



City of Milwaukee
Employees' Retirement System

Bernard J. Allen
Executive Director

David M. Silber, CFA, CAIA
Chief Investment Officer

Melody Johnson
Deputy Director

May 11, 2018

Mr. Jim Owczarski
City Clerk
Room 205, City Hall

Dear Mr. Owczarski:

Please be advised that an Administration & Operations (A&O) Committee Meeting of the Annuity and Pension Board has been scheduled for **Thursday, May 17, 2018 at 9:00 a.m. in the Employees' Retirement System Conference Room at 789 N. Water Street, Suite 300.** If a quorum of the Board is present, this meeting will convene as a Special Board Meeting. The agenda is as follows:

I. Experis Internal Audit Reports.

Please be advised that the Administration & Operations Committee may vote to convene in closed session on the following item (I.A.), as provided in Section 19.85(1)(d), Wisconsin State Statutes, to consider "strategy for crime detection and prevention." The Committee may then vote to reconvene in open session following the closed session.

A. IT Vulnerability Assessment Presentation.

B. Risk Assessment and Internal Audit Plan for Fiscal Year 2018.

II. Approval of A&O Committee Audit Charter and Internal Audit Charter.

III. IT Projects Portfolio.

IV. Organizational/Personnel Update.

Sincerely,

A handwritten signature in black ink, appearing to read "Bernard J. Allen", is written over a printed name and title.

Bernard J. Allen
Executive Director

BJA:jmw

PLEASE NOTE - Upon reasonable notice, efforts will be made to accommodate the needs of disabled individuals through sign language interpreters or other auxiliary aids. For additional information or to request this service, please call 414-286-3557.



City of Milwaukee Employees' Retirement System

Risk Assessment and Internal Audit Plan for Fiscal Year 2018

MAY 11, 2018

EXPERIS FINANCE
RISK ADVISORY SERVICES
WISCONSIN OFFICE

This report is intended solely for the use of City of Milwaukee Employees' Retirement System 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
Background	3
Scope and Objectives.....	3
Risk Assessment Results and Audit Plan Justification Summary.....	3
Conclusion	4
SUMMARY OF RISK ASSESSMENT METHODOLOGY	5
1. Key Areas Understanding	5
2. Risk Rating Framework Definitions	5
3. Inherent Risk Factors Identification and Definition	6
4. Operational Areas Assessment and Rating.....	7
<i>Ethics and Governance</i>	7
<i>Accounting & Finance Process</i>	8
<i>Investment Management Process</i>	9
<i>Enrollment & Member Services</i>	10
<i>Benefit Calculation</i>	11
<i>Contributions</i>	12
<i>Benefit Payroll</i>	12
<i>Benefit Administration</i>	13
<i>HR / Payroll Process</i>	14
<i>Vendor Management</i>	14
<i>IT General Controls</i>	15
<i>Vulnerability Assessment</i>	16
<i>Social Engineering Assessment</i>	16
<i>Business Continuity</i>	16
5. Risk Based Audit Plan Development	17
EXHIBIT I – 2018 RISK BASED INTERNAL AUDIT PLAN.....	18
EXHIBIT II – 2018 RISK BASED INTERNAL AUDIT PLAN HOURS	19
APPENDIX I – RISK BASED PROCESS RATINGS	21
APPENDIX II – CATEGORY RISK RATING DEFINITIONS	22

EXECUTIVE SUMMARY

Background

The City of Milwaukee Employees' Retirement System (ERS) is headquartered in Milwaukee, Wisconsin. ERS has the responsibility of administering the benefits of its member constituency, which is comprised of employees and retirees of the City of Milwaukee and its related agencies. Benefits are managed in accordance with legislative guidance and contractual obligations.

Scope and Objectives

Experis Finance performed a high level assessment of the risks associated with various operational and IT areas within ERS at the direction of the ERS Board. From this assessment, a Risk-based Internal Audit Plan was developed to determine the adequacy of the ERS's internal controls and operating procedures. The plan provides emphasis to areas perceived to have higher risk and allows audit resources to be used in the most cost effective manner. The risks identified in this report, and their ratings, are based upon industry knowledge and standards in conjunction with ERS's practices, and are not an indication of where gaps currently exist.

Discussions with process owners and management were performed to determine the primary risks to ERS and internal audit focus. The results of the internal audit procedures performed throughout fiscal year 2017 were also reviewed and assessed. The results of this Risk Assessment are summarized in Appendix I. Based on the Risk Assessment, the Internal Audit Plan was developed (Exhibit I) and related internal audit hours assigned (Exhibit II).

Risk Assessment Results and Audit Plan Justification Summary

The Internal Audit Plan focuses on the risks identified during the Risk Assessment, inherent risks within processes based on industry knowledge, and areas critical to the ERS's strategic goals and operational functionality. In 2018, the Audit Plan will continue to follow the rotational cycle that has been plan in prior years. This year, an area of concern noted for the ERS, while outside its control, is the funding requirement for the employers. The discount rate, that has been set as part of the funding policy, is higher than average when compared to other public pension funds. This presents a Governance risk for the organization and the employers, and puts pressure on the organization to meet the higher than average investment rate of return. The *2018 Risk Based Internal Audit Plan-Exhibit I* includes the following full-scope audits:

- Investment Management
- Contributions
- Benefit Payroll
- Vendor Management
- IT General Controls
- Vulnerability Assessment
- Social Engineering Assessment

- Business Continuity

Hours have been included in this year's Audit Plan to also include the follow-up of previous audit areas that had findings and for any special projects requested by management.

Conclusion

This Risk Assessment and Internal Audit Plan should be reviewed and updated by management and members of the Administration & Operations (A&O) Committee as significant changes occur, and at a minimum on an annual basis. Any changes in ERS's control environment (including but not limited to employee turnover of mid-level and senior level management, procedural changes, changes to the MERITS system, IT infrastructure, etc.) should be communicated, so the audit plan can be adjusted as needed.

SUMMARY OF RISK ASSESSMENT METHODOLOGY

The following steps were performed in completing the Internal Audit Risk Assessment:

1. Key Areas Understanding

Gained an understanding of key operational areas and procedures through employee interviews and a review of documentation:

- Key operating processes, programs and personnel were identified.
- Recent Board Minutes were reviewed to consider relevant issues facing ERS.
- Interviews with the ERS management and key personnel were conducted to obtain their perspective of the risks faced by ERS and to verify their roles and responsibilities in the ERS's current operating environment, and strategic initiatives.
- The results of previous audits were reviewed and discussed with management and considered in the assessment.
- Discussed planned employee job transitions and employee issues within the organization in 2018.
- Discussed changes to the IT environment related to logical access, change management and operations.
- Discussed the impact of cyber security risks and third-party risk management.
- Discussed the potential impact of other external risks that could impact ERS operations, such as the European Union's (EU) General Data Protection Regulation and recent changes in the financial market.

2. Risk Rating Framework Definitions

The Risk Rating definitions are as follows:

Risk Ratings	Definitions
Likelihood	Likelihood that a risk would occur during a specified period of time.
Impact	Impact on earnings, management availability, and the fulfillment of business objectives.
Velocity	The speed of occurrence of a particular risk impacting the organization.

The following table shows the Risk Ratings definitions considered when determining the definitions for the Risk Factors (see #3 below):

	Low	Medium	High
Likelihood	The risk is unlikely to occur during the specified period of time.	The risk is likely to occur during the specified period of time.	The risk is expected to occur during the specified period of time.
Impact	The risk will not materially affect earnings, management availability or fulfillment of business objectives.	The risk will affect complete achievement of anticipated earnings, management availability or fulfillment of business objectives.	The risk will materially affect achievement of anticipated earnings, management availability or fulfillment of business objectives.
Velocity	Risk will occur slowly	Risk may occur quickly,	Risk may occur quickly,

	Low	Medium	High
	and allow for sufficient preparatory time. Management has the ability to react in time to mitigate risk.	and management has the ability to react in time to mitigate risk.	and management does not have the ability to react in time to mitigate risk.

3. Inherent Risk Factors Identification and Definition

The following inherent risk factors associated with the key operating areas within ERS were identified and defined:

Risk Factors	Definition
Prior Year Audit Comments	Final audit rating based on the number and severity of any issues.
Management Concern	Concerns expressed during interviews regarding overall controls in a process area.
Financial Statement Materiality	The risk that financial statements that are prepared and reported are materially inaccurate and lead the reader to arrive at the wrong conclusion.
Strategic Risk	The risk arising from adverse investment / business decisions, improper implementation of decisions, or lack of responsiveness to market or industry changes.
Operational & Control Risk	The risk arising from inadequate or failed internal processes or systems and the misconduct or errors of people. In addition, the risk that the internal control environment does not provide the discipline and structure to identify the failures, misconduct, errors or adverse events above.
Interest Rate & Market Risk	The risk to the Organization's condition resulting from adverse movements in market rates or prices. This can occur to earnings or changes in the value of the investment portfolio. This results from re-pricing risk, basis risk, yield curve risk and from options risk
Liquidity Risk	The risk that the Organization will not be able to meet its obligations as they come due because of the inability to liquidate assets or obtain adequate funding.
Compliance & Regulatory Risk	The risk arising from violations of laws, rules, regulations or from nonconformance with prescribed practices, internal policies and procedures, ethical standards or adverse judgments that can disrupt or negatively affect ERS operations and performance.
Reputational & Public Scrutiny Risk	The risk to current operations arising from negative public opinion resulting from an event within the entity.

