TECHNOLOGY AND INNOVATION
MAINFRAME REVIEW
AUDIT 21-16
OCTOBER 4, 2021

City of Tampa
Jane Castor, Mayor

Internal Audit Department
315 E. Kennedy Boulevard
Tampa, Florida 33602
Office (813) 274-7159

October 4, 2021

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: T&I-Mainframe Review, Audit 21-16

Dear Mayor Castor:

Attached is the Internal Audit Department's report on T&I-Mainframe Review.

The Technology and Innovation (T&I) Department has already taken positive actions in response to our recommendations. We thank the management and staff of T&I for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover
Internal Audit Director

cc: John Bennett, Chief of Staff
Dennis Rogero, Chief Financial Officer
Russell Haupert, Chief Information Officer
Eric Hayden, Infrastructure Services Manager
Martin Zinaich, Information Security Officer
Brian Morrison, Assistant City Attorney II

TECHNOLOGY AND INNOVATION
MAINFRAME REVIEW
AUDIT 21-16

/s/ Kevin Hegarty

Associate Auditor

/s/ Patrick Sullivan

Associate Auditor

/s/ Kevin Monaghan

Senior Auditor

/s/ Vivian N Walker

Senior Auditor

/s/ Joel Eshleman

Audit Manager

/s/ Jim Kreiser

Audit Principal

/s/ Lance Schmidt

Audit Principal

/s/ Christine Glover

Audit Director

TECHNOLOGY AND INNOVATION
MAINFRAME REVIEW
AUDIT 21-16

BACKGROUND

The City of Tampa (City) maintains an International Business Machine (IBM) mainframe to support its pension operations. The mainframe environment is complex and requires specialized individuals to maintain its ongoing operations. The City's Technology and Innovation Department (T&I) currently maintains the mainframe and the pension applications continuing to operate within the environment. The City has initiated a process to modernize the mainframe environment by transitioning to newer technologies.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY 2021 Audit Agenda. The objectives of this audit were to ensure that:

1. The system of internal controls related to security and logical access is adequate.

2. The system of internal controls related to change management is adequate.

3. The system of internal controls related to scheduled jobs is adequate.

STATEMENT OF SCOPE

The audit period covered information technology activities that occurred from January 1, 2021, to June 30, 2021. Tests were performed to determine whether T&I personnel were fulfilling their stated duties and responsibilities in an effective and efficient manner. Original records as well as copies were used as evidence and verified through observation and physical examination.

STATEMENT OF METHODOLOGY

The following steps were performed in order to determine the accuracy, consistency, and relevance of controls:

1. Inquired (of management) about the control activities and processes performed to support the mainframe and pension applications.

2. Inspected available policies and operating procedures to document the control activities and processes.

3. Inspected supporting documentation to determine the operating effectiveness of control activities.

4. Inspected system reports to validate system configurations.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

NOTEWORTHY ACCOMPLISHMENTS

T&I should be commended for having well designed and operating controls, while maintaining lean staffing.

AUDIT CONCLUSIONS

Based upon the test work performed and the audit findings noted below, we conclude that:

1. The system of internal controls related to security and logical access is adequate. However, improvements related to system support, naming conventions, encryption, and access are needed.

2. The system of internal controls related to change management is adequate. However, policies and procedures need to be updated.

3. The system of internal controls related to scheduled jobs is adequate. However, the disaster recovery plan needs to be updated.

UNSUPPORTED IBM OPERATING SYSTEM (Z/OS) AND IBM RESOURCE ACCESS CONTROL FACILITY (RACF)

STATEMENT OF CONDITION: The current version of the z/OS operating system and the RACF installed on the mainframe at the City of Tampa is no longer supported by IBM. The current version of z/OS (2.2) and RACF (HRF77A0) ended support from IBM on September 30, 2020.

CRITERIA: All software should be updated to a level that is currently supported by the vendor.

CAUSE: In order to update the operating system and RACF, new mainframe hardware would need to be purchased and upgraded.

EFFECT OF CONDITION: If the City encounters problems or errors within the mainframe environment and requires additional support from IBM to resolve the issue, the City may be required to pay additional consulting fees to IBM to research and resolve the issue.

RECOMMENDATION 1: We recommend that the City develop a definitive upgrade and system retirement path that will allow for an accurate evaluation on the cost/benefit analysis to decide the need to maintain the mainframe environment.

MANAGEMENT RESPONSE: We agree and are engaged in removing all remaining systems per the retirement plan underway. The current hardware does not support a higher version of the z/OS operating system and the RACF. It is cost prohibitive to obtain a new mainframe that has approximately six (6) months remaining use. We estimate completing the project June 1, 2022.

