TXBASE AUDIT

PROGRAM EVALUATION AND AUDIT

METROPOLITAN
COUNCIL

December 2018

The Council purchased TXbase in 1996 and customized the program to meet the workforce and business needs of Metro Transit and Metropolitan Transportation Services (MTS). The TXbase system is composed of a software application and a database management system. Metro Transit uses the TXbase system to integrate maintenance, inventory management, purchasing and finance for Metro Transit business processes. TXbase transfers financial data to the PeopleSoft Financial system, the system of record for managing procurement for the Metropolitan Council. The TXbase system is also used for time and absence management for Metro Transit Maintenance, Metro Transit inventory, MTS, Community Development, and Regional Administration. All TXbase timesheets are aggregated with absence data managed in the Hastus system for Metro Transit bus and rail operators. Aggregated absence and time entry data entered in TXbase are transferred to the PeopleSoft Human Resource system to process payroll and manage FMLA leaves. The TXbase system has been tailored by a Metro Transit business system manager and Information Services (IS) application developers to facilitate business processes and share information with PeopleSoft systems to keep the Council running smoothly and efficiently.

Within the system, users are assigned unique UserIDs with role-based permissions. Ideally role permissions correlate with the tasks specific to the individual employee's needs to use the system. TXbase role permissions allows the system administrator to assign roles read or write access, along with access to view specific modules (screens) with the system. Inadequate user administration processes could result in unauthorized user access and disclosure of sensitive information. Management of user access is critical for ensuring the integrity and availability of systems and data. The standard operating processes for TXbase are a mix of Metro Transit processes and IS processes and procedures.

Purpose

The purpose of this audit is to determine whether TXbase IT procedures and processes are operating in a manner that is efficient, well-controlled, properly managing major risks, and ensuring appropriate compliance with applicable laws, regulations, policies and industry recommended practices.

This audit also considered the Council's Thrive 2040 Outcomes and Principles. The maintenance of security and controls for the TXbase system is reflected in Thrive 2040's desired outcomes of stewardship and sustainability. Thrive 2040's principles of collaboration and accountability should be reflected in the controls used to administer the TXbase system.

Scope

This audit focused on TXbase system's technology general controls and security infrastructure, including compliance with Metro Transit and IS related policies and procedures, as well as industry best practices in technology governance and IS system management.

Methodology

The following methods of inquiry were used:

1. Interviews with staff including:
    - ➢ Metro Transit staff involved with requisition approval in TXbase
    - ➢ Metro Transit staff involved with payroll approvals in TXbase

    - Metro Transit Managers
    - Information Services staff
2. Review TXbase IT General Controls, and complete testing in standard User Administration Audit Program for:
    - Requisition Approvals
    - Payroll Approvals
    - Password Administration
3. Code Change Management
    - General Review
    - Reviewed leading IT practices including ISO and NIST guidance
4. Continuity of Operations
    - Review TXbase production and database backup and recovery planning
    - Reviewed leading IT practices including ISO and NIST guidance

Assurances

This audit was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and the U.S. Government Accountability Office's Government Auditing Standards.

OBSERVATIONS

User Administration

Metro Transit lacks a formal user administration processes for payroll approval access.

Metro Transit has inadequate controls for periodically reviewing user and system role access for payroll approvals. Within the TXbase system, three access rights within the system are required to allow a user to approve payroll. Audit observed 21 retired and terminated employees that still had access to approve payroll for a job group or cost center. Additionally, the access review observed some active employees who had transferred jobs but had maintained payroll approval authority to a job group or cost center from their previous position. None of the user access issues noted resulted in a user having full access to approve timesheets inappropriately, and no inappropriate timesheet approvals were noted. Per the Business Systems Manager for TXbase, all 21 former employees had their access removed from the payroll approver module in TXbase in response to these audit findings.

When periodic user access reviews are not performed, the potential for unauthorized access increases. This could result in a transferred or rehired employee having access to approve payroll without formal approval to do so. The lack of a periodic review process likely contributed to the inappropriate approval access observed. Audit also found there is not a Metropolitan Council policy or procedure designating who has authority to grant access to approve payroll in Council time management systems, which further complicates user and role review processes.

Metro Transit does not have formal user administration processes for requisition approval access.