Risk Factors	Definition
Reporting and Data Integrity Risk	The risk from inaccurate or unauthorized reports or data used by management or the Board for critical decision making purposes.
Fraud Risk	The risk intentional acts are committed on or by ERS by internal or external sources that can cause a loss of ERS funds, value, or reputation and result in an unauthorized benefit by others.
IT & System Application Risk	The risks of inappropriate/excessive logical access, inconsistent/absent change management processes, or informal/immature data center operations. The risks apply at multiple levels which include the network, application, database, and operating system levels.

The Risk Ratings (see #2 above) and inherent Risk Factors are rated in Appendix I and defined in Appendix II.

4. Operational Areas Assessment and Rating

Each key operational area was assessed according to the Risk Factors and Risk Ratings defined above. An overall risk rating was assigned, and used in determining the risk based audit plan. Each of the sections analyzed has its rating listed within this section; refer to Appendix I-Risk Based Process Ratings to see a summary of rankings for review at the entity level.

Ethics and Governance Medium (3)

Summary

Medium-High and High Risk Factors:

- Strategic Risk
- Reputational Risk

Mitigating Control Factors Currently in Use

- AO Committee and Board of Directors have defined meeting agenda's and follow meeting procedures.
- Management has engaged capable advisors and experts to assist them navigate market risks.

Detailed Analysis

The Ethics and Governance process is responsible for the organization's governance process, management of day to day operations and the communication of policies and values, "Tone from the Top".

Strategic Risk continues to remain elevated in 2018 and reflects a number of external factors that ERS Management will need to monitor and address in 2018. Those external factors include:

- The impact of the recent actuary report on the Projected Benefit Obligation (PBO)

- Investment volatility impacted by rising interest rates, potential inflation and changing US economic policies

These factors may present new challenges to both management and the BOD in 2018 and beyond. Without the appropriate governance authority to do so, the agencies and the staff face a challenge to meet a long term investment rate of return that is above the average of other public pension plans.

Reputational & Public Scrutiny Risk also remains high in 2018 as the responsibility of managing the pension assets and payment of retiree pension payments are the responsibility of ERS management and the A&O Committee.

While external environmental factors have elevated in 2018, the Ethics & Governance Process is based on a solid foundation and management has engaged capable advisors and experts to assist them during this period of change.

In 2017, an audit of the Ethics and Governance process was performed and identified no issues at that time. Since the process is considered to have an overall Medium risk profile and was audited in 2017, an audit is not considered necessary in this fiscal year.

Accounting & Finance Process Medium (3)

Summary

No High Risk Factors.

Mitigating Control Factors Currently in Use

- Accounting and Finance Standard Procedural Instructions (SPI's) detail the procedures necessary to compile and complete the annual financial statements.
- Northern Trust's Investment Management system is reviewed and tested by a third party resulting in a Statement of Controls (SOC) report that is issued to ERS.
- The General Ledger, Payroll and Procurement/Accounts Payable systems are maintained and managed by the City of Milwaukee. Transactions made within these systems must follow defined procedures to execute those transactions within those systems.
- All cash disbursements and payroll payments are approved by the appropriate member of ERS management.

Detailed Analysis

The Finance and Accounting Process is responsible for the recording and reporting of financial transactions within ERS. At year end, this process is responsible for the preparation and reporting of ERS's annual financial statements.

Operational and Control Risk and Management Concerns were lowered in 2018 as compared to the 2017 risk assessment, following the recruitment of a new CFO who, in addition to the CFO responsibilities, also assumed many responsibilities of the previous Pension Accounting Specialist. The primary functions transferred to the new CFO were the preparation of the organization's annual financial filings. The new CFO has experience in this industry as he previously prepared Pension Statements at the Wisconsin Retirement System (WRS).

In 2017 an audit of the Finance and Accounting process was performed and two internal control deficiencies were identified, thus the Medium (3) rating for Prior Year Audit Comments category. One of these two deficiencies introduced an immaterial financial misstatement to the published 2015 financial statements. Both of these deficiencies were corrected in 2017.

The Accounting and Finance process is considered to have an overall Medium (3) risk. Since it was audited in 2017, a full scope audit will not be conducted in 2018; rather follow-up procedures will be conducted related to the review of the key financial reporting workbooks and the financial reporting SPIs issues identified in the 2017 audit. Not performing an internal audit in 2018 will also give the new CFO the opportunity to assess and adjust the control environment over a full fiscal year before the audit in 2019.

Investment Management Process Medium-High (4)

Summary

Medium-High and High Risk Factors:

- Management Concerns**
- Financial Statement Materiality Risk
- Strategic Risk
- Interest Rate / Market Risk*
- Reputational & Public Scrutiny Risk*

*Inherent risk factors assigned an additional weight: Inherent risks are risks under the assumption no internal controls are applied. Some of these risks may not be directly controllable by ERS's internal control environment, but can have a significant impact on the organization. The risks are listed as they are relevant to the organization's operation and are considered by management on a daily basis.

**Management Concerns are not related to the overall process or management of the area, but are directed towards meeting a higher than average investment rate of return within the limits set by the City's pay practices.

Mitigating Control Factors Currently in Use

- The Investment Management team regularly reviews the performance of their Investment managers, including performing on-site due diligence at the managers' offices.
- Investment Managers' accounts and invoices are reviewed against manager statements.
- Manager invoiced fees are independently recalculated by members of the ERS Investment Management team.
- New Investment Managers are selected based on advice of their Investment and Pension Advisor, Callan.
- Investment policy, which drives the investment strategy at ERS, is developed in conjunction with Callan.

Detailed Analysis

The Investment Management process is responsible for the management of the City of Milwaukee's Pension Assets and directing the investment portfolio (approximately \$5.3 Billion) to meet City of Milwaukee pension obligations. The department is currently composed of the CIO and two Investment Analysts.

While there are no changes in the overall Risk Assessment from 2017 to 2018, the inherent risk factors influencing and impacting key risk areas continue to be present within the Investment Management process.

Financial Statement Materiality and Strategic Risk continue to be elevated as portfolio investments represent the majority of ERS assets. In addition, management of these assets is critical to the success of City of Milwaukee ERS and its population of employees, retirees and beneficiaries.

Reputation & Public Scrutiny Risk remains elevated in 2018 given the public's continued interest in local public pensions, the materiality of the assets managed and the impact of funding shortfalls on local taxation. Management has represented these risks cannot be controlled via internal controls and management is aware of them; they are listed here to ensure continued visibility.

Overall there are Management Concerns over the retention of Investment Management employees. While this concern is one of Governance, it is one that directly impacts Investment Management. This concern is driven by several factors, including:

- An improving job market that has very low unemployment rate
- Rising wages across all private industry sectors

The Investment Management process continues to have a Medium-High risk profile due to its importance, the magnitude of the investment balance and the overall inherent risks associated with investment management. An audit of this process is scheduled for fiscal year 2018.

Enrollment & Member Services

Low-Medium (2)

Summary:

No High Risk Factors.

Mitigating Control Factors Currently in Use

- The MERITS system is a defined process that requires ERS employees to enter specific employee data. Critical employee data that is missing from MERITS is flagged as a follow-up item by the system; these flags can't be deleted until the data is entered.

Detailed Analysis

The Enrollment and Member Services process is responsible for both the on-boarding of employees into the Retirement System at the time they are hired and then, later, assisting those employees once they move into retirement.

Operational & Control Risk and Management Concerns were reduced in 2018 as ERS was able to internally recruit and fill a number of open positions in 2017. These open positions were filled with individuals who were already ERS employees and had

some familiarity with the Enrollment and Member Services. Management has indicated that they are confident that these new employees have demonstrated growth in their new roles and are capable of performing their assignments in 2018.

Based on the above changes, the process is considered to have an overall lower Medium (2) risk profile and will not be audited in 2018 as this was most recently audited in May 2017 with no issues identified.

Benefit Calculation Medium (3)

Summary

Medium-High and High Risk Factors:

- Financial Statement Materiality Risk
- Reputational & Public Scrutiny Risk

Mitigating Control Factors Currently in Use

- The Benefit Calculation process is integral to the MERITS system and requires the Benefit Calculation professional to follow defined processes and procedures within the system to generate the participant's benefit payment.
- After the initial retiree payment is calculated, the computation is reviewed and recalculated by another employee, independent of the initial calculation.