TARGET IMPLEMENTATION DATE: Per Plan, Fire & Police Pension will start parallel processing of Pension Gold System Oct-Dec 2021 with go-live Jan 1, 2022. General Employee Pension will start parallel processing of Pension Gold System Feb 2022 with go-live April 1, 2022. Mainframe to be retired by June 1, 2022.

REAL DATA SET NAME

STATEMENT OF CONDITION: Access Control Facility 2 (ACF2) and RACF are software modules in the Mainframe system that provide the tools to manage user access to critical resources. The Real Data Set Name (RDSN) option in RACF allows the system to identify real data names on log printouts and operator messages instead of data set names created at the time of install. This RDSN option is also required in order to conform to RACF naming conventions. Currently, the RDSN in RACF is set to inactive in the system's Set RACF Options List command.

CRITERIA: The z/OS Security Server RACF Security Administrator's Guide states that the Real Data Set Name option should be set to active.

CAUSE: During the conversion from ACF2 to RACF, the RDSN setting value in RACF was not evaluated as there was not a corresponding value/setting in ACF2.

EFFECT OF CONDITION: Not setting the Real Data Set Name option to active would only allow the modified data set name to conform to the RACF naming conventions in log records or operator messages, instead of the City assigned data set name.

RECOMMENDATION 2: We recommend that the City evaluate the impact of changing the Real Data Set Name option to active on its operations.

MANAGEMENT RESPONSE: We agree and are engaged in removing all remaining systems per the retirement plan underway. Due to the system being retired within the next 6 months – the RDSN option will not be implemented due to being not advisable to make this level of change to an unsupported system while the pension project is coming to its closure.

TARGET IMPLEMENTATION DATE: Fire & Police Pension will start parallel processing of Pension Gold System Oct-Dec 2021 with go-live Jan 1, 2022. General Employee Pension will start parallel processing of Pension Gold System Feb 2022 with go-live April 1, 2022. Mainframe to be retired by June 1, 2022.

ACCOUNTS WITH SELECTED ATTRIBUTES

STATEMENT OF CONDITION: During the review of accounts listed in the Selected Attributes Report in the Data Security Monitor, rights for three of the accounts with access to SPECIAL AND OPERATIONS ATTRIBUTES could not be evaluated as necessary.

CRITERIA: The SPECIAL and OPERATIONS attributes provide users and accounts elevated privileges that should only be assigned based on a business justification. The SPECIAL attribute gives the user complete control over all the RACF profiles in the RACF database and authority to issue all RACF commands, except those reserved for the auditor's use. The OPERATIONS attribute gives the user authority to perform maintenance operations and provides full authority to access RACF-protected Data Access Storage Device data sets and certain resource classes.

CAUSE: Accounts were created for specific purposes and supporting documentation for the access was not maintained nor was the account deactivated when the purpose was no longer valid.

EFFECT OF CONDITION: Providing users and accounts with access in excess of that needed to perform assigned responsibilities increases the risk that unauthorized transactions could be performed and go undetected.

RECOMMENDATION 3: Management has reviewed the accounts in question and adjusted their access based on the findings. The auditor has not validated their adjustments to access. Procedures should be established to ensure no future occurrences.

MANAGEMENT RESPONSE: We agree. During the review of the mainframe accounts – the cause from above was accurate. The accounts identified have already been revoked and no longer accessible.

TARGET IMPLEMENTATION DATE: Implemented as of August 1, 2021

MAINFRAME ENCRYPTION

STATEMENT OF CONDITION: An encryption methodology for the mainframe and its connections has not been developed. Communications protocols between the emulator and the mainframe do not use an encrypted channel to transmit data. Additionally, the data at rest on the mainframe has not been encrypted.

CRITERIA: Encryption should be deployed to ensure confidentiality by concealing the content of stored data as well as the content of messages during transmission. Encryption protects privacy, prevents identity theft, allows files to be securely shared, and protects lost or stolen devices. Numerous information technology standards have established requirements for data encryption.

CAUSE: The mainframe is not connected to the network; therefore, the City has not implemented encryption on it.

EFFECT OF CONDITION: Not deploying an encryption increases the risk that information can be accessed or disclosed to unauthorized individuals.

RECOMMENDATION 4: We recommend that the City develop a definitive upgrade and system retirement path that will allow for an accurate evaluation on the cost/benefit analysis to decide the necessity to maintain the mainframe environment as it relates to encryption.

MANAGEMENT RESPONSE: We agree and are engaged in removing all remaining systems per the retirement plan underway. Due to the system being retired within the next 6 months – the encryption technology will not be implemented due to being not advisable to make this level of change to an unsupported system while the pension project is coming to its closure.