Requisition approval authority is delegated by using the Procurement department's *Signature Authority Delegation Form*. When delegating approval authority, the form allows Metro Transit's

General Manager to limit staff to approve requisitions of a specific amount for specific department(s) by designating an approved Cost Center number. Metro Transit then has user administration processes for assigning requisition approval access within the TXbase system. Currently, user administration processes do not include formal documented procedures for entry of approval authority limits and cost centers. When Audit reviewed system access to approve requisitions, we observed that access does not always match approved authority on the *Signature Authority Delegation Form*. For 10 of the 26 (38%) approval authorities reviewed, the TxBase cost centers assigned to the user did not match cost center delegations listed on delegation form. In some instances, approval limits entered in TXbase did not match the limit noted on the delegation form or the MetNet Signature Authority List. Access approval issues could be the result of the lack of comprehensive periodic access reviews. Department business processes have led to the system administrator granting approval authority at a lower limit than is designated on the delegation form, and sometimes to cost centers not explicitly listed on the form. This has allowed managers and senior management to ensure their accountants and supervisors to initially approve requisitions, before the expense is routed to managers in rail, bus, and/or senior managers for approval.

Periodic access reviews of requisition approval authority are complicated by system limitations, as well as the format of the Signature Authority List posted on MetNet. Metro Transit assigns access by TXbase Cost Center, while MetNet Signature Authority List shows designated approvers by project. Within TXbase, a project code is a separate field in the account string, and projects often span multiple Cost Centers at Metro Transit. Additionally, previous TXbase system administrators did not consistently document account terminations and the removal of requisition approval authority in the system. While the current system administrator has been reviewing to confirm terminated employees do not have active requisition approval authority assigned to them, there is no documented process and no reviews beyond deactivating terminated users while leaving approval authority active in the separate TXbase module. There are no comprehensive access review processes to ensure the ongoing need for access that was previously assigned to users.

Some risk is mitigated by the fact that terminated users cannot access the system, which would prevent them from accessing the requisition approval module in TXbase, though such approval authority may be accessible if an employee is rehired. Additionally, the current system administrator completed an audit of terminated employees in TXbase, to confirm that terminated employee accounts were deactivated in TXbase. Without confirming an end date has been entered in the approval module for terminated employees, there is a risk that a rehired employee could retain requisition approval authority. The lack of periodic review processes could result in unauthorized user access and disclosure of sensitive information. Management of user access is also critical for ensuring the integrity and availability of systems and data.

Recommendation

1. **(Essential) Comprehensive access reviews should be performed annually for all TXbase users and roles. Reviews should be performed by managers with knowledge of users' activities and their appropriate levels of access. The review should include confirmation of ongoing appropriateness of users' assignment to system roles as well as the access assigned to those roles.**

   Management Response: *The Business Systems Manager will conduct an annual review of all TXbase user accounts and access levels to ensure all users are in roles with the appropriate functionality to meet their business needs.*

Staff Responsible: *Glenn Gilbert*

Timetable: *March 31, 2019*

Thrive 2040 Principles: *Accountability*

Password requirements for TXbase system passwords do not meet the requirements of the Council's Password Procedure.

Strong passwords are critical for preventing unauthorized access to systems. The TXbase system requires user passwords when a user has opted to not authenticate to the system via their network login. TXbase system password requirements are established for the TXbase access role, and role password requirements are then attributed to a user by the system when roles are assigned. For multiple TXbase roles, password requirements do not meet the Council Password Procedure requirements. Additionally, there is a requirement for complex passwords for sensitive roles. However, passwords for system administrators do not require password expiration or password complexity for TXbase. Weak passwords could lead to a system breach and/or issues with data integrity and availability.

Recommendation

2. **(Essential) Metro Transit should implement strong password requirements for the TXbase System in accordance with the Metropolitan Council's *Password Procedure*. Specifically, Metro Transit should ensure that system administrator accounts meet password complexity requirements as detailed in the Password Procedure.**

   Management Response: *TXbase application password requirements will be adjusted to conform to the Metropolitan Council's Password Procedure.*

   Staff Responsible: *Glenn Gilbert*

   Timetable: *December 31, 2018*

   Thrive 2040 Principles: *Accountability*

Change Management

TXbase system change management processes are informal and do not ensure all changes are formally tested and approved prior to implementation.

IS Application Developers are responsible for code change management for the TXbase system. IS has established some controls over TXbase system changes, such as maintaining separate development and production environments. However, IS and Metro Transit change management processes for TXbase are largely informal and do not ensure that only authorized and tested changes are moved into production. Code change processes do not include formal impact assessments or documented approval of changes by business process owners or Metro Transit management. IS and Metro Transit do not always use a formal tracking mechanism to track changes and approvals. Additionally, there is no formal change control process or formal assessment that designates the appropriate scope of changes that would require the use of a formal change control process. Further, a formal tracking mechanism is not always used to track TXbase changes and approvals and there is no systematic logging of changes to ensure changes follow required processes.

