OpenVMS Payroll
Module Access Audit
November 2020

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

November 2, 2020

MEMORANDUM

TO: Darryl Gissel, Audit Committee Chairman
Scott Wilson, Audit Committee Member
Linda Hunt, Audit Committee Member
Ashley Beck, Audit Committee Member

FROM: Barbara Baughman
Auditing Manager

SUBJECT: OPEN VMS PAYROLL MODULE ACCESS AUDIT

Enclosed is our report on the audit of Open VMS Payroll Module Access. 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 recommendations. The results of the follow-up review will be reported to the Audit Committee.

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

Barbara Baughman

Barbara Baughman
Auditing Manager

TABLE OF CONTENTS

CHAPTER ONE - BACKGROUND, OBJECTIVES, SCOPE, & METHODOLOGY

BACKGROUND
OpenVMS is a general-purpose, multi-user virtual memory-based operating system. Prior to the implementation of the Munis Human Resources module in 2018, the Open VMS payroll module was used by the City to maintain and process payroll and personnel transactions. The module also integrated with another software, Secure 32, to print payroll checks. The Open VMS payroll module is currently used to update and track non-Munis applicant hiring restrictions and as a reference for approximately 22 years of historical personnel and payroll data.

Security to the Open VMS payroll module is controlled by access to the City's network, access to the Open VMS operating system, and additional access to the Open VMS payroll module. Information Services is the administrator of the City's network and the Open VMS operating system. Human Resources is the administrator of the Open VMS payroll module. Access to the payroll module includes permissions to inquire, add, change, delete, or maintain security for various screens within the module, which includes all permissions.

OBJECTIVE
The audit objective was to determine if access to the Open VMS payroll module was limited to valid users and if users' permissions were consistent with their job duties.

SCOPE AND METHODOLOGY
The scope of the audit included user accounts that were active as of January 21, 2020. We performed the following tasks to accomplish our objective:
- Interviewed Information Services, Human Resources, and Finance-Accounting staff; and
- Identified accounts with permissions to change, add, delete, or maintain security and confirmed the following:
    - The employee was active; and
    - The employee's job duties aligned with their payroll module permissions.

CHAPTER TWO - AUDIT ISSUES

ACCESS AND SECURITY
Open VMS payroll module accounts were not limited to valid users and users' permissions were not consistent with their job duties.

Two of 19 user accounts (11%) with broad permissions belonged to inactive employees. One employee, a Student Intern, had permissions to "Change Demographic Information" and the second employee had permissions to "Delete" records. One employee resigned in December 2018 and the other in August 2019. Although the Open VMS payroll module accounts were active, the department had notified Information Services staff of their resignations. Information Services removed their access to the City's network, therefore, the inactive employees no longer had access to the first step in accessing the Open VMS payroll module.

Open VMS payroll module security policies require supervisors "to notify the security administrator immediately whenever an employee is terminated or transferred so the employee's passwords and other access privileges can be modified or cancelled". In these two instances, the Payroll Module Administrator was not notified. Also, the Payroll Module Administrator does not have a process to periodically review payroll module security or to ensure that departments are following security policies.

Job duties for eight of the 19 users (42%) did not align with their security. Five users had the capability to "Change Demographic Information". Three accounts included "Security Maintenance" permissions which allowed the user to add, change and/or delete information. Their job duties do not require permissions other than an inquiry capability.

Recommendations:
The Open VMS Payroll Module Administrator should deactivate the inactive employees' accounts.

The Open VMS Payroll Module Administrator should immediately confirm the employee status and appropriate security for all users and update their security permissions accordingly.

The Open VMS Payroll Module Administrator should ensure that information is available on the Metronet or in another accessible format to inform supervisors of who to contact and how to proceed to deactivate a user's account.

The Open VMS Payroll Module Administrator should establish a process to periodically review and confirm employee status and appropriate security permissions for all users.

CHAPTER THREE – EXIT CONFERENCE

An exit conference was held on October 15, 2020 with the following persons attending: Pat Guidry, Information Services Project Manager, Barbara Baughman, Auditing Manager, and Andrew McNicoll, Auditor. All issues and recommendations were discussed.

A second exit conference was held on October 16, 2020 with the following persons attending: Michelle Longino, Human Resources Division Manager, Brian Bernard, Human Resources Director, Barbara Baughman, Auditing Manager, and Andrew McNicoll, Auditor. All issues and recommendations were discussed.