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

RICHARD STENSRUD
Executive Director

JOSEPH MAROTTA
Interim Deputy Executive Director

January 2, 2019

Bethany Rhodes, Director/General Counsel
Ohio Retirement Study Council
30 E. Broad St., 2nd Floor
Columbus, OH 43215

Dear Ms. Rhodes:

Pursuant to R.C. 3309.044, enclosed please find a report of actions taken by the Audit Committee of the SERS Retirement Board for calendar year 2018. The attached report was prepared by SERS' Chief Audit Officer, Joe Bell, and incorporates the reporting format approved by the Ohio Retirement Study Council.

Please feel free to contact Joe Bell or myself if you have any questions.

Sincerely,

Richard Stensrud

Richard Stensrud
Executive Director

Enclosure

School Employees Retirement System of Ohio
CY2018 Annual Audit Report

Closed Audits: Recommendations

Audit Area	Risk Rating [1]	Scope	Recommendations	Mgmt.'s Response	Implemented	Implementation or Target Implementation
Information Security Program – Maturity Assessment (Jan. 2018)	High	Information Security (IS) Program Review included: A. Program Governance, Management & Culture B. Security Risk Mgmt, Planning, Budget & Resources C. Security Controls, Compliance & Access Management D. Threat Detection and Response E. Employee Behavior & Risk Awareness F. Incident Response and Crisis Management G. Third-Party Risk Management	1. Consolidate cybersecurity practices into IS program for consistent communication of risk and risk remediation activities 2. Establish risk management plan with quantitative risk metrics to track/remedy cybersecurity risks 3. Adopt risk management framework to drive the setting of clear and measurable risk management activities and goals 4. Perform full inventory of logical and physical assets within SERS' information system 5. Conduct full inventory of data and business processes to identify gaps in SERS' risk remediation plans 6. Establish continuous vulnerability management plan 7. Develop protocols for risk notification and remediation for business, data & application owners with escalation process for untreated high-priority risks 8. Establish strong change management plan to track all changes through the life cycle of the application and assets 9. Establish metrics to build a Common Operating Picture 10. Include information sharing and communications plan for sharing cybersecurity information externally	1. See NOTE 2. See NOTE 3. See NOTE 4. See NOTE 5. See NOTE 6. See NOTE 7. See NOTE 8. See NOTE 9. See NOTE 10. See NOTE NOTE: adequate per auditor	1. No 2. No 3. No 4. No 5. No 6. No 7. No 8. No 9. No 10. No NOTE: 3 years to address	1. 2020 2. 2020 3. 2020 4. 2020 5. 2020 6. 2020 7. 2020 8. 2020 9. 2020 10. 2020 NOTE: 3 years to fully address
		Comments: External firm evaluated maturity level of Information Security program. Assessment identified maturity levels, evaluated gaps and prioritized recommendations. Maturity assessed at varying levels of implementation with comments aimed at improving maturity level. All 10 comments were considered high priorities but were not risk-rated using below rating levels. The comments will require significant effort to fully address and are estimated to span 3 years based on many factors (e.g. resource allocation and staff availability). Scope Limit: Point in time maturity level assessment. Intended scope of inquiry and observation, not direct examination or testing of controls.				

[1] Risk Rating Levels:
High: Requires immediate attention and remediation.
Moderate (Mod.): Requires near-term attention.
Low: Improvements possible but does not require attention in immediate or near-term.

Closed Audits: Recommendations (cont.)