Detailed Analysis

The Benefit Calculation process calculates and determines the amount of the pension payments that will be made to future retirees. While the process has a higher inherent risk, as a benefit miscalculation could result in loss of funds and reputational harm, the process is tightly controlled by management and has a number of mitigating controls. Many of the control procedures and computations, especially those associated with retiree payments, are audited by team members that were independent of the initial computations.

Operational & Control Risk was reduced in 2018. The risk was reduced as management has indicated that they have confidence in the employees performing these roles. In 2017, an audit of this process was performed. The results of the audit identified no internal control deficiencies. Reputation & Public Scrutiny Risk remains raised in 2018 given the public's continued interest and scrutiny in local public pension plans.

After considering these changes, the overall Risk Rating associated with this process is rated Medium (3). As the process was audited in May 2017, it will not be audited in 2018.

Contributions
Low-Medium (2)

Summary:

No High Risk Factors.

Mitigating Control Factors Currently in Use

- Employee Contributions from the City of Milwaukee and participating agencies are reviewed and reconciled by the ERS Contributions team.

Detailed Analysis

The Contributions function conducts the receipt and recording of employee pension contributions from each of the agencies participating in the retirement plan. The processes used by ERS to reconcile contributions are well defined and closely monitored by ERS management.

Fraud Risk was lowered in 2018 as the likelihood to misdirect payments being made from a contributing agency to the retirement fund is limited due to the cash management procedures and controls that have been implemented by ERS. Prior Audit Comments risk factor was lowered in 2018 as no comments were identified during the 2014 and 2016 audits.

Based on the above, the process is considered to have an overall Medium risk profile and will be audited in 2018 as the most recent audit was performed in April 2016.

Benefit Payroll
Medium (3)

Summary:

Medium-High and High Risk Factors:

- Management Concerns
- Financial Statement Materiality
- Strategic Risk
- Reputational & Public Scrutiny Risk

Mitigating Control Factors Currently in Use

- Benefit payments are reconciled to each benefit calculation, MERITS benefit system, and bank records.
- Proper segregation of duties exists between custody of check stock, initiating member payment run, authorizing member payment run, running print job, and custody of printed checks, and is reflected in system access.
- Bank authorization for check signing and initiating and authorizing wire transfers and ACH are appropriate per position descriptions and properly uphold segregation of duties.

Detailed Analysis

The Benefit Payroll process disburses and distributes retiree pension payments.

Strategic Risk remains high in 2018 as the Benefit Payment Process is considered to be one of the most critical functions within ERS. In addition, management decisions influencing the delivery of pension payments would significantly impact ERS

operations. Reputational and Public Scrutiny Risk continues to remain high as the process has a higher inherent risk as:

- Regular benefit payments must be made to the fund participants, and
- The miscalculation of benefits payments may result in reputation risk to ERS.

Management Concerns continue to remain high as the process is critical to ERS operations. While employee turnover that occurred in prior years has subsided, management continues to be concerned about employee retention due to an improving economy, overall low unemployment and wage and salary limits implemented by the City of Milwaukee.

Prior Audit Comments risk factor was lowered in 2018 as no comments were identified during the 2014 and 2016 audits. The process is considered to have an overall Medium risk profile and will be audited in 2018.

Benefit Administration ***Low-Medium (2)***

Summary:

No High Risk Factors.

Mitigating Control Factors Currently in Use

- Deposit and withdrawal amounts for life/health/dental benefit contributions per bank records tie out to posting in MERITS, and amounts payable to the benefit provider.
- Retiree elections for health/dental benefits are accurately reflected in MERITS and corroborated to benefit provider invoicing.

Detailed Analysis

Life, health and dental benefit plans are self-funded by the City and are administered by third-party service providers. Benefit Administration employees are responsible for:

- Assisting retirees with insurance inquiries,
- Updating member insurance rates, and
- Reconciling member and plan premiums.

The Benefit Administration process in place is mature and has a relatively low inherent risk profile.

Prior Audit Comments risk factor was reduced in 2018 as no comments were identified during the 2014 and 2016 audits. Other than the change to Prior Audit Comments, the Risk Assessment for the Benefit Administration process will remain unchanged from 2018. This evaluation was based on the following:

- This process is not expected to undergo any system or procedural changes and
- It is not expected to be impacted by any external factors that would otherwise introduce any additional risk to the process.

Based on the above, the process is considered to have an overall Low-Medium (2) risk profile and will not be audited in 2018 as the most recent audit was performed in May 2017.

HR / Payroll Process
Low-Medium (2)

Summary:

No High Risk Factors.

Mitigating Control Factors Currently in Use

- The Payroll process is maintained and managed by the City of Milwaukee. Transactions made within the system must follow defined procedures to execute those transactions within those systems.
- Employee hires, promotions and terminations must be approved by the City of Milwaukee Department of Employee Relations.

Detailed Analysis

The ERS HR / Payroll process utilizes the procedures and software provided by the City of Milwaukee Department of Employee Relations. The HR/Payroll function includes the administration of employment and personnel records, employee time and attendance reporting, the payment and recording of the biweekly payroll and the annual Performance Evaluation process.

The payroll system is run by City of Milwaukee Department of Employee Relations and therefore, ERS's risk is somewhat limited to the system the City uses. Similarly Reputational & Public Scrutiny Risk was reduced in 2018 as the process is maintained and operated by the City of Milwaukee. The process is not expected to undergo any system or procedural changes, nor is it expected to be impacted by any external factors that would otherwise introduce any additional risk to the process. As a result, the Risk Assessment for this process is unchanged from 2017.

Based on the above, the process is considered to have an overall Low-Medium risk rating at a (2) profile. This will not be audited in 2018 as it was most recently audited in May 2017.

Vendor Management
Low-Medium (2)

Summary:

Medium-High and High Risk Factors:

- Reputational & Public Scrutiny Risk

Mitigating Control Factors Currently in Use

- The City of Milwaukee has implemented standardized contracts for service providers who wish to provide services to the City of Milwaukee. These contracts have specific provisions that each service provider must agree to before the contract can be entered into by the City or a member agency.
- In order for a contract to be executed, each contract must follow the contract approval process outlined by the City of Milwaukee.

Detailed Analysis

The Vendor Management process is responsible for the management and administration of the contracts entered into by ERS. The majority of these contracts are related to Management of the Pension Assets and IT services supporting the organization. As part of its efforts to minimize risk in this function, ERS has standardized the provisions and terms in its contracts for its regular and reoccurring contractors.

IT and System Application Risk was lowered in 2018, as the process only utilizes a database to track and manage the contracts entered into by ERS. This database has a limited risk profile as it is only used internally by ERS employees and is not externally accessible.

Reputational & Public Scrutiny Risk continues to remain high, as any negative issue involving a vendor would undoubtedly invite raised scrutiny from the public of ERS operations.

No audit issues were identified during the 2016 audit. Based on the above, the process is considered to have an overall Low-Medium risk profile and will be audited in 2018 as the most recent audit was performed in March 2016.

IT General Controls ***Medium (3)***

Summary:

Medium-High and High Risk Factors:

- Reputational & Public Scrutiny Risk

Detailed Analysis

The IT General Controls consists of logical access, change management and operations. The primary application continues to be MERITS which is used to manage the data of retirees. The network logical access continues to be managed with the Microsoft Active Directory tool. Changes are documented in the Tracker change control database.

The prior year comments and management concern risks were both rated low to medium since there were no audit findings in 2017 and management had no notable concerns. The Operational & Control risk was rated Medium due to the reliance on MERITS which depends on general controls.

With the emergence of new threats and increased occurrences of attacks on networks, there is now a greater risk with the operations of an IT infrastructure that may have a detrimental impact on the organization's reputation. The Reputational risk is therefore now rated higher.

A new regulation, the General Data Protection Regulation (GDPR) which regulates the processing of personal data of European Union (EU) citizens was discussed with management. Management is encouraged to continue to assess the potential impact of GDPR for personal data of retirees residing in the EU.

Overall, failures in general controls could harm ERS's reputation resulting in dissatisfied employees and customers. Additionally, the absence or lack of general controls could expose ERS to a potential data breach. The audit plan for fiscal year 2018 will test the general control environment to determine if controls continue to

operate effectively. Due to the nature of IT, the scope could be modified to include current or emerging threats. Management considers IT General Controls to be a Medium Risk (3).

Vulnerability Assessment Medium-(3)

Summary:

Medium-High and High Risk Factors:

- Reputational & Public Scrutiny Risk
- Fraud Risk

Detailed Analysis

Risks associated with cybersecurity continue to be considered high due to the large number of data breaches in today's society. Cybersecurity risks are on-going, but ERS has maintained controls such as firewalls, access protection and limited external network points to mitigate those risks. The most recent Vulnerability Assessment was completed in February 2018 for fiscal year 2017. An assessment is planned for fiscal 2018 due to the Medium risk rating. Management considers Network Security to be a Medium Risk (3).