TARGET IMPLEMENTATION DATE: Fire & Police Pension will start parallel processing of Pension Gold System Oct-Dec 2021 with go-live Jan 1, 2022. General Employee Pension will start parallel processing of Pension Gold System Feb 2022 with go-live April 1, 2022. Mainframe to be retired by June 1, 2022.

PERIODIC ACCESS REVIEW

STATEMENT OF CONDITION: While a periodic access review is performed to validate that pension application users are active employees it does not validate that the access assigned to a user aligns with their job responsibilities.

CRITERIA: User Access should be reviewed periodically to ensure that employees have appropriate access and that terminated users are removed.

CAUSE: A standard operating procedure or process has not been developed to include user access rights as part of the periodic access review.

EFFECT OF CONDITION: Employees could have access to systems or applications that may not be appropriate.

RECOMMENDATION 5: We recommend that management include the review of the user access rights in their periodic access review.

MANAGEMENT RESPONSE: We agree with the recommendation that a periodic access right level review be established.

TARGET IMPLEMENTATION DATE:
User access level report creation – 11/01/2021

Access level review procedure formalized documentation – 11/01/2021

Implementation of access level review – 11/30/21

POLICIES AND PROCEDURES

STATEMENT OF CONDITION: A complete set of policies and procedures have not been developed to support the operation of the mainframe environment. While specific policies and procedures have been development for the granting and modifying user access, the following policies and procedures have not been documented:

- Change Management: Processing requirements for authorizing, testing, and approving change requests.
- Computer Operations: Processing requirements for backup procedures and handling of scheduled job failures.

CRITERIA: Information Technology (IT) policies and procedures should include standards for system access (onboarding, offboarding, change management, and computer operations) to guide system administrators and operators on the expectations and approved process for supporting the mainframe.

CAUSE: The City has not formalized or documented standard procedures that it is already utilizing.

EFFECT OF CONDITION: A lack of formalized policies and procedures can lead to an incomplete understanding of the IT environment and its functionality.

RECOMMENDATION 6: We recommend that management create policies that outline the proper guidelines and procedures for change management, and computer operations.

MANAGEMENT RESPONSE: We agree the actual mainframe environment has recently deviated from system documentation.

There are a variety of procedures that the Operations staff are well versed in controlling change management, backup/recovery, and job abend procedures. Common in the industry, specific Job abend and restart instructions are documented within the actual scheduling system and not in an external book. This is because if the scheduling system is not available, we cannot run the jobs or address the abends and external documentation would not yield a benefit and would be quickly outdated. As systems have been fast tracked and retired from production, our system documentation is pending these updates. With the single remaining application, Pension, we acknowledge that the current system documentation has not been updated and needs to be more formalized to address this inquiry.

To complete necessary remediation, we will do the following:
We have implemented a new turnover process that replaces the Librarian functions for Operations. The change management process for programs/JCL is still under the control of the application team and the team lead for migration from test to production. The changes are documented in FootPrints and that ticket number is referenced in the turnover request. There is an email thread that shows the approval processes from team lead to Operations.

The backup procedures are handled in separate processes. System backups are completed by the Operations staff on pre-determined time frames whereas the application backups are performed based on the requirements the application team lead has designated. These procedures will be formalized and submitted for review by management.

The scheduled job failures for application JCL is documented within the Control-M modules – with step by step instructions for restart/recovery/restore/notifications. We will select samples from within the Control-M system to be used for formal documentation of the job failure response process. For non-application JCL (system) the Operations run sheets will be formalized and documented for restart/recovery/restore/notifications. These procedures will be formalized and submitted for review by management.

TARGET IMPLEMENTATION DATE: November 1, 2021

DISASTER RECOVERY

STATEMENT OF CONDITION: The City has documented the disaster recovery steps necessary to restore the mainframe to operations in the event of an incident that limits or eliminates the mainframe processing environment. However, the document did not indicate that it had been reviewed or updated since 2019 and it was referencing a previous operating system.

CRITERIA: The Disaster Recovery Plan should be reviewed and updated annually to ensure that it is up to date in the event that it needs to be implemented.

CAUSE: The current Disaster Recovery Plan has not been reviewed or updated during the past year.

EFFECT OF CONDITION: Not having a current Disaster Recovery Plan in place can limit the City's ability to restore necessary systems and applications in a timely manner.

RECOMMENDATION 7: We recommend that the City review the disaster recovery plan on an annual basis to ensure that it is current and include a versioning section to evidence the review.

MANAGEMENT RESPONSE: We agree as we froze plan updates during the end-of-service mainframe transition project underway. This specific documentation has not been updated since 2019 as this was originally the early timeframe planned for retiring the equipment.

TARGET IMPLEMENTATION DATE: November 1, 2021 – documentation will be reviewed and appropriate changes if/where necessary reflecting the current mainframe portions of the disaster recovery plan for its final period of planned operation.