Audit Area	Risk Rating	Scope	Recommendations	Management's Response	Implemented	Implementation or Target Implementation
Employer Reporting and Contributions (March 2018)	High	<u>Finance Department</u> Review included: A. Employer reporting and contributions B. Transaction reconciliation, monitoring, handling of over/underpayment C. Communication (employers; transmission/ sensitive data handling)	1. Update written policies/procedures for employer reporting and contribution processes (Mod.) 2. Review employers with more than one active administrator account; review SERS' employee duties for incompatible roles (Mod.) 3. Develop risk-based strategy & monitoring approach to lessen risks of employer self-reporting (Mod.) 4. Conduct ongoing monitoring to avoid large or aged payments due from employers (Low) 5. Evaluate necessity and frequency for requiring employer web administrators password changes (Low) 6. Establish ongoing monitoring for employer contribution reporting and ensure timely escalation of higher risk items (Low) 7. Timelines for penalties should be communicated to employers, along with pre-implementation testing (Low) 8. Enact protocol for employers to notify SERS if a breach/fraud has occurred at an employer (Low)	1. Update policies and procedures. 2. Review/modify those with more than one active admin account; review SERS employee duties. 3. Develop risk-based employer audit plan. 4. Monitoring handled during annual employer statement process. 5. Will review with risk management process. 6. Created desk practice to query and escalate large outstanding items. 7. Testing and communication occurred before enacting penalties. 8. Will develop a communication protocol for employers.	1. Yes 2. Yes 3. Yes 4. Yes 5. No 6. Yes 7. Yes 8. No	1. Sept. 2018 2. Sept. 2018 3. Dec. 2018 4. Aug. 2018 5. June 2019 6. Oct. 2018 7. Aug. 2018 8. June 2019
		Comments: Finance's controls were operating effectively to ensure employer reporting and contribution processes were properly designed and operating effectively in accordance with laws, policies and procedures. No significant issues were identified. This audit focused on employer reporting and contributions for the audit period July through December 2017 and scope of review excluded testing of census data information that is annually performed by the external auditors. Penalties for late reporting were suspended during the audit due to the SMART and eSERS upgrades and were excluded from the scope of this audit. Scope of review includes a limited access control review, not a detailed review of eSERS, SMART or other SERS' IT applications.				

Closed Audits: Recommendations (cont.)

Audit Area	Risk Rating	Scope	Recommendations	Management's Response	Implemented	Implementation or Target Implementation
IT Governance (April 2018)	Mod.	<u>IT Department</u> Review included: A. Strategic alignment B. Risk management C. Value delivery D. Performance measurement E. Resources management	1. Provide roadmap of IT's strategic direction, key annual activities and periodic progress updates. 2. Ensure metrics help oversight functions better assess IT performance. Coordinate IT and IS roles when reporting IT and security risks. 3. Provide more informative analysis on IT decision-making. Facilitate leadership discussion on IT and security risks. 4. Refine and communicate performance metrics. 5. Include IS representative on new tool/ technology decisions and change management processes. NOTE: Comments not risk-rated and no significant issues were identified.	1. Facilitate annual strategic plan with leadership, present to Board and provide progress updates. 2. Expand metric tracking and reporting as it implements ITIL practices. Once ERM is operational, IT will follow the framework to communicate the IT risk profile. 3. Developed and shared sourcing policy for procurement decisions. Developed SMART software test automation to improve quality and testing cycle time of releases. 4. IT tracks and reports system-related metrics and will modify as needed. 5. IT continues to seek IS integration opportunities in change management procedures.	1. No 2. No 3. Yes 4. Yes 5. Yes	1. June 2019 2. Sept. 2019 3. Oct. 2018 4. June 2018 5. June 2018
		Comments: The IT governance mechanisms, processes, and organizational structures are effectively designed to ensure: ➢ IT's strategies are aligned with organizational objectives ➢ Risks are identified and managed properly ➢ IT investments are optimized to deliver value to the organization ➢ IT performance is defined, measured, and reported using meaningful metrics ➢ IT resources are managed effectively This assessment reviewed the IT governance structure and controls in place. The ITIL framework was recently selected and is in the initial stages of implementation. As such, internal audit concentrated on control design adequacy and interviews of select individuals involved or impacted by IT governance activities. There was limited focus on information security due to a recently completed IS capability maturity review.			

Closed Audits: Recommendations (cont.)

