SCHOOL EMPLOYEES RETIREMENT SYSTEM OF OHIO
300 E. BROAD ST., SUITE 100 • COLUMBUS, OHIO 43215-3746
614-222-5853 • Toll-Free 800-878-5853 • www.ohsers.org

Request for Proposal - External Quality Assessment of Internal Audit Office
Questions Submitted to SERS

Question 1: **Are you able to share the anticipated budget for this project?**

Answer: The prior assessment was performed in late 2017 with a cost of $18,200 (included 2-3 onsite travel days). This review can be performed remote, in person or both.

Question 2: **Is this anticipated to be a full external quality assessment or a self-assessment with independent validation?**

Answer: This will be a full external quality assessment.

Question 3: **Is there an established QAIP for SERS?**

Answer: Yes. Internal Audit is a one-person department with an established QAIP program that will be provided to the successful bidder.

Question 4: **What is the anticipated internal audit year / scope period?**

Answer: The primary period of review will involve FY22 (July 1, 2021 through June 30, 2022). Prior data is available if desired by the selected vendor.

Question 5: **How many audits were completed in the most recent internal audit plan in scope for this assessment?**

Answer: The FY22 Internal Audit Plan's status in mid-June included:

<u>12 Projects Completed</u>

- 3 compliance audits, 2 operational audits, 1 outsourced IT audit
- QAR Self-Assessment, Audit Committee Annual Report, FY23 Audit Planning, 2 minor consultant engagements, and Continuous auditing/monitoring project

One audit currently in progress which will be completed in July and one audit on hold.

Question 6: **Does the audit plan include any activities that may not be covered by the IPPF?**

Answer: FY22's audit plan activities were all included by the IPPF. Certain smaller engagements, compliance reviews and consulting/admin projects have reduced documentation requirements.

Question 7: **Does SERS have a preference as to whether the work is conducted on-site, hybrid or remote?**

Answer: SERS is flexible to the bidder's preferred approach to deliver a quality review. SERS will accommodate schedules, provide access and coordinate document exchange. The prior review combined remote (pre-work, report writing) and onsite interviews/ document reviews over a few days. Some hybrid component is expected as most SERS employees work a hybrid work schedule.

Question 8: **What GRC system is utilized by the internal audit department?**

Answer: Audit workpapers not contained within a GRC system, rather they are prepared within Microsoft Word, Excel, Powerpoint, and Adobe Acrobat. Files can be securely exchanged via the bidder's secure portal or SERS' Sharefile application. Firms should indicate in their Responses how they prefer to securely exchange files.

Question 9: **Can successful bidder obtain GRC direct access?**

Answer: Please see response to Question 8.

Question 10: **Can the successful bidder review the most recent QAR or self-assessment and what actions may have been taken?**

Answer: The July 2017 External Quality Assessment is attached as Appendix A. The Internal Audit activity fully complied with *IIA Standards* and Code of Ethics. Only minor comments were reported and all recommendations were implemented.

Question 11: **When was the last quality assessment review completed?**

Answer: Please see response to Question 10.

Question 12: **Can successful bidder obtain a copy of the QAR report?**

Answer: Please see response to Question 10.

Question 13: **Are there any known issues with the conduct of IAD's work or related noncompliance, please elaborate it any?**

Answer: No.

Question 14: **Was the prior QAR report a clean assessment, or were issues noted?**

Answer: Please see response to Question 10.

Appendix A

EXTERNAL QUALITY ASSESSMENT OF INTERNAL AUDIT ACTIVITIES

School Employees Retirement System (SERS) of Ohio

July 2017

plante moran

audit • tax • consulting • wealth management

TABLE OF CONTENTS

plante moran

Plante & Moran, PLLC
Suite 600
65 E. State St.
Columbus, OH 43215
Tel: 614.849.3000
Fax: 614.221.3535
plantemoran.com

EXECUTIVE SUMMARY

As requested by the Audit Committee chairperson, Plante Moran, PLLC conducted an external quality assessment (QA) of the internal audit (IA) activity of the School Employees Retirement System (SERS) of Ohio. The principal objectives of the QA were to assess the IA activity's conformance to The Institute of Internal Auditors' (IIA's) *International Standards for the Professional Practice of Internal Auditing* (*Standards*), evaluate the IA activity's effectiveness in carrying out its mission (as set forth in its charter and expressed in the expectations of SERS' management), and identify opportunities to enhance its management and work processes, as well as its value to SERS.

OPINION AS TO CONFORMANCE TO THE *STANDARDS*

It is our overall opinion that the IA activity generally conforms to the Standards and Code of Ethics. For a detailed list of conformance with individual Standards, please see attachment A. The QA team identified opportunities for further improvement, details of which are provided in this report.

