Jefferson Wells™
ManpowerGroup

City of Milwaukee Employes' Retirement Services

Information Technology General Controls (ITGC) Audit

DECEMBER 8, 2020

JEFFERSON WELLS
RISK ADVISORY SERVICES
WISCONSIN OFFICE

This report is intended solely for the use of ERS and is not intended to be and should not be used by any other parties without the prior written consent of Experis Finance.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

PROCEDURES PERFORMED 4

This report is intended solely for the use of ERS and is not intended to be and should not be used by any other parties without the prior written consent of Jefferson Wells.

EXECUTIVE SUMMARY

Background

At the direction of the Administration and Operations Committee, the IT General Controls (ITGC) Audit was completed to cover the period January 2020 – November 2020. The audit reviewed controls within the IT environment which includes logical access, change management and data center operations. The primary application used by most business areas is MERITS which is used to manage multiple aspects of pension funds. Additionally, Microsoft technology is used for network access and user operating systems.

Audit Objectives & Scope

The objective of the audit was to determine if controls where in place for information systems, and management was able to provide evidence on completing the controls. The scope included the following areas:

- Network Logical Access for Windows Active Directory and MERITS Application

  [redacted]

- Change Management

  [redacted]

- Data Center & Network Operations

  [redacted]

Various audit techniques were utilized to assess and examine the effectiveness of the ERS IT control environment. Audit techniques included conducting interviews with ERS personnel, evaluating completeness of policies and procedures, and reviewing other pertinent reports and supporting documentation. See the Procedures Performed section of this report for detailed testing performed.

Overall Assessment

The IT environment continues to have controls and processes in place for logical access, change management and operations. The application portfolio remains consistent (primarily MERITS) and there were no major changes introduced for the period under review. During the COVID 19 pandemic, ERS successfully deployed technology solutions to employees to allow remote access to key applications. **<u>There were no issues identified during the testing</u>**.

Audits are only one part of a comprehensive risk management and control program. This report is provided with the objective to assist the Board, Audit Committee and Management in the effort to eliminate, reduce or mitigate overall risks. These have all been discussed with management during the assessment as identified.

This report is intended solely for the use of ERS and is not intended to be and should not be used by any other parties without the prior written consent of Jefferson Wells.

PROCEDURES PERFORMED

Processes and items audited or reviewed within IT included the following, but were not limited to:

- Reviewed high level network diagrams to determine if a layered structure is in place to protect applications and data.
- Reviewed policies and procedures related to employees working remotely due to the COVID 19 pandemic.
    - Remote Access Policy – Based on review of the policy, determined there are security standards for connecting to the ERS network and for computers that are allowed to connect remotely to the organizational network. The policy specifies how remote users can connect to the organization's resources and the requirements each system must meet before connecting. It is designed to allow flexibility for users to work outside ERS' offices while preventing damage to the organization's network or computer systems.
    - Virtual Private Network (VPN) Access – Reviewed user listing of individuals with VPN access and determined permissions where appropriate
    - Password Policy – Based on review of the policy, determined there is a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.
        - Reviewed password settings for the network and determined they are aligned with the policy.
- Reviewed monitoring procedures and collected evidence for servers, VM's, interface connections and other network devices.
- Reviewed a sample of 20 infrastructure changes, non-infrastructure changes, system/database changes, and emergency changes for adherence to the Change and Patch Management procedures to determine if changes were occurring as management intended.
- Reviewed user access provisioning procedures to determine whether access was granted after management's approval and removed timely when a business need no longer existed. Tested 3 new and 2 terminated employees' access to verify access was either approved or removed in a timely manner.
- Reviewed the minutes from the bi-annual user access review on 9/24/2020 to determine if the review was completed and included relevant applications and/or security groups.
- Reviewed MERITS data replication configuration and determined the replication is occurring as intended.

This report is intended solely for the use of ERS and is not intended to be and should not be used by any other parties without the prior written consent of Jefferson Wells.