Audit Area	Risk Rating	Scope	Recommendations	Management's Response	Implemented	Implementation or Target Implementation
SMART Operational Review (Oct. 2018)	High	Multi-Department Review included: A. Inbound/ outbound documentation B. Scanning C. Workflow/ processing D. Transaction handling & reconciliations E. Correspondence F. Training	1. Consider completeness control totals to validate input/output points in SMART 2. Continue to reexamine resource needs as part of post-SMART evaluation 3. Automate certain ad hoc management queries to encourage routine monitoring 4. Expand metrics to aid process monitoring 5. Prepare consistent, up to date written procedure documentation 6. Continue agile-based change management to consolidate multi-function testing timely 7. Continue to develop a workflow to track Member Self Service (MSS) account changes NOTE: Comments not risk-rated and no significant issues were identified.	1. Evaluate if completeness concerns emerge 2. Ongoing review; consider in strategic plan 3. Ad hoc reporting project has begun 4. Ongoing review; consider in strategic plan 5. Ongoing review to update documentation 6. Agile-based testing has begun, where appropriate 7. Workflow for tracking MSS changes has begun	1. No 2. No 3. No 4. No 5. No 6. No 7. No	1. As needed 2. June 2019 3. June 2019 4. June 2019 5. Dec. 2019 6. June 2019 7. Mar. 2019
		Comments: Controls were properly designed and placed into operation to ensure: ➢ Complete, accurate, and timely mail and print shop intake, routing, and outbound processes to customer ➢ Timely, accurate document scanning for records management imaging ➢ Adequate access, workflow routing, application development/change management, system monitoring, and business continuity ➢ Accurate, complete and timely records and calculations for transaction processing and monitoring of collections, payments and decisions ➢ Proper and consistent use of communication and approved correspondence forms ➢ Adequate training resources exist for employers, members, and SERS' employees Engagement was a high-level operational review of controls of key processes impacted by SMART. Testing of internal control design concentrated on inquiry, observation, and limited process walk-throughs. Period of review focused on more recent transactional activity (January – June 2018). Scope of review did not include a detailed IT application review of SMART. Audits of the member self-service portal and sensitive data transmissions with third parties are planned for FY2019 and thus received limited review.			

Closed Audits: Recommendations (cont.)

Audit Area	Risk Rating	Scope	Recommendations	Management's Response	Implemented	Implementation or Target Implementation
Laptop Encryption and Inventory (Dec. 2018)	Mod.	IT & Finance Departments Review included: A. Laptop inventory list B. Laptop encryption C. Asset safeguarding D. Incident response E. Laptop disposal	1. Develop written procedures to define all facets of a laptop's asset management (Mod.) 2. Reconcile IT and Finance's laptop inventory lists and develop ongoing processes to maintain (Mod.) 3. Develop a laptop lifecycle plan that includes planning, acquisition, maintenance and disposal (Mod.) 4. Inspect non-laptop stored devices to ensure no sensitive information remains (Low) 5. Reconcile laptop names to align with correct Asset ID numbers (Low) 6. Review purchases to ensure exclusion of sales tax (Low)	1. Operational procedures will be developed 2. Reconciliation will occur between IT and Finance's inventory lists with ongoing coordination 3. Each laptop's lifecycle will be evaluated for future decision making needs 4. Reviewed and determined no sensitive information exists on other stored devices 5. Reconciled new laptop device names to computer names and will continue on older laptop devices 6. Exemption certificate procedures will be implemented at outset of purchases to prevent sales taxes	1. No 2. No 3. No 4. Yes 5. No 6. Yes	1. Mar. 2019 2. Mar. 2019 3. Mar. 2019 4. Dec. 2018 5. Mar. 2019 6. Dec. 2018
		Comments: Controls were adequately designed and operating effectively for laptops to ensure: ➢ Laptop inventory list was complete, accurate and up to date ➢ Laptops were properly encrypted ➢ Laptops were properly accounted and safeguarded ➢ Sufficient incident response plan exists for lost or stolen laptops ➢ Laptop disposal process ensures removal of sensitive data Scope of review focused solely on SERS-provided laptops and iPads and did not extend to desktops, cell phones, employee-owned computers or other remote computing devices. Scope included a limited access control review and data analysis queries, not a detailed review of SERS' IT applications or encryption software.			

