Employees' Retirement System of the State of Rhode Island

Findings and Management Comments

Audit of the Financial Statements for the Fiscal Year Ended June 30, 2025

David A. Bergantino, CPA, CFE

Auditor General

State of Rhode Island
General Assembly
Office of the Auditor General

Office of the Auditor General
State of Rhode Island - General Assembly
David A. Bergantino, CPA, CFE – Auditor General
oag.ri.gov
33 Broad Street • Suite 201 • Providence, RI • 02903-4177
tel: 401.222.2435 • fax: 401.222.2111

January 2, 2026

JOINT COMMITTEE ON LEGISLATIVE SERVICES:

SPEAKER K. Joseph Shekarchi, Chairman

Senator Valarie J. Lawson
Senator Jessica de la Cruz
Representative Christopher R. Blazejewski
Representative Michael W. Chippendale

RETIREMENT BOARD OF THE EMPLOYEES' RETIREMENT SYSTEM OF THE STATE OF RHODE ISLAND:

We have audited the financial statements of the Employees' Retirement System of the State of Rhode Island (System) for the year ended June 30, 2025 and have issued our report thereon dated December 30, 2025 in accordance with Section 36-8-19 of the Rhode Island General Laws. The System's financial statements and our Independent Auditor's Report thereon are included in the Annual Comprehensive Financial Report of the System.

In accordance with *Government Auditing Standards*, this report includes our Independent Auditor's Report in Section I on our consideration of the System's internal control over financial reporting and our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements. We reported a significant deficiency in internal control which is included in Section II of this report. We noted no material weaknesses in internal control or material noncompliance.

We also reported other matters included herein as management comments in Section III which include recommendations to enhance internal control or result in other operational efficiencies.

The System's management has provided their planned corrective actions relative to these findings and management comments, which have been included herein.

Sincerely,

David A. Bergantino

David A. Bergantino, CPA, CFE
Auditor General

Employees' Retirement System of the State of Rhode Island

Findings and Management Comments
Audit of the Fiscal 2025 Financial Statements

TABLE OF CONTENTS

SECTION I

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

AUDIT OF THE EMPLOYEES' RETIREMENT SYSTEM OF THE STATE OF RHODE ISLAND

FISCAL 2025

Office of the Auditor General
State of Rhode Island - General Assembly
David A. Bergantino, CPA, CFE – Auditor General
oag.ri.gov
33 Broad Street • Suite 201 • Providence, RI • 02903-4177
tel: 401.222.2435 • fax: 401.222.2111

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*

JOINT COMMITTEE ON LEGISLATIVE SERVICES, GENERAL ASSEMBLY,
STATE OF RHODE ISLAND:

RETIREMENT BOARD OF THE EMPLOYEES' RETIREMENT SYSTEM OF THE
STATE OF RHODE ISLAND:

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States (*Government Auditing Standards*), the financial statements of the plans within the Employees' Retirement System of the State of Rhode Island (System) as of and for the year ended June 30, 2025 and the related notes to the financial statements, which collectively comprise the System's basic financial statements, and have issued our report thereon dated December 30, 2025.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the System's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the System's internal control. Accordingly, we do not express an opinion on the effectiveness of the System's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We identified a deficiency in internal control, described in the accompanying Schedule of Findings and Responses as Finding 2025-01, that we consider to be a significant deficiency.

Joint Committee on Legislative Services, General Assembly
Retirement Board of the Employees' Retirement System of the State of Rhode Island

Report on Compliance and Other Matters

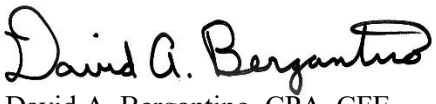
As part of obtaining reasonable assurance about whether the System's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

System Management's Response to Findings

Government Auditing Standards requires the auditor to perform limited procedures on the System's response to the findings identified in our audit and described in the accompanying Schedule of Findings and Responses. The System's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the System's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.