The IIA's Quality Assessment Manual suggests a scale of three ratings, “Generally Conforms,” “Partially Conforms,” and “Does Not Conform.” “Generally Conforms” means that an IA activity has a charter, policies, and processes that are judged to be in conformance with the Standards. “Partially Conforms” means deficiencies in practice are noted that are judged to deviate from the Standards, but these deficiencies did not preclude the IA activity from performing its responsibilities in an acceptable manner. “Does Not Conform” means deficiencies in practice are judged to be so significant as to seriously impair or preclude the IA activity from performing adequately in all or in significant areas of its responsibilities.

SCOPE AND METHODOLOGY

As part of the preparation for the quality assessment, the Chief Audit Officer (CAO) prepared an advanced preparation document with detailed information and made available surveys from auditees and a representative sample of SERS executives. Before commencement of the onsite work by the quality assessment team on July 24, 2017, the team leader conducted a preliminary meeting with SERS to gather additional background information, selected executives for interviews during the onsite fieldwork, and finalized planning and administrative arrangements for the QA. As part of the review, extensive interviews were held with SERS' Audit Committee (AC) chairperson, executives (including Executive Director, Deputy Executive Director, Chief Financial Officer, General Counsel, and Enterprise Risk Management Officer), external auditors, and the CAO. The IA activity's risk assessment and audit planning processes, audit tools and methodologies, engagement management processes, and a representative sample of the IA activity's workpapers and reports were also reviewed.

RECOMMENDATIONS AND OBSERVATIONS: SUMMARY

The IA activity environment where we performed our review is well structured and progressive where the *Standards* are understood, and the CAO is endeavoring to provide useful audit tools and implement appropriate practices. Consequently, our comments and recommendations are intended to build on this foundation already in place in the IA activity.

Recommendations and observations are divided into three groups:

- First, is that which concerns the AC and suggest actions by them.
- Second, are those that relate to the IA activity's structure, staffing, deployment of resources, and similar matters that should be implemented within the IA activity, with support from senior management.
- Third, are observations that recognize best practices employed by the IA activity leading to a level of performance beyond generally conforming to the mandatory guidance of The IIA's International Professional Practices Framework (IPPF).

Highlights of the more significant recommendations and observations are summarized below, with detailed descriptions following later in the report.

PART I – MATTER FOR CONSIDERATION BY SERS AUDIT COMMITTEE

1. **Revise the AC Charter.** The AC should consider documenting in the AC Charter their purpose and responsibilities regarding compliance. (Leading Practice)

PART II—RECOMMENDATIONS FOR THE INTERNAL AUDIT ACTIVITY

1. **Consider Updating Risk Assessment Format and Presentation.** The CAO should consider de-bundling HIPAA and Cybersecurity into their own risks and provide clarification on the inclusion and non-reliance of external audit work. (Standard 2010)

2. **Perform Assessment of Information Technology Governance Program.** The CAO should assess whether the information technology (IT) governance of the organization supports the organization's strategies and objectives. (Standard 2110)

PART III—OBSERVATION OF BEST PRACTICES

1. **Summarize Findings Documentation.** The CAO should consider establishing a summary of findings document to capture all findings from the audit engagement in one stand-alone workpaper. (Standard 2330)

Thank you for the opportunity to be of service to SERS. We will be pleased to respond to further questions concerning this report and furnish any desired information.

Jeffrey S. Wright

Jeffrey S. Wright, CIA
Senior Manager – Enterprise Risk Services
Plante & Moran PLLC

RECOMMENDATIONS AND OBSERVATIONS: DETAILS

PART I—RECOMMENDATION FOR CONSIDERATION OF SERS AUDIT COMMITTEE

These recommendations originated principally from the comments received from the interviews with selected executives, and follow-up of these matters. All are of direct importance to enhancing effectiveness and added value of the IA activity.

1. REVISE THE AUDIT COMMITTEE CHARTER

The IIA Model AC Charter recommends:

- Purpose Section: the purpose of the AC includes the review of the organization's process for monitoring compliance with laws and regulations and the code of conduct.

- Responsibilities Section: the responsibilities of the AC includes assessment of Compliance activities including:

  - ○ 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 instances of noncompliance.

  - ○ Review the findings of any examinations by regulatory agencies, and any auditor observations.

  - ○ Review the process for communicating the code of conduct to company personnel, and for monitoring compliance therewith.

  - ○ Obtain regular updates from management and company legal counsel regarding compliance matters.

The SERS AC Charter currently does not have these requirements.