Closed Audits: No Recommendations

Audit Area	Risk Rating	Scope	Management's Response
Undue Influence Compliance Review (July 2018)	Low	<u>All Departments</u> Independently verify key SERS staff performed their job duties in good faith according to SERS' policies, and reaffirm no one had attempted to coerce their work or influence their job performance.	Not Applicable.
		Comments: Reviewed submitted *SERS Statement Regarding Undue Influence* certification forms and no documented comments were reported.	
Conflicts of Interest Compliance Review (July 2018)	Low	<u>Investment Department and Investment Compliance</u> Review disclosures by investment staff and external investment service providers for conflicts of interest compliance. Review includes: • Investment staff certification • Financial Disclosure Statement • Professional Conduct Statement • Investment Manager Agreement • Required Annual Disclosure Form	Not applicable.
		Comments: Reviewed SERS' investment staff disclosures and external investment service providers without any exceptions noted.	
Investment Incentive Compensation Review (Sept. 2018)	Low	<u>Investment Department and Enterprise Risk Management</u> Evaluate controls and payments associated with the FY2018 Investment Incentive Compensation Plan.	The ERM Officer was effective in completing the calculations in an accurate manner with supporting documentation. Some minor calculation errors were identified during testing and properly and timely adjusted by the ERM Officer.
		Comments: The investment incentive plan appears supportive of the Board's intent to reinforce a performance philosophy to attract and retain high-quality talent within Investments. Performance incentive calculations were properly computed.	

Active Audits: As of December 2018

Audit Area	Risk Rating	Scope	Target Completion
N/A	N/A	There were no active audits as of December 2018.	N/A

Other Audit-Related Activity

Area	Risk Rating	Subject/ Project	Description
SMART	High	Software Implement	Internal Audit maintained involvement in post-implementation activities by participation in SMART's ongoing committee meetings. Ongoing participation in post-implementation continues and has been incorporated into audit engagements, as applicable.
Medical & Pharmacy Claims	Mod.	Third Party Review	Minor Internal Audit involvement to review audit scope, report, and remediation of medical and pharmacy claims/rebate audit vendor's results. Process managed and directed by Assistant Director, Health Care Services.
Fiduciary Audit	N/A	Comment Remediation	Internal Audit provided ongoing remediation of fiduciary audit comments and reported results to Board. Final tracking report to Board indicated most comments were remediated, communicated to ORSC, or will be considered in SERS' future strategic plan.
External Audit	N/A	Financial Statements	External auditors provide all required written communication and verbal updates on the audit of the annual financial statements to the Audit Committee and Board.
Committee Report	N/A	CY2017 Annual Report	Pursuant to R.C. 3309.044, a report of actions taken by the Audit Committee of the SERS' Retirement Board for calendar year 2017 was submitted on January 16, 2018.
Internal Audit Annual Plan	N/A	FY2019 Plan	The FY2019 Internal Audit Plan was approved by the SERS Audit Committee on June 20, 2018.
Comment Remediation	N/A	Issued Audit Comments	Perform audit remediation activities involving internal, external, and other audit comments.
Financial Reporting	N/A	Financial Statement Controls	The Chief Financial Officer regularly provides updates to the Committee on financial reporting processes, changes in accounting and financial reporting standards, comprehensive annual financial report overview, processes in place to limit material control weaknesses and fraud, and periodic updates on activities involving external auditors or other oversight entities.
Internal Audit Operations	N/A	Internal Audit Quality Assurance	Internal Audit consists of one employee, a Chief Audit Officer (CAO). The CAO continues to maintaining quality within audit practices to maintain conformance with IIA *Standards*. Audit activities include: • Updated Internal Audit Operations Manual, Audit Committee and Internal Audit Charters, and standard work paper forms • Completed 10 of 13 strategic initiatives from the FY2017-19 internal audit strategic plan • Completed CAO annual goals aimed at improving audit effectiveness, plan completion, coordination and collaboration & skill sets.

Composition of Audit Committee at the end of calendar year 2018 reporting year (R.C. 3309.044)

Barbra M. Phillips (Chair), Employee Member

Catherine P. Moss, Retiree Member

James A. Rossler Jr., Appointed Member