Patch management processes are also informal, though IS is working to include TXbase system patches in the Council-wide patch management process. There is also no documented emergency change process in place for the TXbase system, although IS staff state they have been finalizing the recovery plan that will be necessary to implement any emergency changes. Change management risk is partially mitigated by the fact that system code changes to the user-facing instance of TXbase are automatically logged in a version control system, though the type of change and reason for the change is manually entered by application developers.

Testing for changes is also limited and informal. While code change testing is logged in the development instance of TXbase with documented test notes, the testing documentation available is incomplete and inconsistent. Currently testing documentation maintained is in the form of a help desk ticket, or in the form of a note entered in the version control system. No formal approval of a change after end-user testing is maintained. Furthermore, TXbase does not have a separate test environment, as leading practices would generally require. Instead, all changes are tested in the development environment and migrated directly into the production environment without system generated documentation of developer and end-user testing.

Metro Transit has designated TXbase as a business-critical system, with recovery point and recovery time objectives that make it a high to medium risk system. Unauthorized or inadequately tested system changes could result in data integrity and system availability issues. In addition, industry leading standards specify the need for formal change processes for high and medium risk systems, and specifies requirements for these processes. Log management processes for medium and low risk changes generally require that all developers implementing system changes at least manually log changes, and compensating controls should be implemented to analyze logs for anomalous activity.

Recommendation

3. **(Essential) Metro Transit and IS should develop a single, formal change management process for all TXbase application and infrastructure changes that include formal impact assessments, documented approvals for migration of changes, an emergency change management process, and the use of a ticketing tool or tracking mechanism to ensure authorized and tested changes are moved into production.**

   Management Response: *Currently we have every TXbase application change documented in the Weekly task list, Share point Task list and in RFC – Request for Change (LANDesk). We will immediately begin to store every change in one place (LANDesk) and follow the IS change management process. RFC [Request for change LANDesk] will be the place to document all changes from emergency changes, minor enhancements, data change, major projects, and any new additions. Every change will go through a formal approval process that the IT Application Manager & Business Systems Manager will be responsible for. All major changes will be reviewed by the change management board for approval.*

   Staff Responsible: *Ernie Zahradka, Nagarajan Subramanian*

Timetable: *December 31, 2018*

Thrive 2040 Principles: *Collaboration and Accountability*

4. **(Essential) Metro Transit and IS should establish a test environment for the TXbase system.**

   Management Response: *IS agrees that establishment of a test environment for TXbase is an essential component of its architecture. IS proactively commenced this work in 2018 with development and approval in October of a revised system architecture that includes new test environments for the application.*

   The new test environment is dependent upon procuring the hardware, configuration, upgrading to Sybase version 16, rigorous user acceptance testing, and final implementation of the full Sybase/AIX database system architecture. Information Services plans for completion of this work no later than Q4 2019. Information Services has been working on the possibility of repurposing servers currently used for the WAMO application and incorporating them into a TXbase recovery strategy. If these servers become available, a test environment could be stood up for TXbase within a month or less.

   Staff Responsible**:** *Ernie Zahradka, Nagarajan Subramanian*

   Timetable**:** *December 31, 2019*

   Thrive 2040 Principles: *Collaboration and Accountability*

5. **(Significant) Testing processes for all TXbase application and infrastructure changes should be enhanced. Metro Transit and IS should formally document and retain testing strategies, plans, and results. Testing procedures should include testing performed by end users where appropriate prior to IS migrating the changes into production.**

   Management Response: *We will create a TXbase test server to streamline the test process and this infrastructure change is part of the response to Audit Recommendation 4 above. A TXbase test plan document will be developed to include the details about the screen/module name, process to be tested, personnel responsible, and the results of the testing.*

   Staff Responsible: *E*rnie Zahradka, Nagarajan Subramanian

   Timetable: *December 31, 2019.*

   Thrive 2040 Principles: *Collaboration and Accountability*

6. **(Consideration) Metro Transit should develop logging and monitoring procedures for all TXbase system changes. Any procedures should be in accordance any future Metropolitan Council log management standards. Log management procedures should include: configuring and securing system logs; retaining all logs in compliance with Metropolitan Council retention requirements; developing a log analysis strategy; active monitoring of logs for anomalies; remediating**

medium/high risk anomalies; and documenting actions taken to remediate high risk anomalies. Metro Transit should consider leveraging available tools and resources from IS or ECM when developing and implementing log procedures.