RECOMMENDATIONS

The AC should consider documenting in the AC Charter that the AC is responsible for Compliance in the purpose and responsibilities sections.

INTERNAL AUDIT RESPONSE

- **The CAO agrees with the recommendation and will work with the Audit Committee and management to include the changes in an updated AC charter.**

PART II—RECOMMENDATIONS FOR THE INTERNAL AUDIT ACTIVITY

1. CONSIDER UPDATING RISK ASSESSMENT FORMAT AND PRESENTATION

Standard 2010 requires the CAO must establish a risk-based plan to determine the priorities of the IA activity, consistent with the organizations goals.

We reviewed the Fiscal Year 2018 IA Risk Assessment and noted the following:

- Certain IT risks are bundled together that are usually addressed separately. For example, SMART application security, HIPAA, and cybersecurity are all grouped into one risk (Enterprise Security Program).
- The Risk Assessment and IA Plan allocated internal audit resources to 14 of the top 18 risk areas to the organization over the last 3 fiscal years. However, we noted 4 top risk areas without IA hour allocations due to the external auditors performing substantive tests in these areas and 2 of those 4 having additional coverage from SERS monitoring functions. As a result, the CAO has not prioritized internal audit resources to the following 4 risk areas:
    - Member Services - Retirement benefits/ calculations/ services
    - Investments - Alternative Investments: Real Estate, Private Equity, Hedge Funds
    - Finance - Investment Accounting - Custody and Master Record keeper
    - Member Services - Survivor benefits/ calculations
- The Finance – Payment Processing / Payables auditable area currently has an Impact of Fraud, Waste or Data Loss (category F – 15%) rating of 4.
- The Human Resources – Employee Payroll, Timekeeping & Leave auditable area currently shows the Last Year Audited of FY 2016.

RECOMMENDATION

The CAO should consider the following:

- Consider de-bundling HIPAA and Cybersecurity into their own risks as these audits will have distinctly different audit scope, approach and objectives.
- Include additional clarification in the Risk Assessment in the note under 'The 3 Lines of Defense Model' section that SERS is not relying on the work of the

external auditors, rather avoiding duplication of efforts by not allocating IA hours to these areas.

- Change the category F fraud rating of Finance – Payment Processing/ Payable to a 5 due to the increase in volume and sophistication of fraud attempts related to accounts payable in the current market environment.

- Delete the reference to FY 2016 in the Last Year Audited column as payroll process was not audited in its entirety.

INTERNAL AUDIT RESPONSE

The CAO agrees with the recommendation and will de-bundle HIPAA and cybersecurity into separate auditable units in FY19's audit plan. The CAO will add the clarifying external auditor language and other suggested changes into FY19's audit plan.

2. PERFORM ASSESSMENT OF THE INFORMATION TECHNOLOGY GOVERNANCE PROGRAM

Standard 2110.A2 – The CAO must assess whether the information technology (IT) governance of the organization supports the organization's strategies and objectives.

The CAO participates on the IT Steering Committee and is tracking the IT findings noted in the most recent fiduciary audit, however, a formal assessment of the IT Governance program is not presented to the Audit Committee.

RECOMMENDATION

CAO should consider adding a dedicated IT governance audit to the IA plan with issuance of a formal assessment to the AC. We noted there is 16 hours allocated in the FY 2018 budget.

INTERNAL AUDIT RESPONSE

The CAO agrees with the recommendation and will continue to evaluate the current and future evolution of the IT governance structure.

PART III—OBSERVATION OF BEST PRACTICES

1. SUMMARIZE FINDINGS DOCUMENTATION

Standard 2330 requires internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.

The SERS CAO prepares sufficient workpaper documentation to support the results and conclusions in the audit reports. However, the support for each finding is dispersed throughout the various workpapers of each audit engagement and does not contain the final disposition. We recommend the CAO create a summary of findings document to inventory all the findings discovered throughout the engagement workpapers. In addition, list the final disposition of each finding as to whether it was disclosed in the final report or the reasons for not being reported.

INTERNAL AUDIT RESPONSE

The CAO agrees with the recommendation and will incorporate a comment tracker summary sheet within audit engagements.