Social Engineering Assessment Medium (3)

Summary:

Medium-High and High Risk Factors:

- Reputational & Public Scrutiny Risk
- Fraud Risk

Detailed Analysis

The objective of the social engineering audit is to determine employees' awareness of information security and the effectiveness of training. Unintentional release of sensitive information via email and/or telephone puts organizations at risk of unauthorized access to their data. This will be included in the audit plan for FY 2018.

Business Continuity Medium (3)

Summary:

Medium-High and High Risk Factors:

- Strategic Risk
- Reputational & Public Scrutiny Risk

Detailed Analysis

The primary IT data center for ERS is located in the ERS offices. As IT services are critical components of efficient ERS operations, ERS has adopted a Business Continuity and Disaster Recovery Policy. The purpose of the policy is, "to ensure

continuity of operations in the event of catastrophic equipment failure, data loss, or disaster that makes operations at the primary office unviable." To support this Policy ERS has developed a formal Disaster Recovery (DR) Plan for ERS to use to recover its IT systems timely in the event of an unplanned event impacting the IT infrastructure or its facilities. ERS has also developed a formal Business Continuity (BC) plan to support continued business operations for critical services if the ERS offices are not available for use.

ERS maintains a Remote Office (RO) about 10.5 miles away from the primary location. The RO is available as an alternate work location for staff members to perform critical services. Management completes annual testing in some capacity using the remote office.

ERS has access to an alternate data processing facility located near Madison, WI, to support ongoing operations should an unplanned incident at ERS offices cause an interruption of operations at the primary ERS data center. ERS sends "snapshots" of the critical systems to the alternate data center every four hours.

The Strategic and Reputational risk were rated high due to the general public expectation that companies must have applications and the underlying data available at all times. The last audit was completed in 2015 which did not identify any significant issues. Additionally, the business operations and supporting IT systems have been noted as stable which has justified the cycling of this audit previously. Due to the High risk factors and time since last audit, the FY18 plan includes business continuity audit.

5. Risk Based Audit Plan Development

Priority in the audit plan was given to operating areas with the highest perceived risk based on the factors above. Processes/functions that are identified as "High" and "Medium-High" risk may be on an annual audit cycle; "Medium" and "Low-Medium" risk processes/functions will have an annual to every three year cycle; and "Low" risk areas will be audited every three to four years, unless otherwise stated in the Risk Based Narrative section of this report. See the following Exhibit for the recommended *Risk Based Internal Audit Plan*. Risk assessments and risk based audit plans are most effectively executed if the formal risk assessment and audit planning process is performed at least annually. As risks and circumstances change throughout the year, the risk assessment and audit plan are adjusted.

The audit scope listed on the audit plan are not all-inclusive, rather an example of areas that will most likely have an area of focus. The actual prioritization and scope of the audits will be determined during the planning phase prior to fieldwork.

**Milwaukee Employees' Retirement System
2018 Risk Based Internal Audit Plan
March 2018**

Audit Area: Scope	Risk Rating	Last Audit	2018	2019	2020	Comments*
Ethics and Governance	3	May-17		X		
Board and AO Committee Governance				X		
Board and Management Reporting				X		
Whistleblower Governance and Reporting Protocols				X		
Accounting & Finance:	3	December-17	X	X		
Standard Procedural Instructions (SPIs)			X	X		Limited to determination of proper control design by performing a walk-through rather than testing to determine prior year's audit issue have been properly resolved.
Financial Statement / Footnote Preparation			X	X		
Reconciliation process:				X		
Accounts Payable (AP)/Employee Expense				X		
GL Journal Entry				X		
Manual Expense Checks				X		
Year-end Close Process				X		
Fixed Asset				X		
System Access (PeopleSoft/ACCPAC)				X		
Budgeting Process				X		
Third Party Controls Review (SSAE/SOC-1)				X		
Investment Management	4	March-16	X		X	
Calendar of Scheduled Events			X		X	
Investment Manager Monitoring / Due Diligence			X		X	
Northern Trust System Access			X		X	
Investment Manager Account Reconciliation			X		X	
Invoiced Fees Payable / Payment			X		X	
Enrollment & Member Services	2	May-17		X		
MERITS System Access				X		
Data Entry / Data Review				X		
Employee Communications				X		
Benefit Calculation Process	3	May-17		X		
SPIs				X		
MERITS System Access				X		
Pension Payment Recalculation / Approval				X		
Pension Payment Support / Review				X		
Contributions	2	April-16	X		X	
SPIs			X		X	
Member Contribution Reconciliation			X		X	
Member Organization Reconciliation			X		X	
Benefit Payroll	3	April-16	X		X	
SPIs			X		X	
Retiree Payment Reconciliation			X		X	
Retiree Payment Disbursements			X		X	
MERITS System Access			X		X	
Benefit Administration	2	May-17		X		
SPIs				X		
MERITS System Access				X		
Health Insurance Premium Reconciliation				X		
Life Insurance Premium Reconciliation				X		
Dental Insurance Premium Reconciliation				X		
Health , Dental and Life Insurance Rate Administration				X		
HR/Payroll:	2	May-17		X		
People Soft System Access				X		
Payroll System User Access				X		
New/Terminated Employees				X		
Vacation Time Process				X		
Payroll Expense Reconciliation				X		
Employee Payment/Paycheck recalculation				X		
Vendor Management	2	March-16	X			Since this is a lower Medium area, consider an every 3 year cycle. Next audit expected in 2021, unless rating change prior to that.
SPIs			X			
Contract Compliance			X			
Financial Compliance			X			
Information Technology:			X	X	X	
IT General Controls (Logical Access, Change Management, Operations)	3	June-17	X	X	X	
Vulnerability Assessment (Internal and External Networks)	3	February-18	X	X	X	
Social Engineering Assessment	3	December-17	X	X	X	
Business Continuity	3	November-15	X		X	

*If no comment is noted, an "X" represents a full audit (including Control Design Documentation and Operational Control Testing) is performed.

**Milwaukee Employees' Retirement System
2018 Risk Based Internal Audit Plan Hours
March 2018**

Description / (scope on Exhibit I)	Risk Rating	Estimated Hours 2018	Estimated Cost	Comments
Risk Assessment	N/A	70 @ \$160 /hr	\$11,200	Engagement Manager Rate
Engagement Management - Administration and quality assurance - Management meetings - A&O Committee meetings and document preparation	N/A	30 @ \$200 /hr 112 @ \$160 /hr	\$6,000 \$17,920 \$23,920	Director Rate Engagement Manager Rate
Investment Management	4	80 @ \$118 /hr	\$9,440	Professional Rate
Contributions	2	80 @ \$118 /hr	\$9,440	Professional Rate
Benefit Payroll	3	80 @ \$118 /hr	\$9,440	Professional Rate
Vendor Management	2	60 @ \$118 /hr	\$7,080	Professional Rate
IT General Controls	3	90 @ \$148 /hr	\$13,320	IT Professional Rate
Vulnerability Assessment	3	120 @ \$170 /hr	\$20,400	Security COE Rate
Social Engineering Assessment	3	50 @ \$170 /hr	\$8,500	Security COE Rate
Business Continuity	3	60 @ \$148 /hr	\$8,880	IT Professional Rate
Follow-up Procedures: Accounting and Finance	N/A	12 @ \$118 /hr	\$1,416	Professional Rate
Management and Special Projects: TBD	N/A	60 @ \$170 /hr	\$10,200	Security COE Rate
Total Audit Hours / Cost		834	\$122,036	
Total Annual Service Hours / Cost		904	\$133,236	

The Audit Plan is subject to change based on the results of the on-going risk assessment review and any changes to legal or regulatory emphasis. Any changes would be reviewed by the Audit Liaison and approved by the Audit Committee.

