User Access Audit

March 2022

City of Baton Rouge **Parish of East Baton Rouge**
Finance Department **Internal Auditing Division**
P.O. Box 1471 **Baton Rouge, LA 70821**
Phone (225) 389-5159 **Fax (225) 389-8639**
www.brla.gov

Department of Finance
Internal Auditing Division

City of Baton Rouge
Parish of East Baton Rouge

222 St. Louis Street
Post Office Box 1471
Baton Rouge, Louisiana 70821

(225) 389-3076
Fax (225) 389-8639

March 28, 2022

MEMORANDUM

TO: Darryl Gissel, Audit Committee Chairman
LaMont Cole, Audit Committee Member
Linda Hunt, Audit Committee Member
Ashley Beck, Audit Committee Member

FROM: Barbara Baughman
Auditing Manager

SUBJECT: **USER ACCESS AUDIT**

Enclosed is our report on the User Access Audit. The audit was conducted in accordance with our annual work program. This report presents all audit issues and corresponding recommendations.

The Internal Auditing Division will conduct a follow-up review regarding implementation of corrective action. The results of the follow-up review will be reported to the Audit Committee.

We would like to thank the Information Services Department management and staff for their assistance during the audit.

Barbara Baughman

Barbara Baughman
Auditing Manager

TABLE OF CONTENTS

CHAPTER ONE - BACKGROUND, OBJECTIVES, SCOPE, & METHODOLOGY

BACKGROUND

Per the Annual Operating Budget, the Information Services (IS) Department is dedicated to improving City-Parish operations by providing effective, efficient, reliable, and sustainable technology services. IS provides support for enterprise systems, local systems, local area networks, geographical information systems, and the City-Parish's wide area network.

The Budget also says the Human Resources (HR) Department's goal is to support the Mayor-President and City-Parish departments as they recruit, retain, and train a talented diverse workforce that efficiently meets the needs of the public.

The Munis Payroll module is part of the BRIDGE project that replaced the legacy Financial and Payroll systems. The legacy system was over 22 years old and had become difficult to maintain including its capability to capture data and create required reports. Munis is a web-based system maintained by IS that was introduced in two phases. Phase I – Financials, Procurement, and Inventory (financials) went live in October 2017. Phase II – Human Resources, Recruiting, and Payroll (payroll) went live October 2018.

ExecuTime is the new City-Parish software that provides payroll processing, time entry, and benefits accrual tracking. Using ExecuTime, employees can enter and track time types, manage time-off requests, and apply job costing. The system also includes electronic time sheet approvals.

OBJECTIVES

The objective of this audit was to determine that controls over access to the payroll and timekeeping systems are adequate, access is limited to valid users, and roles and permissions are appropriate.

SCOPE AND METHODOLOGY

The scope of the audit included current users of the payroll and timekeeping systems, current practices for user access management, and transactions from November 2019 through January 2020. To accomplish audit objectives, we performed the following:

- Interviewed IS, HR, and user departmental staff to review controls for user access management;
- Verified validity of system access for a sample of Munis logins on a business day and a weekend day; we were unable to verify failed login attempts due to the lack of a Munis system log;

- Evaluated transaction controls for a sample of Munis payroll module user account creations and revisions to ensure proper authorizations and controls over requests, that creations and revisions were performed by valid employees within the scope of their job duties, that requests were supported by proper documentation, and that creations and revisions were in compliance with City-Parish policies and procedures.
- Evaluated access for a sample of Munis payroll module users to ensure that users are valid employees, that roles and permissions align with the users' job duties, and that access was properly requested, approved, and assigned; we could not confirm users' last login due to Munis' lack of a system log; and
- Evaluated access for a sample of ExecuTime users to ensure that users are valid employees, that roles and permissions align with the users' job duties, and that access was properly requested, approved, and assigned; we could not confirm users' last login due to system limitations.

CHAPTER TWO - AUDIT ISSUES

SYSTEM ACCESS

Munis does not include a system log that captures successful or failed logins. Best practices state logging user identities, their access rights, and the functions they perform in the application provides the organization with a means to examine unauthorized attempts to perform certain functions by registered or unregistered users.

Per IS, in order to access Munis, a user must be enabled in a City-Parish active directory and have Munis roles and permissions. Our sample of program activity found that all users were City-Parish employees who were included in a City-Parish active directory.

CONTROLS OVER IS TRANSACTIONS FOR USER ACCOUNTS

Munis Authorization forms were not available for review for changes made to users' roles and permissions by IS staff for seven of twenty (35%) sample users. In two instances, emails, rather than authorization forms, were on file and in five instances no documentation was on file. One email request was from a departmental payroll supervisor requesting permissions for a division manager. The payroll clerk would not be the manager's supervisor. Proper separation of request and authorization could not be confirmed for the other five requests where no documentation was on file. However, all sample users were valid employees and all changes to access were made by IS staff in the scope of their job duties.