Management Response: *LANDesk is used to track all system changes found in Audit Recommendation 3. Log management requirements are included in the change management process and will be elaborated on when a formal change management standard that is being considered as part of the Technology Governance framework initiative.*

Staff Responsible: *Ernie Zahradka, Nagarajan Subramanian*

Timetable: *Subject to development of new technology standards.*

Thrive 2040 Principles: *Collaboration and Accountability*

Continuity of Operations

Essential System Administration staff lack sufficient backup staff support.

TXbase has one System Administrator along with a Database Administrator and two Application Developers with administrative privileges. A Principal Application Developer in the Transit Systems Unit within Information Services (IS) has responsibility for programming of TXbase. TXbase was acquired in 1996 and the Principal Application Developer was hired at the same time to support the system. The Business Systems Manager in Metro Transit's Strategic Initiatives Department is responsible for managing user accounts and user responsibilities within TXbase. Together the Principal Application Developer and the Business Systems Manager have responsibility for customizing TXbase to meet the business needs of the users.

The Principal Application Developer for TXbase is in the process of training other application developers to serve as backup support. The Business Systems Manager for TXbase does not have an identifiable staff backup. The Business Systems Manager is the sole point of contact for system users. The Business Systems Manager knowledge of the users' business needs and knowledge of the capabilities of TXbase is not replicated among other staff persons. Although the Principal Application Developer is able to assist with the assigning of user responsibilities, the Principal Application Developer is not well versed in the business needs of users. Additionally, the Principal Application Developer at the time of the audit was the sole primary developer supporting TXbase's purchasing module. The critical roles that the Business Systems Manager and Principal Application Developer perform could be lost without sufficient staff backup. The IS department is in the process of training the Primary Application Developer's backup. In response to a 2012 audit finding, the previous Metro Transit Business Systems Manager did document portions of the position responsibilities, but there is no comprehensive documentation of the position's responsibilities and activities or trained backup.

Recommendation

7. **(Essential) All essential staff should have trained backup. The Business Systems Manager for TXbase currently lacks a backup. Backup staff or other means of backup should be identified and trained now, and in the future as staffing changes occur.**

Management Response: *Existing documentation of critical tasks, system interfaces, and routine system administration functions will be expanded and assembled into a format suitable for training and reference. One or more Metro Transit staff will be identified and trained to provide backup for each essential and time-sensitive task. Backup staff will be identified in an online resource and will be reviewed annually. Training will be reviewed annually.*

The IT Application Manager will ensure that an Application Developer III (TXbase) will be tasked and trained to perform 25% of time working on tasks from the TXbase outstanding tasks list. An application Developer IV will be the lead and mentor the Application Developer III if/when needed. In addition, the Application Developer III will also be aware of all changes that the Application Developer IV places in our new builds for TXbase. The Application Developer III already has access to all the front-end and back-end code and will follow the TXbase system change guidelines with monthly check points with the business on the technical side.

Staff Responsible: *Ernie Zahradka, John Levin*

Timetable: *Business Systems Manager backup staff identified by March 31, 2019; training completed by end of September 30, 2019. Application Developer backup in place December 31, 2018.*

Thrive 2040 Principles: *Accountability*

The TXbase system Continuity of Operations Plan is incomplete and does not ensure the security, retention, and recoverability of data.

IS does backup TXbase critical system data on an hourly basis. Backups of data include incremental and full system back up to servers and to disk. Backups of the TXbase database are facilitated by separate, physically remote Sybase servers. The TXbase database is needed to run the front-end application, which underlines the necessity of Sybase database server availability. However, there are a limited number of Sybase servers, which is currently limited to a single production server and a development server. Current recovery planning does not have resiliency for the production and development instances of TXbase.

The TXbase application also relies upon Citrix to distribute the user-facing system needed to use TXbase data to run business processes and timecards. The Citrix application is the mechanism through which TXbase is rolled out to most system users at the Council. The IS department manages Citrix. Citrix relies upon a server farm to run the application. While Citrix servers have very recently been upgraded, the server farm does not have physical redundancy. This risk is somewhat mitigated as currently the Citrix Application is supported by multiple co-located serves, which ensures the application is not dependent upon a single server. However, having the remote physical location of multiple servers helps ensure the continuity of operations and confirms a system is not dependent upon a single site to operate.