David A. Bergantino, CPA, CFE
Auditor General

December 30, 2025

SECTION II

SCHEDULE OF FINDINGS AND RESPONSES

AUDIT OF THE EMPLOYEES' RETIREMENT SYSTEM OF THE STATE OF RHODE ISLAND

FISCAL 2025

Finding 2025-01 ***significant deficiency / repeat finding***

INTERNAL CONTROL OVER DEFINED CONTRIBUTION PLAN FINANCIAL REPORTING

Background: The Employees' Retirement System of the State of Rhode Island (System) oversees a defined contribution (DC) plan for members which is part of the overall "hybrid" pension benefits, in conjunction with defined benefit plans, for most covered employees. The DC plan is administered totally by the Teachers Insurance and Annuity Association of America (plan administrator) and the System is reliant on information provided by the plan administrator for financial reporting purposes. No independent records are maintained by the System for the DC plan activities.

As expected, total assets of the DC plan have grown considerably since plan inception and members are beginning to withdraw funds to meet their retirement objectives. Total assets in the DC plan at June 30, 2025 approximated $2.5 billion.

Criteria: Management is responsible for the accuracy of the System's financial reporting and related internal control over financial reporting. The System should have sufficient information to support effective compliance monitoring of statutory and plan requirements in addition to the plan administrator's reporting that is the source for financial reporting of the DC plan.

Condition: The System does not receive information on the employer remittances of employer and employee contributions to the DC plan and therefore has limited information to ensure employer compliance with the DC plan provisions. System management currently places significant reliance on employer financial audits to identify if employers are not complying with statutory requirements for contributions to DC plans in place of more active monitoring.

During fiscal 2025, the System conducted a risk assessment over defined contribution plan financial reporting in response to the prior year finding. The System's initial assessment documented broad risks relating to financial reporting, information technology, and plan membership and identified current policies and procedures conducted by the System or other data sources being relied on. The assessment, however, lacked the identification of specific risks associated with financial reporting for the defined contribution plan and the designated controls that mitigate significant risks. In addition, the System relies significantly on the controls of the plan administrator and receives Service Organization Control (SOC) reports to obtain assurance regarding the adequacy and effectiveness of the plan administrator's internal controls. Since the System places significant reliance on these reports in relation to defined contribution plan financial reporting, the risk assessment should identify specifically the plan administrator's key controls that are relied on to mitigate financial reporting risks identified. As an example, the System relies completely on plan reporting from the plan administrator for financial reporting for the defined contribution plan, yet the risk assessment does not delineate the key plan administrator controls that ensure the reporting is complete and accurate.

Due to the significance of financial activity (i.e., contributions, distributions, investment activity and valuation) reported by the plan administrator, these items should be specifically considered in the risk assessment for defined contribution plan financial reporting. In addition to identifying the plan administrator's key controls in these areas that are included in the scope of the SOC reports, the System should also identify specific monitoring controls designed to ensure the completeness and accuracy of information reported by the plan administrator.

While the System does review the SOC reports for the plan administrator and identifies user entity controls, the System considers many of the user entity controls to be the responsibility of the participating employers and does not currently have procedures in place to evaluate how effectively employers comply with those responsibilities.

As a step to begin addressing this control deficiency during 2025, the System began performing quarterly reviews of total contributions for each unit to ensure the allocation between employer contributions and employee contributions was reasonable when compared to statutorily required contributions. This monitoring control was deemed effective to provide reasonable assurance that employee contribution allocations to the defined contribution plan were materially accurate and presented properly in the financial statements.

