City of Milwaukee Employes' Retirement Services

Information Technology General Controls (ITGC) Audit

MARCH 10, 2016

EXPERIS FINANCE
RISK ADVISORY SERVICES
WISCONSIN OFFICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

At the direction of the Administration and Operations Committee, the IT General Controls (ITGC) Audit was completed February 10, 2016 – February 24, 2016. An ITGC review attempts to gain an overall impression of the controls that are present in the environment surrounding the information systems. An ITGC audit reviews controls over the Information Technology environment, computer operations, access to programs and data, and program changes.

Audit Objectives & Scope

The objectives of the audit were to determine the level of controls within the environment surrounding information systems including:

- Logical Access Security Controls are defined and operating effectively
- Change management controls are defined and used consistently
- Data Center and Network Operations controls are defined and used effectively
- Controls have been designed in the IT environment for network security

The determination is that the general controls encompass the entire ERS environment and MERITS is the primary application. Although other applications exist, testing should be deemed reliable as long as the overlaying general controls are applied and functioning properly. Therefore, the scope was determined to be Windows Active Directory and MERITS logical application access.

Design and Operating Effectiveness Testing of:

- Logical Access Security (Windows Active Directory (AD) and MERITS application user access)
  - Access / Authentication Security
  - Privileged Users
  - Default User IDs
  - Generic User IDs
  - Periodic review of User IDs
  - Remote Access
- Change Management
  - System/database changes
  - Emergency changes
  - SDLC changes
- Data Center & Network Operations
  - Monitoring
  - Logging
  - Emergency procedures
  - Environmental controls
  - Access (physical and logical)

Controls have been designed in the IT environment for:

- Network Diagrams
- Monitoring and Logging
- Patch Management
- Malicious Software Management
- Router Management
- Firewall Management
- IDS/IPS Management
- Wireless Management
- Incident Response
- Facility Physical Security
- Environmental Management (UPS, Generator, HVAC)
- Encryption
- Information Security Program
- Risk Assessment
- Configuration Management

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

ERS management has implemented controls to manage general controls for the IT environment. Based on the results of our review, **no internal control deficiencies** were noted.

PROCEDURES PERFORMED

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

- Reviewed network diagrams for layered protection of the network.
- Reviewed monitoring procedures to determine if they exist and were followed for servers, interface connections and other network devices.
- Reviewed a sample of 30 changes; 24 system/database changes, 4 emergency changes and 2 SDLC changes for adherence to the Change and Patch Management procedures to determine if changes were occurring as management intended.
- Reviewed anti-virus policy to determine if one exists and reviewed a report of current signature files to determine anti-virus software is current on user's desktops.
- Inquired if firewall review procedures exist and whether a firewall review was performed.
- Reviewed incident response and intrusion detection procedures. Inquired whether any incidents occurred and were documented as required.
- Reviewed wireless security policy and configuration procedures to determine if they exist and if procedures enforce policy requirements.
- 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 four terminated employees to verify access removal in a timely manner.
- Reviewed user access review procedures for the network and application to determine if reviews are being completed and documented as required by procedures.
- Reviewed data backup procedures and backup job monitoring procedures to determine they existed and followed existing procedures.
- Reviewed job monitoring procedures to determine if they existed and followed existing procedures
- Reviewed data center room physical security and environmental controls to determine whether access to the data center is controlled and that the data center is protected from environmental risks.
- Compared the Password Policy requirements to the password configuration in Group Policy to assess whether the policy settings were configured as management intended.