ATTACHMENT A

School Employees Retirement System (SERS) of Ohio Quality Assessment Evaluation Summary

(GC = Generally Conforms, PC = Partially Conforms, DNC = Does Not Conform)

Quality Assessment Evaluation Summary—Overall Evaluation	GC	PC	DNC
OVERALL EVALUATION	X		

Quality Assessment Evaluation Summary—Major/Supporting Standards		GC	PC	DNC
1000	**Purpose, Authority, and Responsibility**	X		
1010	Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the IA Charter	X		
1100	**Independence and Objectivity**	X		
1110	Organizational Independence	X		
1111	Direct Interaction with the Board	X		
1112	Chief Audit Executive – Roles Beyond External Auditing	X		
1120	Individual Objectivity	X		
1130	Impairment to Independence or Objectivity	X		
1200	**Proficiency and Due Professional Care**	X		
1210	Proficiency	X		
1220	Due Professional Care	X		
1230	Continuing Professional Development	X		
1300	**Quality Assurance and Improvement Program**	X		
1310	Requirements of the Quality Assurance and Improvement Program	X		

Quality Assessment Evaluation Summary—Major/Supporting Standards		GC	PC	DNC
1311	Internal Assessments	X		
1312	External Assessments	X		
1320	Reporting on the Quality Assurance and Improvement Program	X		
1321	Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"	X		
1322	Disclosure of Nonconformance	X		
2000	**Managing the Internal Audit Activity**	X		
2010	Planning	X		
2020	Communication and Approval	X		
2030	Resource Management	X		
2040	Policies and Procedures	X		
2050	Coordination	X		
2060	Reporting to Senior Management and the Board	X		
2070	External Service Provider and Organizational Responsibility for Internal Auditing	X		
2100	**Nature of Work**	X		
2110	Governance	X		
2120	Risk Management	X		
2130	Control	X		
2200	**Engagement Planning**	X		
2201	Planning Considerations	X		
2210	Engagement Objectives	X		

Quality Assessment Evaluation Summary—Major/Supporting Standards		**GC**	**PC**	**DNC**
2220	Engagement Scope	X		
2230	Engagement Resource Allocation	X		
2240	Engagement Work Program	X		
2300	**Performing the Engagement**	X		
2310	Identifying Information	X		
2320	Analysis and Evaluation	X		
2330	Documenting Information	X		
2340	Engagement Supervision	X		
2400	**Communicating Results**	X		
2410	Criteria for Communicating	X		
2420	Quality of Communications	X		
2421	Errors and Omissions	X		
2430	Use of “Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*”	X		
2431	Engagement Disclosure of Nonconformance	X		
2440	Disseminating Results	X		
2450	Overall Opinions	X		
2500	**Monitoring Progress**	X		
2600	**Communicating the Acceptance of Risks**	X		
	The IIA’s Code of Ethics	X		

RATING DEFINITIONS

“Generally Conforms” means the assessor has concluded the following:

- For individual standards, that the internal audit activity conforms to the requirements of the standard (e.g., 1000, 1010, 2000, 2010, etc.) or elements of the Code of Ethics (both Principles and Rules of Conduct) in all material respects.

- For the sections (Attribute and Performance) and major categories (e.g., 1000, 1100, 2000, 2100, etc.), the IA activity achieves general conformity to a majority of the individual standards and/or elements of the Code of Ethics, and at least partial conformity to others, within the section/category.

- For the IA activity overall, there may be opportunities for improvement, but these should not represent situations where the IA activity has not implemented the *Standards* or the Code of Ethics, has not applied them effectively, or has not achieved their stated objectives.

“Partially Conforms” means the assessor has concluded the following:

- For individual standards, the IA activity is making good faith efforts to conform to the requirements of the standard (e.g., 1000, 1010, 2000, 2010, etc.) or element of the Code of Ethics (both Principles and Rules of Conduct) but falls short of achieving some major objectives.

- For the sections (Attribute and Performance) and major categories (e.g., 1000, 1100, 2000, 2100, etc.), the IA activity partially achieves conformance with a majority of the individual standards within the section/category and/or elements of the Code of Ethics.

- For the IA activity overall, there will be significant opportunities for improvement in effectively applying the *Standards* or Code of Ethics and/or achieving their objectives. Some deficiencies may be beyond the control of the IA activity and may result in recommendations to senior management or the board of the organization.

“Does Not Conform” means the assessor has concluded the following:

- For individual standards, the IA activity is not aware of, is not making good faith efforts to conform to, or is failing to achieve many/all of the objectives of the standard (e.g., 1000, 1010, 2000, 2010, etc.) and/or elements of the Code of Ethics (both Principles and Rules of Conduct).

- For the sections (Attribute and Performance) and major categories (e.g., 1000, 1100, 2000, 2100, etc.), the IA activity does not achieve conformance with a majority of the individual standards within the section/category and/or elements of the Code of Ethics.

- For the IA activity overall, there will be deficiencies that will usually have a significant negative impact on the IA activity's effectiveness and its potential to add value to the organization. These may also represent significant opportunities for improvement, including actions by senior management or the board.