The System will need to more fully consider remaining risks associated with financial reporting for the defined contribution plan to ensure the material completeness and accuracy of financial statement amounts. Certain risks currently not being addressed by the System, beyond relying on the controls of the plan administrator, include but are not limited to the following:

- Risks that employers are not remitting contributions to the defined contribution plan in a timely manner. The risk assessment provided by the System indicated that it relies on employer unit financial audits to detect if employers are not making required DC contributions timely but did not identify any monitoring performed by the System. Since the plan administrator communicates with plan sponsors when contributions are not received in accordance with payroll schedules, the System should consider a documented monitoring process that ensures that corrective actions were taken by the employer unit and that the employer remained current with contributions in subsequent periods.
- Risks that employers are not remitting the statutorily required contribution amounts to the plan administrator. While the System has access to contribution data via the plan administrator portal, it does not currently perform any monitoring to validate that employers are remitting the appropriate amount of contributions based on employee pensionable wages each pay period. The System should consider utilizing the contribution data available in the plan administrator portal in combination with the reported pensionable wages uploaded by employers to the defined benefit plan system to monitor for potential instances of noncompliance with statutorily required contribution amounts.
- Risks that new employees are not enrolled in the defined contribution plan timely and properly. The System does not evaluate enrollment in the DC plan for completeness. The System should periodically reconcile the population of the defined benefit pension plan with those enrolled in the DC plan and confirm the appropriateness of those omitted from the DC plan or included only in the DC plan.
- Risk that assets reported by the plan administrator which are utilized for financial reporting of the DC plan are not complete and accurate. In response to this risk, the System should consider periodic (at least monthly) analytical reviews of investment growth and performance, contributions to and distributions from the plan and fees paid. The analytical reviews should include documentation of follow-up and resolution when actual results differ from expectations.

The System is highly reliant on plan administrator controls to mitigate certain risks, including those associated with the accuracy of plan reporting and participant distributions. In accordance with that reliance, the System must ensure that significant complementary user entity controls are in place and operating effectively in those areas. Our review of the plan administrator SOC reports noted the following user entity controls, as examples, deemed significant in relation to plan reporting, asset valuation and pricing, and participant distributions:

- Plan sponsors are responsible for reconciling plan reports to internal records in a timely manner.
- Plan sponsors are required to provide employee termination data in a timely manner.
- Plan sponsors are responsible for monitoring the plan's withdrawal programs in accordance with adopted plan guidelines.

The System must implement specific monitoring procedures that provide reasonable assurance of the operation and effectiveness of significant plan sponsor controls. In addition, since the plan administrator relies heavily on a third-party subservice organization for trading activities, the System needs to obtain and consider the SOC report for that subservice organization and potential monitoring of the plan administrator's relevant user entity controls deemed critical to the trading service provided.

Many of the monitoring procedures identified above would be better suited to an internal audit function within the System rather than layering these additional duties on the existing financial reporting and operations staff. While not implemented in fiscal 2025, the System has been developing a request for proposal to contract some internal audit resources. The System also continues to work with the plan administrator to implement an industry standard SPARK data file format, a standardized format for retirement plan information developed by the SPARK (Society of Professional Asset Managers and Recordkeepers) Institute. The SPARK data file format would allow the System to utilize reports generated by the plan administrator to more effectively monitor contributions submitted by employers.

As the System considers implementing additional monitoring procedures in relation to identified risks to DC plan financial reporting, the System should specifically detail the documentation requirements for monitoring procedures being implemented in response to this finding to allow for those procedures to be evaluated as controls over financial reporting.

Cause: At the inception of the DC plan, the plan design, enacted by legislation, provided for employer and employee contribution data to flow directly from the employer to the plan administrator without any data capture by the System. The System lacks sufficient accounting and contribution data to monitor compliance (through effective control processes) with contribution requirements and to ensure the completeness and accuracy of plan administrator reporting that is the sole basis for amounts reported in the DC plan financial statements. System reliance on plan administrator SOC reports lacks the necessary monitoring of complementary user entity controls to ensure their operating effectiveness in conjunction with plan administrator controls over critical functions.

Effect: Material misstatements could exist in the financial statements of the DC plan and not be identified in a timely manner.

RECOMMENDATIONS

2025-01a Continue to identify and implement monitoring procedures (similar to those suggested for risks detailed above) designed to ensure the completeness and accuracy of plan administrator reporting that supports amounts reported in the financial statements.

