and password complexity.

2. In order to promote changes into production, the members of the LIRR Kronos application team use the username and password for a single shared account to access the Kronos Workforce Integration Manager tool. The password to this shared account is not being stored in a secure location such as password vaulting.

Cause:
Although Management has a formal policy as it pertains to password parameters, they have not sufficiently reinforced the policy and haven't monitored adherence to the policy. D&T noted that the root cause was attributed to oversight on behalf of management.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access to the Oracle database supporting the CAMS application, Oracle database supporting the TSS application, and the Kronos application, which could potentially lead to inappropriate changes to the application or underlying data.

Recommendation:
We recommend that LIRR management align the password parameters for the Kronos application with the LIRR security policies and industry best practices. We recommend that LIRR management use a password vault or similar solution to secure the password for the shared account used to access the Kronos Workforce Integration Manager.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: The password criteria for all logon profiles is being updated to align with MTA policies. With the upgrade to the new Kronos application in the cloud, Single Sign On will be setup for all users. Any non-SSO accounts would be for the Production Support team, or for employees without network accounts. Each user will have a unique User ID. **Estimated Completion Date 1st Quarter 2022**

18. TSS Application Privileged Access

Agency:
Long Island Railroad Company ("LIRR" and/or "company")

Criteria:
Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.

Condition:
During our audit procedures, D&T noted that there is one user account with inappropriate privileged access on the TSS application per their job function and inquiry with management.

Cause:
D&T noted the root cause of this deficiency is that IT Management does not perform a periodic review of administrator accounts to recertify the appropriateness of access.

Effect:
Given that privileged access has not been appropriately restricted, there is a risk of users having access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.

Recommendation:
We recommend that management remove the inappropriate access and periodically recertify the appropriateness of administrator accounts.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: The account in question "privilege" accounts have been removed. Estimated **Completion Date 3rd Quarter 2021**

19. Change Management - Access to Production – CAMS Application & LIRR Kronos Application

Agency:
Long Island Railroad Company ("LIRR" and/or "company")

Criteria:
Access to implement changes into the application production environment should be appropriately restricted to the IT Security Administrator and segregated from application developers.

Condition:
LIRR Kronos Application and Database: The users with access to promote changes into production for the LIRR Kronos application are also the users who develop the changes. This is a segregation of duties risk. Management does not have a formal retrospective review in place where a full listing of changes promoted into production is exported and reviewed on an established frequency.

Cause:
The root cause of this deficiency is that the team managing the relevant application and its database is small and IT management is not able to appropriately segregate the users who are developing changes and the users who are promoting changes into production. Additionally, IT management has not recognized and addressed this risk by formalizing a monitoring review over changes promoted into production for the relevant application and database.

Effect:
Given that logical access has not been appropriately segregated, there is a risk of unauthorized changes being implemented into the production environment that would circumvent the change management process.

Recommendation:
We recommend that MTA IT design and implement a review control to monitor changes promoted into the production environment for both the CAMS and Kronos applications.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: Due to the nature of the Kronos application and limited staff, developers need access to promote and duplicate their application changes to production. All production migrations are accompanied by tickets in ServiceNow and include user approvals. The current Kronos application will include separate User IDs for Application Support team members so that we can audit changes more effectively. **Estimated Completion Date 1st Quarter 2022**

20. LIRR Kronos Application and Oracle Database Terminations

Agency:
Long Island Railroad Company ("LIRR" and/or "company")

Criteria:
Access for terminated and/or transferred users is removed or modified in a timely manner.

Condition:
During our audit procedures, D&T noted that there is not a process in place for the LIRR Kronos application team to be notified when users are terminated. As such, management is not disabling accounts belonging to terminated users in a timely manner.

Cause:
The root cause of this deficiency is that IT Management does not have a formal user deprovisioning process in place to remove access for terminated users on the application or supporting database.

Effect:
There is a risk that the accounts could be compromised and result in unauthorized access to the application, which may create improper segregation of duties.

Recommendation:
We recommend that LIRR management design a process to remove access from the Kronos application and supporting Oracle database when users are terminated from LIRR.

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2020): Management Concurs: The move to Single Sign On will create a de facto termination of the user's access upon leaving the MTA. MTA IT will work on a report process to identify employee and manger accounts in Kronos that exist for employees that have been terminated so they can be addressed in a timely manner. **Estimated Completion Date 1st Quarter 2022**

We identified the following other deficiencies involving the Authority's internal control over financial reporting for the periods prior to the year ended December 31, 2020 that we wish to bring to your attention at this time.

21. Impact Oracle Database Password Parameters

Agency:
MTAHQ

Criteria:
The identity of users should be authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
D&T noted that password settings for the DEFAULT profile on the Oracle database supporting the Impact application are not in line with the MTA Corporate Policy and/or industry standards. There are individual user accounts assigned to the profile and therefore passwords for those individuals do not adhere to the policy for minimum length, expiration, lockout, history, & complexity.

Cause:
Although Management has a formal policy as it pertains to password parameters, they have not sufficiently reinforced the policy and haven't monitored adherence to the policy. D&T noted that the root cause was attributed to oversight on behalf of management.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access to the Oracle database supporting the Impact application which could potentially lead to inappropriate changes to application data.

Recommendation:
We recommend that MTA HQ management either align the password parameters for the DEFAULT profile on the Oracle Database with MTA HQ security policies and industry best practices or restrict DEFAULT profile to system/generic accounts (i.e. removing the user accounts).

Financial Statement Impact:
No Impact – risk associated with this deficiency mitigated by other controls and factors.

Management Response (2019):
Estimated Completion 3rd qtr. 2020
Management concurs: domain password policies for HQ Domain has been remediated.

Management Response (2020): Management Concurs: Management will align Oracle database password security to align with MTA HQ password policies. **Estimated Completion Date 4th Quarter 2021**

APPENDIX B

DEFINITIONS

The definition of a deficiency, a significant deficiency, and a material weakness are as follows:

A *deficiency* in internal control over financial reporting 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 deficiency in design exists when (a) a control necessary to meet the control objective is missing, or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the MTA's financial reporting.

A *material weakness* is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the MTA's annual or interim financial statements will not be prevented or detected on a timely basis.

APPENDIX C

MANAGEMENT'S RESPONSIBILITY FOR, AND THE OBJECTIVES AND INHERENT LIMITATIONS OF, INTERNAL CONTROL OVER FINANCIAL REPORTING

The following comments concerning management's responsibility for internal control over financial reporting and the objectives and inherent limitations of internal control over financial reporting are included in generally accepted auditing standards.

Management's Responsibility

The MTA's management is responsible for the overall accuracy of the financial statements and their conformity with accounting principles generally accepted in the United States of America. In this regard, the MTA's management is also responsible for designing, implementing and maintaining effective internal control over financial reporting.

Objectives of Internal Control over Financial Reporting

An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America, An entity's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the entity; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America, and that receipts and expenditures of the entity are being made only in accordance with authorizations of management and those charged with governance; and (3) provide reasonable assurance regarding prevention, or timely detection and correction, of unauthorized acquisition, use, or disposition of the entity's assets that could have a material effect on the financial statements.

Inherent Limitations of Internal Control over Financial Reporting

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements. Also, projections of any assessment of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

* * * * *