IS does not have written policy or procedures for their process of adding or revising users' roles and permissions or for their requirements for providing security and access to ExecuTime and Munis. Although IS issued a security policy for users in 2020 detailing the end user's responsibility for Munis security, it does not include guidance for IS staff.

The Munis Security Authorization form requires Departmental approval by "Admin" or "Supervisor", however, there is no definition of "Admin". Additionally, there is no confirmation by IS as to whether the person signing the form has the departmental authority to sign the form.

USER ACCESS

Munis Payroll

Authorizations

Authorizations were not on file with IS for roles and permissions assigned to 12 of 14 user accounts. Assignments for the 12 accounts were made by Tyler Technologies or IS staff during the implementation of Munis financials and Munis payroll. Changes were made after the

implementations for two additional accounts. Four of these accounts had the Munis administrator role and eight had roles with limited access. During implementation, Tyler Technologies and IS assigned roles based on the users' permissions in the legacy system or on the permissions needed for IS and Tyler Technologies staff.

The City-Parish Security Policy states a Munis Security Authorization form must be completed for all new users and for changes to the status of existing users. In addition, the Munis Financials Go-Live Kit states that the approved security form should be submitted to the BRIDGE team via email.

Internal Auditing confirmed that role additions to user accounts were made by Tyler Technologies or IS staff within the scope of their job duties. Additionally, role assignments aligned with users' job duties.

Users Accounts

Two sample user accounts in Munis with Administrator permissions are assigned to generic system accounts. These accounts were created by and are used by Tyler Technologies. The accounts are not linked to a specific employee. The other 14 sample user accounts are linked to valid employees. The last login for these accounts could not be confirmed because Munis does not include a system log that captures logins.

ExecuTime

ExecuTime security does not allow a user to have permission to input data for one location and permission to view data for all locations. These permissions are setup in categories which results in a user being able to input for all locations viewed.

Access Reviews

IS does not periodically confirm users' roles and permissions in Munis or ExecuTime with the users' departments to ensure continued validity of the user or the role. The external auditors recommended user reviews of all systems should be performed annually per the 2017 Report to Management.

The City-Parish Security Policy states supervisors are responsible for notifying the BRIDGE team whenever an employee is terminated or transferred so access can be modified or cancelled. However, IS stated that they are not always notified.

CHAPTER THREE – RECOMMENDATIONS

Internal Auditing recommends the following to address the issues noted in the audit:

1. Information Services should have the software developer create a report to document failed login attempts that captures the user's name and the date and time of the attempt. IS should review the report on a regular basis to monitor for potential problems.

2. Information Services should only complete requests for access or revisions of access that are properly authorized. Request documentation should be maintained on file.

3. Information Services should create policies and procedures detailing their process and requirements for assigning, reviewing, and terminating users' roles and permissions in ExecuTime and Munis.

4. Information Services should have departments submit a list of employees that are authorized to approve Munis Security Authorization forms. They should compare authorizations to the list prior to completing transactions for users' access.

5. The Information Services Director should review and approve all accounts with Administrator access.

6. The Information Services Director should determine if the generic system user accounts are still necessary and have the appropriate permissions. He should determine if a unique user account would meet requirements and provide additional accountability.

7. Information Services should consult with the ExecuTime developer to determine if updates are available that allow more detailed management of security.

8. Information Services should obtain authorization and confirm permissions for current Munis users with users' departments. Information Services should then continue to review and confirm roles and permissions periodically or at least annually.

CHAPTER FOUR – EXIT CONFERENCE

We held an exit conference on March 9, 2022 with the following persons in attendance:

- Eric Romero, Information Services Director
- Gail Wilcox, Information Services Project Manager
- Barbara Baughman, Auditing Manager
- Andrea George, Chief Auditor

The contents of the report were fully discussed.

CHAPTER FIVE – AUDITEE RESPONSE

See next page.

Department of Information Services

City of Baton Rouge
Parish of East Baton Rouge

222 St. Louis Street Rm. #B284
Baton Rouge, Louisiana 70802
Office: (225) 389-3262
Fax: (225) 389-7745

To: Barbara Baughman, Auditing Manager

From: Eric Romero, Director of Information Services

Date: March 28, 2022

RE: Management response to User Access Audit March 2022

The Department of Information Services has received, and reviewed with Finance Auditing, the User Access Audit – March 2022 report. Information Services understands and agrees with all recommendations made in the report and will work towards the addressing each recommendation.