2025-01b Continue to explore expanding the responsibilities of the plan administrator (or other third party) to include capturing, verifying and validating employee and employer contribution data to enhance monitoring of employer compliance with the plan provisions.

2025-01c Enhance consideration of SOC reports that specifically relate to DC plan reporting by identifying key control objectives being relied on by the System and the specific complementary user entity controls and/or subservice organization controls that merit monitoring by the System due to their importance.

Management's Views and Corrective Action Plan:

As previously reported, the Defined Contribution Plan continued its relationship with TIAA following an RFP in 2023. The revised contract included enhanced requirements for monitoring contribution processing and strengthening internal controls. ERSRI has implemented significant improvements in oversight and process documentation, and these efforts remain ongoing.

The System believes that implementation of an industry-standard SPARK file layout will increase transparency and internal controls. ERSRI is actively working with the plan administrator, TIAA, to implement the SPARK file format for employers with the goal of establishing a formalized monitoring plan for the Defined Contribution component of the retirement benefit during this fiscal year. This finalized plan and related controls will be documented upon completion.

ERSRI maintains robust internal controls and reporting systems for wage and contribution management of the Defined Benefit Plan, and financial reporting for that plan has consistently met the highest standards. As noted by the Office of the Auditor General, the State of Rhode Island has utilized an external plan administrator for the Defined Contribution portion of the hybrid plan since its inception. Accordingly, ERSRI considers it appropriate to maintain distinct, but equally rigorous, control and reporting frameworks for the Defined Contribution and Defined Benefit plans.

Management further notes that the State Investment Commission and the investment division of the Office of the General Treasurer provide rigorous and comprehensive oversight of plan assets. Moreover, ERSRI is not reliant on the plan administrator to fully self-report, but contracts with a third-party consultant, Capital Cities, to monitor all participant-directed programs, including the Defined Contribution Plan. Capital Cities conducts ongoing analytical review of fund performance, and issues quarterly evaluation reports, which are then reviewed closely by Treasury Investment Staff. In addition, Capital Cities presents an annual 401(a) Program Review to the State Investment Commission. Oversight has been further strengthened through the addition of an Investment Associate dedicated to liquid asset classes, including the 401(a) investments.

SECTION III

MANAGEMENT COMMENTS

AUDIT OF THE EMPLOYEES' RETIREMENT SYSTEM OF THE STATE OF RHODE ISLAND

FISCAL 2025

Management Comment 2025-01

INTERNAL AUDIT FUNCTION

The Employees' Retirement System of the State of Rhode Island (System) had previously contracted with an accounting/auditing firm to perform an internal audit function. That contract ended several years ago without replacement.

An internal audit function is an important overall component of management's responsibility to ensure designed controls are in place and operating effectively. The Government Finance Officers Association (GFOA) has adopted a best practice policy and recommends "that every government should consider the feasibility of establishing a formal internal audit function to help management maintain a comprehensive framework of internal controls".

Additionally, internal audit can provide information and assurance to the System's "audit committee" (Administration, Audit, Risk and Compliance Committee) as well as the overall Board about the effectiveness and compliance with the controls management has placed into operation.

The internal audit activities performed under the prior contracted arrangement were narrow in focus. Consideration should be given to establishing a risk-based work plan with input from the Administration, Audit, Risk and Compliance Committee. Areas of higher risk may include the System's investments and the operation of the defined contribution plan which are largely performed by external entities.

The size and complexity of operations under the General Treasurer's oversight, which includes the System, have grown significantly over the years and a dedicated internal audit function that operates within the internal control structure for all operations should be considered. The funding of a dedicated internal audit function could be allocated across General Treasurer operations.

RECOMMENDATIONS

MC 2025-01a Implement a risk-based internal audit work plan to guide the efforts of the internal audit function with input and approval from the System's Administration, Audit, Risk and Compliance Committee.