The close proximity of the servers in a single location could result in a catastrophic loss of all Citrix mediated systems, including TXbase, if the server farm were ever compromised by a disaster. The catastrophic loss of the co-located servers for both the database and the Citrix application data would impact critical business systems for time management for the Council, as well as maintenance, inventory management, purchasing, and finance functions for Metro Transit. In the event of a more extensive disaster affecting the servers, a backup of the system would from disk data take weeks or months and drastically compromise critical business functions.

In addition to the Citrix application, TXbase relies upon a series of development scripts to run interfaces with other systems like PeopleSoft Financial and the Peoplesoft Human Resource Management System, systems of record for financial and human resource data for the Council. Currently the development scripts for the code required to run these interfaces' is only backed up on a Council computer and a remote hard drive.

A failure to establish adequate server resiliency can affect the availability of the TXbase system, and the ability to test system recovery. In the event of a disaster or adverse event, this could result in system availability issues, which would affect the continuity of operations.

Recommendation

8. **(Essential) IS should implement controls to ensure the recoverability of all systems required to run the TXbase system. Recoverability planning should include recovery testing on an annual basis.**

9. **(Essential) IS should ensure adequate server resiliency for the database and application instances required to run the TXbase system.**

Management Response: *Analysis of controls needed to improve the recoverability of the TXbase system commenced in mid-2018 and will continue through 2019. The scope of this work is multi-faceted and complex, encompassing both the Sybase database system and the Citrix system, and will require technical assessments and architecture recommendations, procurement of additional hardware, and installation and testing of configurations in two data centers.*

The installation of two new Sybase database servers (production at FTH and standby at EDC1) as well as COOP plan development is planned for Q1-2019. In addition, IS plans to take interim steps to improve system recoverability by installing the TXbase application directly on critical users' desktops and on computers in several Council training rooms for rapid access by users if necessary. This work will also be completed in Q1-2019 and result in an improved recovery time of less than 8 hours. This will position IS to move forward in development of a fully resilient Sybase database environment.

Continuity of operations plan (COOP) development for the TXbase system (database and application components) and for the Citrix infrastructure environment is dependent upon system architecture design and implementation. Full resilience/recoverability of the TXbase/Citrix system is planned in Q4-2019 and will be tested at least annually thereafter.

Staff Responsible: *Kathy Matter, Brandt Vettel, Emily Gannon*

Timetable:

• Implement TXbase interim recovery strategy	March 31, 2019
• Implement full Sybase/AIX/Citrix resilience/recoverability	December 31, 2019

Thrive 2040 Principles: *Collaboration and Accountability*

CONCLUSIONS

The TXbase system generally has a strong and collaborative organizational support model that provides effective oversight and coordinates personnel from Metro Transit and the IS department for system management. Metro Transit and IS have implemented some IT general controls to cover previously identified control deficiencies. However, the system administrators have developed management processes for user administration and change management that are informal and lack complete documentation. There are other processes that have yet to implement industry leading practices and require further improvements to minimize risk to data confidentiality, integrity, and availability. User Administration controls need improvement. Change management has implemented some vital controls, but still needs to implement vital IT general controls, including change management approval and testing documentation. The Metro Transit Manger of Business Systems and IS Application Developers have demonstrated they are knowledgeable and continuously looking for opportunities to improve and enhance their operations.

RECOMMENDATIONS

Program Evaluation and Audit recommendations are categorized according to the level of risk they pose for the Council. The categories are:

- **Essential** – Steps must be taken to avoid the emergence of critical risks to the Council or to add great value to the Council and its programs. Essential recommendations are tracked through the Audit Database and status is reported twice annually to the Council's Audit Committee.
- **Significant** – Adds value to programs or initiatives of the Council, but is not necessary to avoid major control risks or other critical risk exposures. Significant recommendations are also tracked with status reports to the Council's Audit Committee.
- **Considerations** – Recommendation would be beneficial, but may be subject to being set aside in favor of higher priority activities for the Council, or may require collaboration with another program area or division. Considerations are not tracked or reported. Their implementation is solely at the hands of management.
- **Verbal Recommendation** – An issue was found that bears mentioning, but is not sufficient to constitute a control risk or other repercussions to warrant inclusion in the written report. Verbal recommendations are documented in the file, but are not tracked or reported regularly.

METROPOLITAN
COUNCIL

390 Robert Street North
Saint Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904
public.info@metc.state.mn.us
metrocouncil.org