APPENDICES

**Milwaukee Employees' Retirement System
Internal Audit Risk Based Process Ratings
March 2018**

PROCESS	PRIMARY PROCESS OWNER(S)	PRIOR YEAR AUDIT COMMENTS	MANAGEMENT CONCERNS	FINANCIAL STATEMENT MATERIALITY RISK	STRATEGIC RISK	OPERATIONAL & CONTROL RISK	INTEREST RATE & MARKET RISK	LIQUIDITY RISK	COMPLIANCE & REGULATORY RISK	REPUTATIONAL & PUBLIC SCRUTINY RISK	REPORTING & DATA INTEGRITY RISK	FRAUD RISK	IT & SYSTEM APPLICATION RISK	CALCULATED RISK WEIGHTED RATING	REPORTED RISK RATING (as stated on other schedules)	EXPERIS AUDIT IN FISCAL YEAR 2018?
Financial and Operations																
Ethics & Governance	Executive Director: Jerry Allen Deputy Director: Melody Johnson Chief Investment Officer: David Silber	1	2		4	3			3	4	3	2		2.75	3	NO
Accounting & Finance	Deputy Director: Melody Johnson Chief Financial Officer: Dan Gopalan	3	3	3	3	3			3	3	3	3	3	3.00	3	YES (limited to follow-up)
Investment Management	Executive Director: Jerry Allen Chief Investment Officer: David Silber	1	4	5	4	3	4	2	3	5	3	3	3	3.50	4	YES
Enrollment & Member Services	Retirement Plan Manager: Michael Dziuk	1	2		2	3			2	3	3	2	3	2.33	2	NO
Benefit Calculation	Deputy Director: Melody Johnson Chief Financial Officer: Dan Gopalan	1	3	4	3	3			2	4	3	3	3	2.90	3	NO
Contributions	Deputy Director: Melody Johnson Chief Financial Officer: Dan Gopalan	1	3	3	3	2			2	3	3	2	2	2.40	2	YES
Benefit Payroll	Deputy Director: Melody Johnson Chief Financial Officer: Dan Gopalan	1	4	4	4	3			2	4	3	3	3	3.10	3	YES
Benefit Administration (Life, Health & Dental)	Retirement Plan Manager: Michael Dziuk	1	3	2	2	2			2	3	3	2	3	2.30	2	NO
HR / Payroll	Deputy Director: Melody Johnson Chief Financial Officer: Dan Gopalan	1	2	1	2	1			1	2	2	2		1.60	2	NO
Vendor Management	Deputy Director: Melody Johnson Chief Investment Officer: David Silber	1	3	2	2	3			1	4	2	3	1	2.20	2	YES
Information Technology																
IT General Controls	Chief Technology Officer: Kelly Reid	1	2		3	3			3	4		3		3.00	3	YES
Vulnerability Assessment	Chief Technology Officer: Kelly Reid	2	2		3	3			2	4		5		3.29	3	YES
Social Engineering Assessment	Chief Technology Officer: Kelly Reid	3	2		3	2			2	4		5		3.00	3	YES
Business Continuity	Chief Technology Officer: Kelly Reid	1	2		5	2			2	4		3		2.71	3	YES

**Milwaukee Employees' Retirement System
Category Risk Rating Definitions
March 2018**

	IMPACT, LIKELIHOOD AND VELOCITY RATINGS				
CATEGORY	LOW 1	LOW-MEDIUM 2	MEDIUM 3	MEDIUM-HIGH 4	HIGH 5
PRIOR YEAR AUDIT COMMENTS	No reportable issues for prior audit. Acceptable prior risk rating.	Moderate or Low severity issue for prior audit. Acceptable prior risk rating.	Significant issue(s) for prior audit. Acceptable prior risk rating.	Marginal prior audit rating. Moderate prior risk rating.	Marginal prior audit rating. High prior risk rating.
MANAGEMENT CONCERN	Management confident control procedures are effective; IT - minimal to no management concern.	Management indicated limited concerns in the normal course of business. Could develop into more severe problems if not corrected; IT - minimal to low management concern.	Deteriorating trends in the control environment due to changes in personnel, products, or procedures; IT - low to moderate management concern.	Management acknowledges significant deficiencies exist in the control structure; IT - moderate to high management concern.	Management indicated that controls are not in place; IT high to unacceptable levels of management concern.
FINANCIAL STATEMENT MATERIALITY	Less than 1% of total assets or total income.	1% - 3% of total assets or total income.	3% - 5% of total assets or total income.	5% - 10% of total assets or total income.	Greater than 10% of total assets or total income.
STRATEGIC RISK	Process not directly linked to organization's strategic goals.	Process is linked to at least one strategic goal - however, significant failure in process will not materially impact strategic goals.	Process is linked to a few of the organization's strategic goals - significant failure in process may materially impact strategic goals.	Process is linked to a majority of the organization's strategic goals, and significant failure in the process will impact the achievement of many of the strategic goals.	Process integral in achieving overall strategic goals for the organization. Failure in process will result in not achieving most of the strategic goals.
OPERATIONAL & CONTROL RISK	Transaction volume low / accuracy not compromised / routine transactions / highly automated processes / tenured staff / highly trained and experienced in process.	Transaction volume moderate / accuracy not compromised for timely completion / limited complexity / mainly automated / experienced staff in industry and with organization.	Transaction volume moderate / accuracy not normally compromised for timely completion / some complexity in transactions / majority of process automated - but many manual processes and management reporting / staff relatively experienced.	Transaction volume high / accuracy may be compromised for completion / complex transactions / limited workflow automation / manual management reporting / staff new to process or organization.	Transaction volume high / accuracy can be compromised for completion without easy detection / complex transactions / manual processes / new processes or systems / new staff.
INTEREST RATE / MARKET RISK	Financial results of the activity are not tied to changes in the market rates or pricing.	Financial results of the activity are minimally tied to changes in market rates or pricing. Organization has sufficient resources for funding.	Financial results of the activity are moderately tied to changes in market rates or pricing. Organization has sufficient resources for funding.	Financial results of the activity are tied to changes in market rates or pricing. Organization has limited resources for funding.	Financial results of the activity are tied to changes in market rates or pricing. Organization does not have sufficient resources for funding.

**Milwaukee Employees' Retirement System
Category Risk Rating Definitions
March 2018**

CATEGORY	IMPACT, LIKELIHOOD AND VELOCITY RATINGS				
	LOW 1	LOW-MEDIUM 2	MEDIUM 3	MEDIUM-HIGH 4	HIGH 5
LIQUIDITY RISK	Process has easily converted or liquid assets. No borrowings. Strong resources allows for additional funding if needed. No regulatory sanctions.	Process has moderate converted or liquid assets. Limited borrowings. Strong resources allow for additional funding if needed. No regulatory sanctions.	Process has moderately converted or liquid assets. Limited to moderate borrowings. Resources allow for additional funding if needed. Impact of potential regulatory sanctions.	Process has non-liquid assets. Highly leveraged, heavy reliance on borrowings. Resources allow for limited funding if needed. Impact of potential regulatory sanctions preventing borrowings.	Process has non-liquid assets. Highly leveraged, heavy reliance on borrowings. Organization does not have sufficient resources for funding. Impact of potential regulatory sanctions preventing borrowings.
COMPLIANCE / REGULATORY RISK	Activity has no regulatory changes in-process or expected. Decisions and data are based on highly objective information. Activity has had no legal opinions, lawsuits or adverse judgments recently.	Activity has limited regulatory changes in-process or expected. Decisions and data are based on objective information. Activity has had no legal opinions, lawsuits or adverse judgments recently.	Activity has moderate regulatory changes in-process or expected. Decisions and data are based on objective and subjective information. Activity has had limited legal opinions and no lawsuits or adverse judgments recently.	Activity has numerous regulatory changes in-process or expected. Decisions based on subjective information. Activity has had multiple legal opinions and/or lawsuits recently, but no adverse judgments.	Activity has numerous or volatile regulatory changes in-process or expected. Decisions based on highly subjective information. Activity has had numerous legal opinions and/or lawsuits and / or adverse judgments recently.
REPUTATIONAL & PUBLIC SCRUTINY RISK	Negative events have no immediate impact on reputation.	Negative events have minimal impact on reputation, isolated loss of customers.	Negative events have minimal impact on reputation, loss of confidence/reputation confined to local market, or a few customers with similar product or service.	Negative events have a substantial impact on reputation, with organization-wide loss of customer, members or community confidence.	Negative events have a substantial impact on reputation and future operations, with loss of customers, members or communities.
REPORTING & DATA INTEGRITY RISK	A formal report model governance process, including report and data testing and review is established. Reports are used for internal decision making purposes.	A formal report model governance process, including report and data testing and review is established. Reports are used for internal and external decision making purposes.	A formal report model governance process is not established and reports and data tested and reviewed prior to relying on information produced. However, the internal control review process would likely identify errors or inaccuracies in reports. Reports are used for internal and external	A formal report model governance process is not established and reports and data tested and reviewed prior to relying on information produced. The internal control review process is limited and may identify errors in reports. Reports are used for internal and external decision making purposes.	A formal report model governance process is not established and reports and data tested and reviewed prior to relying on information produced. The internal control review process does not review reports for accuracy and propriety. Reports are used for internal and external decision making purposes.