MC 2025-01b Determine the necessary resources (personnel or contract) to implement an internal audit function based on the developed work plan. Consider implementation of dedicated internal audit resources within the internal control structure for all operations under the oversight of the General Treasurer.

Management's Views and Corrective Action Plan:

We offer one general comment, followed by a discussion of three specific actions implemented after June 30th 2025 designed to specifically strengthen ERSRI's internal controls, enhance transparency, and mitigate risk to the state, ERSRI members, and participating employer units.

As a general matter, and consistent with our recent discussions with the office of the Auditor General, ERSRI believes that the most critical factor in the effectiveness of ERSRI's own internal

audit practices is active and engaged management throughout the organization, with a focus on best-practice development and implementation. While ERSRI does not currently have a full-time equivalent position dedicated exclusively to internal audit functions, the System has demonstrated a clear commitment over time to achieving best-in-class standards in retirement system administration and financial controls.

This commitment began over a decade ago with a comprehensive study into our board's governance, which led to the establishment of a standing Administration, Audit, Risk and Compliance Committee. Subsequent governance enhancements were followed by improvements to the organization of the finance functions and staff, and more recently, the segregation of asset and liability accounting functions. These changes have contributed to ERSRI being recognized as an award-winning organization. Building on this foundation of active risk management and continuous improvement, there are three additional actions we would like to highlight:

1. ***Internal Audit RFP.*** *In fall 2025, the Administration, Audit, Risk and Compliance Committee, followed by the full ERSRI Board, approved a budget that includes the issuance of a Request for Proposal to solicit bids from qualified firms to perform ERSRI's internal audit function. The process will be performed with oversight and approval from the Administration, Audit, Risk and Compliance Committee, and will be supported by dedicated senior staff throughout the development, selection, and completion phases. ERSRI leadership views this audit not as a one-time exercise as a guidepost to inform ongoing strategic planning and the continued refinement of management and control practices.*
2. ***Partnership between the Chief Information Security Officer and ERSRI senior staff.*** *The hiring and onboarding of a Director of Cybersecurity is addressed in our response to a subsequent comment, but ERSRI wishes to highlight an additional benefit of this addition to our leadership team. While a one-time "Cyber-Audit" is a valuable and sometimes urgent exercise, effective cybersecurity requires continuous oversight and active change management, not only to identify best practices but to ensure their implementation and enforcement. The Treasury Director of Cybersecurity is being integrated into all leadership and management meetings, and the ongoing process of assessing information and technology risk, assessed on a division-by-division basis, is being coordinated as part of ERSRI's broader planning and operational management efforts.*
3. ***Additions to the ERSRI Leadership Team.*** *As of June 30, 2025, ERSRI was operating under an Acting Executive Director, who was filling both mandated leadership roles. The Board has subsequently hired a permanent Executive Director who started in fall 2025. New leadership, in addition to the retention of all ERSRI's senior management team, creates additional risk-mitigation opportunities by enabling a comprehensive review of all existing processes and systems as part of the onboarding process. It also creates an opportunity to formalize and document processes that may previously have been implicitly understood, enhancing transparency and consistency.*

Management Comment 2025-02

INFORMATION SECURITY OFFICER

The System previously contracted for an external security assessment of its information technology operations. One of the recommendations from that assessment included adding an information security officer (ISO) with sufficient authority and resources to oversee and maintain an organization-wide information security program. Corrective actions for other issues noted in the assessment are dependent on dedicated information security resources for the System.

Most of the System's information technology (IT) is maintained by external entities which, while lessening the resources needed to manage daily IT operations, increases the need for oversight and monitoring of overall information security best practices and protocols. Information security is of critical importance for all entities involved in the collection, sharing, transmission, and storage of personally identifiable information (PII). A strong and well-designed information security program is essential for protecting an organization's communications, systems, and assets from both internal and external threats.

Overall IT operations that collectively operate under the General Treasurer's oversight, which includes the System, have grown significantly over the years as has the use of information technology and the various risks associated with it. A dedicated ISO responsible for securing the IT operations within these critical functional areas is needed.

