



VIRGINIA RETIREMENT SYSTEM

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2023

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Retirement System (System) as of and for the year ended June 30, 2023, and issued our report thereon, dated December 14, 2023. Our report, included in the System's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the System's website at www.varetire.org. Our audit found:

- the financial statements are presented fairly, in all material respects;
- three internal control findings requiring management's attention that also represent instances of noncompliance or other matters required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings. Those corrective actions may include additional items beyond our recommendations.

RETIREMENT SYSTEM EMPLOYER SCHEDULES

The Commonwealth and its localities have previously implemented Governmental Accounting Standards Board Statements No. 68 and 75. These standards address accounting and reporting of pension and other post-employment benefit activity by employers. Therefore, in addition to our audit of the System's financial statements, we were separately required to audit information prepared by the System for all of the participating employers. In August 2023, the System provided actuarial valuation reports, schedules of the applicable pension and other post-employment benefit amounts, footnote disclosure information, and other financial reporting guidance to the participating state and local government employers for their fiscal year 2023 financial statements. Likewise, our office published the reports that included our audit opinions over the plan schedules and applicable pension and other post-employment benefit amounts for pension and other post-employment benefit plans administered by the System. This information is available at the Auditor of Public Accounts' at www.apa.virginia.gov and at the System's website at www.varetire.org.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-4
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	5-7
APPENDIX – FINDINGS SUMMARY	8
AGENCY RESPONSE	9-10

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve IT Change Control and Configuration Management Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

The System does not manage its Information Technology (IT) change control and configuration management process in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard), and the System's Information Security Program Policy. Specifically, the following two weaknesses exist:

- The System has not reviewed and updated its Change Management Procedure since April 2017. The System's Information Security Program Policy, Section 8.5.1 CM-01: Configuration Management Policies and Procedures, states that the System should review and update its configuration management policies and procedures annually, or more frequently as needed based on environmental changes. The Security Standard, Section CM-1 Configuration Management Policy and Procedures, requires that the System review and update its current configuration management procedure on an annual basis, or more frequently if required to address an environmental change. Without current change control and configuration management policies and procedures, the System may not include all necessary elements in the change control and configuration management system and process to ensure adequate implementation of configuration management controls that meet Security Standard requirements.
- The System does not perform and document an explicit security evaluation of each change request for all changes. The System's Change Management Procedure, Section 'Create/Update Change Management Request', requires that the System record an assessment of the risk associated with each change as part of the change description, with a risk assignment of low, medium, or high. The Security Standard, Section CM-4 Security Impact Analysis, requires that the System analyze changes to information systems to determine potential security impacts prior to change implementation. Security Standard, Section CM-3 Configuration Change Control requires that the System review proposed configuration-controlled changes to an information system and approve or disapprove such changes with explicit consideration for security impact analyses. Not performing and documenting a security evaluation of changes and the subsequent potential security impacts for each change could result in changes with higher risk than anticipated, resulting in potential weaknesses in the System's security posture.

Turnover in key positions, including the position responsible for the change control and configuration management process, resulted in the identified weaknesses. The System has since filled the position and is working to procure a new change management system; therefore, the System chose to prioritize the implementation of the new system over updating the old system and its Change Management Procedure.

The System should review and update its Change Management Procedure annually, as required, to ensure it accurately reflects the System's change management process and includes all Security Standard requirements. The System should also perform and document a security evaluation of changes and the subsequent potential security impacts for each change in each change control request in compliance with its Information Security Program Policy, Change Management Procedure, and the Security Standard. Doing so will help to ensure the confidentiality, integrity, and availability of the System's sensitive data.

Improve Database Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

The System does not secure a database that supports a sensitive and critical system in accordance with the Security Standard and industry best practices, such as the Center for Internet Security Benchmarks (best practices). We identified six control weaknesses and communicated them to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard requires the System to implement certain security controls to safeguard systems that contain or process sensitive data. Without enforcing the minimum requirements in the Security Standard for the database, the System increases the data security risk associated with the sensitive information processed by the system. These findings increase the risk of a data breach or system unavailability, which could lead to financial, legal, regulatory, and reputational damages.

The System's lack of a complete baseline configuration based on best practices and Security Standard requirements contributed to the identified weaknesses. The System should regularly update its baseline to accurately reflect the database configuration and ensure it regularly applies policy requirements. The System should dedicate the necessary resources to configure appropriate security controls for the database in accordance with the Security Standard and best practices. The System should also identify its processes for assessing database activity. Implementing these controls will help maintain the confidentiality, availability, and integrity of the sensitive and mission critical data stored or processed in the database.

Improve Retirement Benefit Calculations

Type: Internal Control and Compliance

Severity: Significant Deficiency

The System improperly calculated retirement benefits for multiple retirees during fiscal year 2023. We noted the following exceptions in annuity payment, partial lump sum payment, and group life insurance payment calculations:

- Out of a sample of 50 new service retirees receiving a partial lump sum payment, the System incorrectly calculated one member's partial lump sum payment and annuity payment at the time of retirement resulting in a net underpayment of \$1,166;
- Out of a sample of 21 disability retirees, the System used the improper salary amount to determine one member's group life insurance amount at the time of retirement resulting in a group life insurance calculation understated by \$40,000. The System did not process any inaccurate payments relating to this error; and
- Out of a sample of 20 deceased members, the System incorrectly calculated one member's group life insurance amount at the time of retirement resulting in an underpayment of \$1,400 to the member's beneficiary.