**Milwaukee Employees' Retirement System
Category Risk Rating Definitions
March 2018**

IMPACT, LIKELIHOOD AND VELOCITY RATINGS					
CATEGORY	LOW 1	LOW-MEDIUM 2	MEDIUM 3	MEDIUM-HIGH 4	HIGH 5
FRAUD RISK	Limited opportunities for fraud and limited motivation by Authority / Department / Personnel to achieve results or goals.	Some opportunities for fraud and/or moderate motivation by Authority / Department / Personnel to achieve results or goals.	Opportunities for fraud or a history of fraud and moderate motivation / pressure by Authority / Department / Personnel to achieve results or goals.	Significant opportunity for fraud or a history of fraud and moderate motivation / pressure by Authority / Department / Personnel to achieve results or goals.	High susceptibility for fraud or a recent fraud and high motivation / pressure by Authority / Department / Personnel to achieve results or goals.
IT & SYSTEM APPLICATION RISK	Basic network topology and IT infrastructure, applications are maintained in-house, minimum subject matter expertise required to support business processes, mature change management processes, application data and reports used for limited decision making purposes internally.	Moderate network topology and IT infrastructure, majority of applications are maintained in-house, occasional subject matter expertise required to support business processes, mature change management processes, application data and reports used in multiple business processes for decision making purposes internally.	Moderate network topology including Internet-facing applications, applications are maintained in-house and in the cloud, subject matter expertise frequently required to support business processes, change management processes established, application data and reports used in multiple business processes for internal and external decision making purposes.	Complex network topology including Internet-facing applications, IT infrastructure is not consistent across multiple locations, applications are maintained in-house and in the cloud, subject matter expertise required to support most business processes, change management processes exists but not consistent, application data and reports used in multiple business processes for internal and external decision making purposes.	Complex network topology including Internet-facing applications, IT infrastructure is not consistent across multiple locations, applications are maintained by third party service providers or in the cloud, subject matter expertise required to support most business processes, absence of change management processes, application data and reports used in multiple business processes for internal and external decision making purposes.

Employees' Retirement System of the City of Milwaukee

Administration & Operations Committee Audit Charter May 2018

Purpose

The purpose of this Administration and Operations (A&O) Committee Audit Charter dated May 2018 is to assist the Board Members in fulfilling their oversight responsibilities for the financial reporting process, the system of internal control, the audit process, and the agency's process for monitoring compliance with laws and regulations and the code of conduct. Because of the existing member composition of the A&O Committee as well as the limited number of members, this committee will also have responsibility for the Internal Audit function.

I. AUTHORITY

II. RESPONSIBILITIES

- (1) Financial Statements**
- (2) System of Risk Management**
- (3) Internal Control**
- (4) Internal Audit**
- (5) External Audit of the Financial Statements**
- (6) Agency's Processes for Monitoring Compliance**
- (7) Special Investigations and Whistleblower Mechanism**
- (8) A&O Committee Management and Reporting Responsibilities**

III. MEETINGS

I. AUTHORITY

The A&O Committee has authority to request the Board to conduct or authorize investigation in to any matters within its scope of responsibility. It is empowered to:

- Recommend independent auditors to be engaged by the agency, review and approve the planned and budgeted fees of the independent auditors, review and evaluate the performance of the independent auditors and obtain Board approval for any proposed discharge of the independent auditors.
- Pre-approve all auditing and non-audit services.
- Resolve any disagreements between management and the audit team encountered during the course of the audit including any restrictions on the scope of the work or access to required information.
- Retain independent accountants, or others to advise the A&O Committee or assist in the conduct of an investigation as necessary.
- Seek any information required from employees, all of who are directed to cooperate with the committee's requests.

II. RESPONSIBILITIES

The committee will oversee the following responsibilities:

(1) Financial Statements

- Review significant accounting and reporting issues, including complex or unusual transactions, highly judgmental areas, and recent professional and regulatory pronouncements, and understand their impact on the financial statements.
- Review with management and the external auditors the results of the external audit, including any difficulties encountered.
- Review the annual financial statements and consider whether they are complete, consistent with information known to committee members and reflect appropriate accounting principles.
- Review with the City Attorney or outside legal counsel the status of legal matters that may have an effect on the financial statements.
- Review with management and the external auditors all matters required to be communicated to the committee under generally accepted auditing Standards.
- Understand how management develops interim financial information, and the nature and extent of external and internal auditor involvement.
- Review interim financial reports with management and the external auditors and consider whether they are complete and consistent with the information known to committee members.

(2) System of Risk Management

- Ensure that the organization has a comprehensive policy on risk management.
- Consider the effectiveness of the organization's risk management system, including risks of information technology systems.
- Consider the risks of business relationships with significant vendors and consultants.
- Review reports on management's self-assessment of risks and the mitigations of these risks.
- Understand the scope of the internal auditor's review of risk management over financial reporting and internal controls and obtain reports on significant findings and recommendations with management's responses.
- Hire outside experts and consultants in risk management as necessary.

(3) Internal Control

- Consider the effectiveness of the organization's internal control system, including information technology security and control.
- Understand the scope of internal auditor's and external auditor's review of internal control over financial reporting and its processes and obtain reports on significant findings and recommendations with management's responses.
- Ensure that the organization has a comprehensive policy on internal control and compliance and periodically review the policies on ethics, the code of conduct and fraud.

- Review the role of the internal auditor's involvement in the governance process, including governance documentation and training.
- Ensure that contracts with external service providers contain appropriate record-keeping and audit language.

(4) Internal Audit

- Assure and maintain through the organizational structure of the agency and by other means, the independence of the internal audit process. Review with management the department charter, objectives, plans, activities, staffing, budget, qualifications, and organizational structure of the internal audit function.
- Obtain the information and training needed to enhance the committee members' understanding of the purpose of internal audits so that the committee may adequately oversee the internal audit function.
- Ensure there are no unjustified restrictions or limitations placed on Internal Audit and internal audit staff. Ensure that internal auditors have access to all documents, information and systems in the organization.
- Receive and review all internal audit reports and management letters. Review any changes in the scope of their internal audit. Review the responsiveness and timeliness of management's follow-up activities pertaining to any reported findings and recommendations.
- Review the performance of Internal Audit periodically.

(5) External Audit of the Financial Statements

- Review the external auditor's proposed audit scope and approach, including coordination of audit effort with internal audit. Pre-approve all services to be performed by the external financial statement auditor.
- Review the independence of the external financial statement audit firm by obtaining statements from the auditors on relationships between the audit firm and the organization, including any non-audit services, and discussing these relationships with the audit firm. Obtain from management a listing of all services provided by the external audit firm.
- Review the performance of the external financial statement audit firm.
- Exercise final approval on the request for proposal, the appointment, and retention or discharge of the audit firm.
- Review and approve the audited financial statements, associated management letter, attestation on the effectiveness of the internal control system and procedures for financial reporting, other required auditor communications, and all other auditor reports and communications relating to the financial statements.
- Define the services that the external financial statement auditor is allowed to perform and the services that are prohibited. Ensure production of a report of all costs of and payments to the external financial statement auditor. The listing should separately disclose the costs of the financial statement audit, other attest projects, agreed-upon-procedures and any non-audit services provided.

(6) Agency's Processes for Monitoring Regulatory Compliance

- Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up (including disciplinary action) of any instance of noncompliance.
- Review the findings of any examinations by regulatory agencies and any auditor observations, including investigations of misconduct and fraud.
- Review the process for communicating to all affected parties the ethics policy, code of conduct and fraud policy to agency personnel and for monitoring compliance.
- Obtain regular updates from management and organization legal counsel regarding compliance matters.
- Monitor changes and proposed changes in laws, regulations and rules affecting the agency.

(7) Special Investigations and Whistleblower Mechanism

- Institute and oversee special investigations as needed.
- Provide an appropriate confidential mechanism for whistleblowers to provide information on potentially fraudulent financial reporting or breaches of internal control to the A&O Committee, City Comptroller's Audit Division-Audit Hotline or City of Milwaukee Ethics Board.

(8) A&O Committee Management and Reporting Responsibilities

- Provide an open avenue of communication between internal audit, the external financial statement auditors, other external auditors, and management Board members.
- Confirm annually that all responsibilities outlined in this charter have been carried out and review the charter on an annual basis to determine updates.
- Report annually to the Board, members, retirees and beneficiaries describing the committee's composition, responsibilities and how they were discharged and any other pertinent information, including approval of non-audit services and proposed changes and ensure appropriate disclosure as may be required by law or regulation.
- Evaluate the committee's and individual member's performance on a regular basis and report to the Board.

III. MEETINGS

The A&O Committee will meet at least four times a year on a quarterly basis. All committee members are expected to attend each meeting. The agendas for meetings should be prepared and provided to members in advance, along with appropriate briefing materials. The committee may invite members of management or others to attend meetings and provide pertinent information as necessary. Minutes will be prepared by and filed with the Board members.

Employees' Retirement System of the City of Milwaukee

Internal Audit Charter May 2018

Purpose

The purpose of this Internal Audit Charter dated May 2018, is to assist the internal auditors in fulfilling their mission and fiduciary responsibilities under the oversight of the Administration and Operations (A&O) Committee. The provisions of this charter apply to the activities of the Employees' Retirement System (ERS) of the City of Milwaukee Internal Audit function only, and should be used for no other purpose. This document includes the following topics.