To address this issue, the Rhode Island Office of the General Treasurer hired a Director of Cybersecurity who assumed responsibilities in November 2025. This individual is expected to dedicate 60% of their time on activities related to the System. In addition, the System has contracted with an IT security firm to update and/or establish policies and procedures, perform a risk assessment, and conduct penetration testing and vulnerability scans which will assist the new security officer in developing and documenting an IT security program for the System.

RECOMMENDATION

MC 2025-02 Begin development of an IT security program that incorporates the policies and procedures and results of the IT security consultant and provides for future monitoring of key controls (including significant service organization controls), planned corrective actions and related time frames for completion, and periodic risk assessment updates. The program should be comprehensive and include components relating to the confidentiality, integrity, and availability of the System's information systems.

Management's Views and Corrective Action Plan:

The hiring and successful on-boarding of a senior Director of Cybersecurity in 2025 is a significant accomplishment for ERSRI and the office of the General Treasurer. The new Director of Cybersecurity is leading the development of a comprehensive information security program that integrates the policies, procedures, and findings from the ongoing IT security consultant engagement. This program will serve as the foundation for ensuring the confidentiality, integrity, and availability of the Retirement System's information assets while addressing identified gaps and strengthening our overall security posture.

To date, the Director of Cybersecurity, in collaboration with the Director of Retirement Business Systems, has completed a Business Impact Analysis (BIA) to inform the consultant's Information Security Risk Management (ISRM) plan. Additionally, external penetration testing of the vendor environment is scheduled for January 2026 and is expected to provide critical data points for risk assessment and control validation.

Ongoing engagements with the IT security consultant through Summer 2026 will incorporate results from penetration testing, the BIA, and key security controls to produce a draft ISRM plan by Fall 2026. This plan will include mechanisms for continuous monitoring of key controls, including significant service organization controls, and a structured process for corrective actions with defined timelines. Periodic risk assessments will be embedded to ensure adaptability to evolving threats and business needs. By integrating these components into our ISRM plan, ERSRI seeks to create a sustainable and proactive approach to information security risk management that strengthens operational resilience and safeguards critical information assets.

Management Comment 2025-03

TIMELY REMOVAL OF AUTHORIZED SIGNATORIES AND ACCESS TO INVESTMENT INFORMATION PORTAL

Communication of changes of authorized signatories for the System's investment accounts and access to the related client information portal is essential to maintaining adequate internal control over investments. We noticed an instance during our audit where a terminated employee, who was an authorized signatory for the System's investment account, did not have their signature authorization removed in a timely manner. Access to the client information portal also was not removed in a timely manner for this employee.

The General Treasurer's office developed procedures in response to this issue in prior years, however, the procedures were not performed to ensure timely remediation of this issue cited in fiscal 2025.

RECOMMENDATION

MC 2025-03 Reinforce procedures and controls to ensure the timely removal of authorized signatories and access to the investment information portal for personnel who terminate from the System or whose job responsibilities no longer require authorization and portal access.

Management's Views and Corrective Action Plan:

In the instance identified, Treasury staff had promptly notified internal managers, investment consultants, and the custodian bank of the employee's departure and had provided an updated list of authorized signatories. However, the System's custodian bank account manager who received the notification failed to refer the information to the appropriate team responsible for processing the access removal request.

To reinforce this procedure, the ERSRI's Investment Accounting Manager has been designated as the organization's primary liaison with the custodian's account activation team. In addition to the standard departure notification that is sent to the account manager, the Investment Accounting

Manager will contact the account activation team directly to request termination of access and will monitor for and document confirmation that access changes have been implemented.

Management notes that the risk associated with this delay was mitigated by existing controls, as no single authorized signatory has the ability to independently direct cash movements, and all transactions require multiple levels of approval.

