

City of Milwaukee Employees' Retirement System

IT Risk Assessment Report

MARCH 2010

JEFFERSON WELLS
330 EAST KILBOURN AVENUE, SUITE 1075
MILWAUKEE, WI 53202
(414) 347-2345

KATHY PORTH, PROFESSIONAL
JACK BULLIS, ENGAGEMENT MANAGER
CONNIE McDONALD, RISK ADVISORY SERVICES DIRECTOR

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
Scope.....	3
Conclusion.....	3
RISK ASSESSMENT PROCESS	4
Procedures Performed	4
Risk Assessment Methodology	4

EXECUTIVE SUMMARY

Scope

At the direction of City of Milwaukee Employees' Retirement System (ERS) management, Jefferson Wells performed a high level risk assessment of the risks associated with the various IT areas of ERS. The purpose of the assessment was to develop a three year risk-based IT internal audit plan.

In performing the risk assessment, various procedures were carried out by Jefferson Wells in order to gain an understanding of the policies and procedures that have been implemented at ERS as well as the current IT risks faced by ERS. Although no detailed internal audit testing was performed, the current internal IT control structure was reviewed, and any gaps or weaknesses identified in this structure were provided to management in a confidential appendix to this report.

Conclusion

This report comprises the process used for performing the IT risk assessment. A confidential appendix was provided to management that included a proposed three year internal audit plan for 2010 through 2012 and certain control enhancements and recommendations for improvement that were identified during the risk assessment process.

RISK ASSESSMENT PROCESS

Procedures Performed

The following procedures were performed as part of the IT risk assessment. All procedures were performed between January 4 and January 22, 2010.

- Met with Management in order to obtain their input regarding risks currently faced by ERS.
- In order to understand the ERS current control environment, IT internal control questionnaires were completed for the processes listed below. These were completed through inquiry of ERS personnel and review of relevant documentation.
 - Physical and Environmental Controls – including physical security of the ERS building, computer rooms, and off-site storage areas.
 - Information Security Controls – including maintenance and management approval of the information security program. Staff training for information security was also reviewed.
 - Application Security Controls – including application security/controls, workstation/laptop security, service level agreements, application training, software purchasing, program development, application documentation, application logging/monitoring, and application change management.
 - Operating System (OS) Change Management Controls – including OS change control procedures, patch management, logging, and security settings.
 - Business Resumption Planning Controls – including a review of the business impact analysis and business continuity plan, maintenance procedures for the plan, and testing performed.
 - Hardware Change Management Controls – including a review of hardware acquisition, implementation, and maintenance controls.
 - Network-based Controls – including general user access controls, network support, network logging and patching, encryption, wireless controls, dial up controls, and external network controls.
 - Operations Management Controls – including performance monitoring, job management, backup/media management, help desk procedures, and software/hardware inventories.
 - Administrative Controls – including HR procedures, strategic planning, budgeting, risk self-assessment, and vendor management.
 - Incident Response – including a review of the incident response plan, the maintenance of the plan, and testing performed.

Risk Assessment Methodology

The following steps were performed in completing this IT Risk Assessment:

1. Gained an understanding of key IT areas and procedures through employee interviews and review of various documents provided by ERS staff.
2. Ranked the key IT areas of ERS as listed in Procedures Performed by degree of risk. The risk was determined from analyzing threats to, and vulnerabilities of, an information system and the potential impact that the loss of information assets or capabilities of a system would have on ERS or its customers and business partners. The levels of risk used were:
 - A “*high*” degree of risk may be defined as any risk that may materially impact the continued availability of the computing environment, the integrity of information assets, or the security of the information assets processed. ERS may be impacted if “high risk” areas are not controlled.
 - A “*medium*” degree of risk includes risks that cause intermediate term delays in service processing, typically one to five days in length. Such risks may not be preventable, detectable, or correctable on a timely basis.
 - A “*low*” degree of risk includes risks that may cause short delays in service processing but have a reasonable chance of being prevented, detected, or corrected quickly.
3. Assessed the overall level of control for each key IT process as listed in Procedures Performed. The degree of control was used to communicate the assessor’s perception of the resources allocated to reduce and/or eliminate risks. Resources could be identified as people, processes, or technology. The levels of control were:
 - A “*high*” degree of control indicates that management has either successfully allocated sufficient resources to reduce the impact of the risk or has potentially over-allocated resources to a lower risk area.
 - A “*medium*” degree of control indicates that minimal resources may be available to reduce the impact of the risk or that management has allocated minimal resources to reduce the impact of the risk if it occurs, however, more resources could be applied at minimal to moderate costs.
 - A “*low*” degree of control indicates that insufficient resources exist to reduce the impact of the risk or that management has not allocated adequate resources to reduce the impact of the risk if it occurs. The effort to mitigate the risk may have a moderate to high cost.
4. Documented the risk and control levels for each item on the IT internal control questionnaire and provided these to management for their review and agreement. A matrix was provided to management in a confidential appendix that summarizes the risk versus control settings for the IT areas listed in Procedures Performed.
5. Developed a risk based internal audit plan for years 2010 through 2012 based on the results of the assessment as well as management’s input and budget constraints. The plan was provided to management in a confidential appendix.