- I. MISSION**
- II. OBJECTIVES & SCOPE**
- III. INDEPENDENCE**
- IV. AUTHORITY**
- V. ACCESS**
- VI. RESPONSIBILITIES & ACCOUNTABILITY**
- VII. PROFESSIONAL STANDARDS**
- VIII. REPORT DISTRIBUTION & FOLLOW-UP**
- IX. RELATIONSHIP TO PREVENTION, DETECTION & CORRECTION ACTIVITIES**
- X. SIGNATURE SECTION**

I. MISSION

The mission of Internal Audit is to provide independent, objective assurance and consulting services designed to add value and improve the operations of ERS. It assists the Board and the Executive Director in accomplishing their oversight responsibilities by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal control, and governance processes. The following are specific tasks to be carried out by Internal Audit to accomplish the mission:

- Supporting the agency's efforts to achieve its objectives through conducting a risk assessment every three years, designing, reviewing and executing an annual audit plan, and providing a wide range of quality independent internal auditing services.
- Assessing the integrity, quality, and efficiency of the systems of internal control.
- Assessing the degree to which ERS complies with various policies, procedures, laws, and regulations in a manner that facilitates operational efficiency, quality of service, and fiduciary responsibility.

- Examining and testing the performance of important control elements.
- Assessing the integrity of the financial reporting processes.
- Communicating results of audit projects through timely written reports delivered to the Board, the Executive Director, and management identified as stakeholders.
- Assessing through follow-up audit projects the degree to which management action plans created in response to recommendations in audit reports are carried out effectively and timely.

II. OBJECTIVES & SCOPE

Auditing Objectives. The objectives of the auditing services are to provide independent assurance to the A&O Committee and management that ERS' assets are safeguarded, operating efficiency is enhanced, and compliance is maintained with prescribed laws and regulations and Board and management policies. These objectives of auditing services include an independent assessment of the agency's risk awareness, reliability and integrity of the organization's data and information, and achievement of the agency's goals and objectives.

Consulting and Advisory Objectives. The objectives of internal audit's consulting and advisory services are to provide ERS management with recommendations for improving processes that will advance the goals and objective to successfully achieve the overall mission of the organization. The objectives will also allow internal audit the opportunity to follow-up with management to ensure action steps were taken to mitigate the risk.

Scope. The scope of work of internal audit is to determine whether the agency's network of risk management, internal control, and governance processes, as designed and represented by management, are adequate and functioning in a manner to ensure:

- Programs are operating within the highest fiduciary standards and are in compliance with the requirements defined in the Federal and State constitutions, laws, and regulations, local government ordinances and rules, and the policies and procedures of the agency.
- Programs and processes are in synchrony with industry best practices, using the best public and private examples and all resources available as benchmarks.
- Significant legislative or regulatory issues impacting the agency are recognized and addressed appropriately and timely.
- Operations, processes and programs are consistent with established missions, objectives and goals and they are being executed in accordance with management's plan.
- Existing policies and procedures are appropriate and updated.
- Internal and external risks are identified and managed.
- Employers appropriately enroll employees, accurately report member earnings, and appropriately report other employee data.
- Interaction with appropriate governance groups occurs as needed.
- Significant financial, managerial, and operating information is accurate, reliable, and timely.

- Resources are acquired economically, used efficiently, and adequately protected.
- Quality service and continuous improvement are fostered in the organization's control process.
- Contractors, including third-party administrators, are meeting the objectives of the contracts, while in conformance with applicable laws, regulations, policies, procedures and best practices and the agency's contract monitoring process is effective to ensure minimal risk.
- Responsibilities and activities of the external financial statement auditors are coordinated with those of the internal auditors in order to provide continuity of audit efforts and to avoid duplication.
- Access for auditors is provided as appropriate.
- Specific operations, processes or programs are reviewed at the request of the A&O Committee, the Board, and management.

Opportunities for improving member service, management of risks, internal control, governance, cost benefit, and the organization's effectiveness and image may be identified during audits. This information will be communicated to the A&O Committee and to appropriate levels of management.

III. INDEPENDENCE

Independent Professional Standards. The A&O Committee recognizes that professional independence requires the auditors have knowledge of operations and appropriate expertise in the subject matter that is being audited. Internal Audit must provide the credentials of any or all staff members upon request of the A&O Committee.

Conflict of Interest. Internal Audit shall discuss any potential issues regarding impairment of independence and/or conflicts of interest and their mitigation(s) with the A&O Committee as necessary.

IV. AUTHORITY

The Internal Audit function is established by the Board of this agency and governed by the A&O Committee. This Charter is approved and all future amendments to it are to be approved by the A&O Committee through a majority vote. This Charter shall be reviewed at least annually and updated as required by the A&O Committee.

Internal Audit functionally reports to the A&O Committee. Meetings are held with the A&O Committee on at least a quarterly basis. The portion of the A&O Committee agenda regarding Internal Audit generally include:

- A discussion of current year Plan status
- Points of emphasis of audit reports issued in the quarter
- Status of audits in process
- Changes or proposed changes to the Plan
- Audit follow-up status reports as necessary (based on exceptions noted)
- Special requests for audits from the Board or from Management with Board approval

- Closed sessions, when necessary, as provided for under the Wisconsin open meetings law

The A&O Committee retains the right to provide input and approve the annual audit plan presented by Internal Audit. The risk assessment and Plan are discussed in the meeting at the end of the quarter in which they are completed. Internal Audit shall inform the A&O Committee of the status of the audit plan and any changes needed. Management may request special audits outside of the plan to be conducted, which must be approved by the A&O Committee. The mission, responsibilities, and workings of the A&O Committee are described in the committee charter.

Internal Audit staff is not authorized to initiate or approve accounting transactions external to those related to the function. Internal Audit staff is not authorized to direct the activities of any agency employee not employed by the function, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.

V. ACCESS

The Internal Audit staff, as appropriate, are granted authority for full, free and unrestricted access to all of the agency's functions, records, files and information systems, personnel, contractors, external auditors, physical properties, rental locations, and any other item relevant to the function, process or department under review. All contracts with vendors shall contain standard audit language enabling the internal auditors and other auditors and specialists to have access to relevant records and information. Documents and information given to Internal Audit shall be handled in the same prudent and confidential manner as by those employees normally accountable for them. All of the ERS employees are required to assist the staff of Internal Audit in fulfilling their audit functions and fiduciary duties.

VI. RESPONSIBILITIES & ACCOUNTABILITY

Internal Audit is responsible for the following in order to meet the mission, objectives and scope of this Charter:

1. Establish policies for conducting Internal Audit activities and directing its technical and administrative functions according to the agency's policies and direction provided by the A&O Committee and professional standards described in Section VII.
2. Perform a risk-assessment every three years and review the flexible annual audit plan that will accomplish the mission, objectives and scope of this Charter. This plan will include some unassigned hours in order to provide flexibility for changing conditions. This plan shall in part be based upon risks and control concerns identified by management.
3. Facilitate the implementation of the audit plan.
4. Implement the annual audit plan, as approved, including, as appropriate, any plan amendments, special tasks or projects requested by management, the Board and the A&O Committee.

5. Obtain updates to follow-up on management action plans as they relate to the recommendations provided by Internal Audit for improvement to ensure the risks are being mitigated timely.
6. Transmit copies of all audit reports and management letters to the A&O Committee.
7. Assess periodically whether the purpose, authority and responsibility, as defined in this Charter, continue to be adequate to accomplish its mission, objectives and scope. The result of this periodic assessment should be communicated to the A&O Committee.
8. Assist in the investigation of significant suspected fraudulent activities within the organization and notify the A&O Committee, the Board and other Executives, as appropriate, of the results.

VII. PROFESSIONAL STANDARDS

Internal Audit shall follow the professional standards of relevant professional organizations. These professional standards include, but are not limited to, the following:

- Institute of Internal Auditors (IIA) Professional Standards and Code of Ethics
- American Institute of Certified Public Accountants (AICPA) Professional Standards and Code of Ethics, as applicable
- Generally Accepted Government Auditing Standards (GAGAS) from the United States General Accounting Office (GAO), as applicable

VIII. REPORT DISTRIBUTION & FOLLOW-UP

Draft audit reports are first distributed to the Executive Director or their designee for comments. After comment, they are then distributed to the applicable department head. Internal Audit is responsible for obtaining management responses and issuing the final version of the audit report according to the following time schedule:

- Once a draft report is issued to a department head, 15 business days are allowed for management responses to be prepared and forwarded to Internal Audit. Internal Audit may extend the deadline, though the maximum number of business days for a response will be 25 days.
- Upon receipt of acceptable management responses, Internal Audit has 10 business days to issue the final version of the report.
- In cases where the department under review does not meet the above schedule, Internal Audit has the authority to issue the report without management responses to the chairman of the A&O Committee.

Final audit reports are distributed as follows:

- The department head, under review, receives a complete copy of the full report.
- The Executive Director, the Board, and the A&O Committee also receive a copy of the full report.

IX. RELATIONSHIP TO PREVENTION, DETECTION AND CORRECTION ACTIVITIES

Internal Audit strives to participate in the initial stages of major agency-wide projects so that risks can be appropriately managed and internal controls instituted in the design phase in order to prevent problems and minimize the associated costs. It recognizes that it is more expensive to detect and correct problems than it is to prevent them in the initial stages of a project.