Management Comment 2025-04

SEGREGATION OF DUTIES FOR CASH RECEIPTS BY CHECK

Segregation of duties is critical to ensuring proper internal control over cash receipts. Insufficient segregation of duties over cash receipts increases the risk of misappropriation of cash and financial statement misstatement. Although the System receives most cash receipts electronically, a small portion are received in the form of checks. The System's processing of cash receipts received by check lacks adequate segregation of duties as a single employee is involved in receiving, depositing, and recording the checks as well as reconciling the bank account. While the System's current processes do allow for some supervisory oversight of these functions, overall control over check receipts would be improved by segregation of duties.

RECOMMENDATIONS

MC 2025-04a Segregate the receipt, logging, and forwarding of checks from the individual responsible for depositing the checks and the individual responsible for recording the receipts in the accounting system. The individual receiving and logging the checks should stamp each check "For Deposit Only" and copy the check before forwarding the original for deposit to a designated employee and the copy of the check for recording to a different responsible employee.

MC 2025-04b Segregate the recording of cash receipts and the bank reconciliation function to prevent both functions from being performed by the same individual.

Management's Views and Corrective Action Plan:

ERSRI has implemented a new process for the receipt, logging, depositing and reconciling of check deposits which segregates duties and documents the process from receipt to reconciliation, including staff sign off for each step.

Management Comment 2025-05

COMPLEMENTARY USER ENTITY CONTROLS

Service Organization Control (SOC) reports are provided by service organizations (i.e., vendors, contractors) to assure customers/clients that controls are sufficiently designed and in operation over the contracted services they provide. Each SOC report identifies complementary user entity controls that are to be implemented and monitored by the user (the System), to enable the service organization's related controls to operate effectively. Due to the importance of functions provided by service organizations to the financial reporting and information system (IS) security of the System, SOC reports serve as a critical monitoring tool in relation to the System's oversight of contracted services.

The System obtains and reviews SOC reports from the various service organizations that provide services (e.g., benefit processing, census data maintenance and investment recordkeeping and management for the defined benefit and the defined contribution plans) to the System to monitor and assess the effectiveness of the service organization controls. As part of that review, the System evaluates complementary user entity controls and documents its response to each control. The System, however, does not currently identify the significance of SOC objectives evaluated in the SOC report and the user entity controls deemed relevant to the control objectives related to the System's financial reporting and/or IS security. In addition, for certain user entity controls performed by the System, documentation of control performance was lacking and could not be evaluated.

Amongst the various SOC reports that the System utilizes for oversight of contract services, we noted instances where the user entity control was delegated to a third party with no monitoring procedures identified by the System. Since management is responsible for financial reporting, monitoring of IS security, and oversight of contract services, monitoring or periodic review of significant user entity controls may be warranted for those determined to be significant to the System's critical functions.

The System should improve its consideration and documentation of user entity controls, and for those deemed significant, consider appropriate monitoring procedures when those controls are being performed by contracted third parties. Such monitoring may be more effectively achieved through internal audit processes rather than the System's internal financial reporting resources.

RECOMMENDATIONS

MC 2025-05a Improve documentation of SOC report reviews by identifying control objectives considered significant to the System's critical functions and the user entity controls deemed most relevant to those control objectives.

MC 2025-05b Ensure that user entity controls performed by the System are appropriately documented.

MC 2025-05c Implement monitoring procedures for user entity controls being performed by contracted third parties that relate to significant control objectives of the service organizations.

Management's Views and Corrective Action Plan:

ERSRI staff receive and review critical SOC reports. As noted in the response to the ***Information Security Officer*** *comment above, "Future engagements with the IT security consultant through Summer 2026 will incorporate data from penetration testing, the BIA, and key security controls to produce a draft ISRM plan by Fall 2026. This plan will include mechanisms for continuous monitoring of key controls, including significant service organization controls, and a structured process for corrective actions with defined timelines." ERSRI will enhance the SOC report review process to improve stronger documentation of the review and consideration of user entity controls deemed relevant.*

The verification of security controls for third-party systems will establish a baseline from which we will continue to formalize and enhance management and financial control documentation.