X. SIGNATURE SECTION

The A&O Committee reviewed and adopted this Internal Audit Charter in May 2018, and transmitted it to the Board. The Internal Audit Charter is effective immediately and is hereby signed by the following persons who have authority and responsibilities under this Charter.

Chair, A&O Committee

Date

Chairman, ERS Board

Date

Executive Director

Date



Administration and Operations Committee

ERS IT Portfolio Report

May 17th 2018

Agenda

- Information Technology Projects Summary
- Application Stats
- What's Next
- IT Portfolio

Information Technology Projects Summary

- IT Server Administrator Position (In progress)
- Storage Area Network (SAN) Replacement (In progress)
- Struts 2 and Optimization (In Progress)
- WebSphere, SQL 2012 and Windows Server Upgrades for MERITs (In Progress)
- ERS Phone System Enhancements (In Progress)
- Experis/IT Vulnerability Audit (Completed)

Application Stats

Category	High Priority	Low Priority	Total
Current Inventory	13	1	14
PIR	4	0	4
CCR	9	1	10
Pending/Hold	1	0	1
Deployed(Awaiting Next stage) /Ready for Production	3	0	3
Net Current Inventory	9	1	10

What's Next...

- Conduct interviews for Server Administrator
- Complete Risk Assessment
- Continue SAN Upgrade (Order hardware)
- MERITS Windows Server, SQL and WebSphere Upgrades
- ERS Phone System Cutover
- Struts/Optimization
- Complete IT Disaster Recovery Test to Femrite

Glossary of Terms

- *Applications/Acronyms Definitions:*

- **Perforce:** Primary application the development team uses to make code changes to MERITS. It provides the environments for testing, development and CCR/PIR deployments.
- **AccPac:** Accounting software that supports the general ledger.
- **Altiris:** Asset management software the technical team uses to inventory and support all IT assets. This application manages updates to computers, imaging, and software distribution from a centralized console.
- **Websphere Application Server (WAS):** The application server that we use to connect Web site users to Member Self Service and other MERITS related web services.
- **JAVA:** The programming language that MERITS was developed in and is running.
- **PIR:** Problem Incident Report- A person reports a bug with the application and requests priority resolution.
- **CCR:** Change Control Request- A person request a new feature, change or enhancement to MERITS.
- **Retirement Application Processing (RAP):** Functional module in Merits that processes retirement applications through workflow.
- **Merits Program Lifecycle Management (MPLM):** Process to upgrade, patch and keep current all of the MERITS related subsystems and ERS business applications.
- **Storage Area Network (SAN):** Primary storage technology used to centrally store all ERS data and manages Disaster Recovery.
- **Disaster Recovery Plan (DRP):** The technical planning, design and testing of all IT systems and staff to ensure that all technical systems can run at the off site location in Madison, WI called Femrite. IT staff does semi annually testing to ensure all applications and IT services are up and running within the designated service level objectives.
- **Recovery Time Objective/Recovery Point Objective (RTO/RPO):** These are I.T. service level goals for the amount of time it takes to cutover I.T. services to the Femrite location and the point in time (per the last backup) where we recover at. Currently at 24 hours recovery time and 8 hours for any loss of data. I.T. currently exceeds this expectation based off the last 2 tests.
- **Business Continuity Plan (BCP):** The process that ensure the ERS can continue running its services and daily operations at the Remote Office in the event that the primary location is not accessible. We engage ERS business users to physically work at the Remote office location and document the results on a reoccurring basis.
- **Remote Office (RO):** Backup Remote work facility located at TPP 10850 W. Park Place. It is connected to both the 789 N. Water Street facility and the Femrite Data Center in Madison, and users can physically work there and connect to any needed data center.
- **MERITS Optimization:** Project approved in 2012 to go through all 17 application modules in MERITS and clean up code, ensure best practices are implemented, SQL stored procedures for faster performance, reporting and user experience. It is the clean up of any non ERS related code that may have been carried over from the original jClarety (HP software) implementation.
- **ARIS:** Web based software used for mapping legal opinions to MERITS workflow processes and procedures.

Portfolio as of May 1, 2018

Project Health	% Complete	Project Priority	Complexity (S / M / L)	Project Name	Project Mgr	Description	Strategic Goal	Status	External Vendor Required: Y/N	Actual Start Date	Target Completion Date	Estimates (Hours)	Actuals (Hours)	Hours Variance = Estimates - Actuals	Hardware/Software & External Labor Budget (\$)	Actual Spent-to-Date on Hardware /Software & External Labor (\$)	Estimate to Completion (ETC) (of Hardware/ Software & External Labor Costs)
G	95%	1	S	IT Vulnerability Audit @	Reid	Internal/External penetration testing	n/a	IP	Y	2/1/18	3/16/18	100	95	5	\$23,800	\$22,610	\$1,190
G	95%	2	L	2018 Network Replacement	Benedict	Create a more resilient network with all gear under support. Replaces Network Re-Architecture	1	IP	Y	2/1/18	6/1/18	511	519	(8)	\$374,118	\$374,692	(\$574)
G	5%	3	M	SQL Server and Windows Upgrade	Manchu	MPLM project; Java and Websphere have reached end-of-life.	1	IP	Y	4/16/18	8/24/18	920	66	854	\$45,463	\$2,977	\$42,486
G	50%	4	L	MERITS Code Deployment Process Review@	Manchu	Review and improve process of code deployment	1	IP	Y	3/26/18	7/1/18	199	42	157	N/A	\$0	N/A
Y	75%	5	L	Phone System Enhancements	Zaffiro	Create a better phone experience for members and staff	4	IP	Y	3/23/18	4/27/18	127	96	32	\$7,340	\$7,040	\$300
G	68%	6	L	Struts 2 Upgrade (functional areas besides MAM)	Manchu	Software development upgrade all functional areas but MAM.	1	IP	Y	10/17/16	8/15/19	11,438	5,579	5,860	\$730,290	\$261,005	\$469,286
G	70%	7	L	CAD/CAR/GL Optimization	Manchu	MERITS optimization & clean-up of Cash Dispersements, Cash Receipts, and General Ledger	1	IP	N	10/6/17	12/27/18	1,738	891	847	N/A	N/A	N/A

Pipeline Projects (Next 6 months)

SAN Upgrade (Raynal)

- Green =

On Target - No Significant Issues
- Yellow =

On Watch List – Issues Being Addressed
- Red =

Project cannot move forward as planned without management attention or approval.

- NS

 = Not Started
- OH

 = On Hold
- @

 = Activity (no charter)
- IP

 = In Process
- C

 = Completed

Special Note: Struts 2 Upgrade costs are part of the 3-year HP maintenance contract.

Completed Projects & Tasks in Last 12 Months	Finished	Hours / \$ Spent
2017 Desktop Rotation (Powell)	5/8/2017	269 hrs / \$39,520
Member Education Videos [POC] (Zaffiro)	5/19/2017	67 hrs / \$1,889
Websphere Server Patching @ (Manchu)	5/26/2017	81 hrs / \$8,762
VMware vSphere Upgrade @ (Raynal)	6/15/2017	73 hrs / N/A
IT General Controls Audit @ (Reid)	6/20/2017	39 hrs / \$13,320
Printer Maint. Contract @ (Zaffiro)	6/21/2017	64.5 hrs / N/A
BAA / PAP Optimization (Manchu)	7/7/2017	3,129 hrs / N/A
DR Test (IT Only) @ (Dugan)	7/11/2017	67.5 hrs / N/A
Install Print Monitoring Software @ (Xiong/Zaffiro)	9/21/2017	57.7 / N/A

	Finished	Hours / \$ Spent
Upgrade Network Infrastructure Firmware @ (Benedict)	9/22/2017	48 hrs / N/A
BCP Test @ (Siddiqui)	9/28/2017	17 hrs / N/A
HCP Optimization (Manchu)	10/2/2017	958.3 hrs / N/A
CMERS.com Upgrade & Redesign (Zaffiro)	11/13/2017	149.75 hrs / \$18,600
100 Meg Femrite Cutover @ (Xiong)	1/5/2018	18.5 hrs / N/A
IT Strategic Planning @ (Reid)	1/29/2018	100 hours / N/A
Social Engineering Audit @ (Reid)	1/31/2018	45 hours / \$9,600
Altiris Upgrade (Raynal)	2/9/2018	535 hours / \$26,090
Video Conferencing Options @ (John)	3/21/2018	55.3 hours / \$5,525
OSC Optimization (Manchu)	4/9/2018	975.25 hours / \$75,444

Organizational/Personnel Update

Administration and Operations Committee

Thursday, May 17, 2018

- ERS is working with DER to fill the following vacancies:
 - Pension Accounting Manager
 - ERS Server Administrator
 - Records Technician II
 - Administrative Assistant II