Retirement benefits are set according to §§ 51.1-155, 51.1-157, and 51.1-505 of the Code of Virginia. The Code of Virginia requires the System to pay member benefits accurately according to the criteria set within each subsection relevant to the member's status as disabled, service-retired, or receiving life insurance benefits. Additionally, the System has defined the proper calculation method for each type of benefit within the VRS member handbook.

Improper calculation of benefits resulted in underpayments to members and beneficiaries. While the dollar amount of likely errors in the total population of benefit payments is immaterial in relation to the System's financial statements, members of the System count on receiving the full and accurate payments they are due. Underpaying benefits or incorrectly calculating benefits may result in financial damage to beneficiaries who receive less than they are owed.

Each error noted within our sample resulted from unusual or infrequent circumstances as follows:

- The service retiree transferred from a Virginia Law Officers' Retirement System (VaLORS) position to a Plan 1 position and then back to a VaLORS position;
- The disability retiree received a pay increase after submitting a retirement application and the employer did not properly update the retiree's salary within the benefits system; and
- The deceased member was a disability retiree on a reduction schedule requiring notification from the third-party administrator (TPA) to the System.

In all three errors, manual processing and supervisory review failed to prevent or detect the calculation errors in the absence of automated solutions for these unusual or infrequent circumstances. In the deceased member error, communication broke down between the TPA and the System.

The System should take inventory of circumstances requiring manual retirement benefit calculations to identify calculations at greater risk of error. When automated solutions are not feasible

for replacing high risk manual calculations, or are not cost-effective, the System should ensure its training, policies and procedures, and supervisory review processes are adequate to ensure accurate benefit calculations for its members.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 14, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Trustees
Virginia Retirement System

Patricia S. Bishop, Director
Virginia Retirement System

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

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, the financial statements of the **Virginia Retirement System** (System) as of and for the year ended June 30, 2023, 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 14, 2023.

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 opinion 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 did identify certain deficiencies in internal control titled "Improve IT Change Control and Configuration Management Process," "Improve Database Security," and "Improve Retirement Benefit Calculations," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the System's financial statements are free of 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 instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled "Improve IT Change Control and Configuration Management Process," "Improve Database Security," and "Improve Retirement Benefit Calculations."

The System's Response to Findings

We discussed this report with management at an exit conference held on January 25, 2024. Government Auditing Standards require the auditor to perform limited procedures on the System's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." 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.

Status of Prior Finding

The System has taken adequate corrective action with respect to the prior audit finding identified as complete in the [Findings Summary](#) included in the Appendix.

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 entity'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.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

ZLB/clj

FINDINGS SUMMARY

(For the Fiscal Year Ended June 30, 2023)

Finding Title	Status of Corrective Action*	First Issued
Improve Service Provider Oversight	Complete	2022
Improve IT Change Control and Configuration Management Process	Ongoing	2023
Improve Database Security	Ongoing	2023
Improve Retirement Benefit Calculations	Ongoing	2023

* A status of **Complete** indicates adequate corrective action taken by the System during the fiscal year. A status of **Ongoing** indicates the existence of a significant deficiency in internal controls requiring corrective action as of fiscal year end.



P.O. Box 2500, Richmond, VA 23218-2500
Toll-free: 888-827-3847
Website: varetire.org
Email: vrs@varetire.org

Patricia S. Bishop
Director

To: Staci A. Henshaw, CPA, Auditor of Public Accounts

From: Patricia S. Bishop, Director

A handwritten signature in cursive script, appearing to read 'Patricia S. Bishop'.

Date: February 8, 2024

Re: 2023 VRS Audit Report - Internal Control

We reviewed the above captioned Auditor of Public Accounts (APA) Internal Control Report. We appreciate the APA's examination of the subject area, and the professionalism and cooperation exhibited by APA staff throughout the audit process. Please find below our responses to the three findings.

Improve IT Change Control and Configuration Management Process

As noted in our memo dated December 18, 2023, when notified by APA of the outdated change management policy, VRS immediately instituted a formal review to update the policy. Due to a high level of turnover and vacancies, prior updates to the policy had not been completed in line with expectations. That stated, a new configuration management policy and associated procedure documents are currently in draft form and the final version will be completed in Spring 2024, aligning with SEC 530 requirements. In addition, VRS will initiate the selection of a new enterprise change management software solution, which is expected to be fully implemented by the end of calendar year 2024. The new solution will meet and implement all SEC 530 requirements.

Improve Database Security

Regarding the "improve database security" finding, VRS made certain changes resulting from the audit findings. As noted in our December 13, 2023, memo, however, certain configuration settings that deviate from CIS benchmarks best practices are unable to be changed due to system requirements of the underlying line of business application. As noted in the same memo, VRS completed items 2, 3 and 6.1 of the audit recommendations. For audit recommendations 1, 4, 5, 6.2, and 6.3 VRS provided detailed justification for our current approach along with the mitigating controls deployed. In addition, the VRS team is updating the system configuration guide to document current settings.

VRS recognizes the importance of strong security and invests significantly in protecting its resources. Further, VRS consistently evaluates its security provisions and appreciates feedback to make them stronger as applicable and appropriate. VRS also utilizes risk mitigating strategies, compensating controls and a comprehensive suite of tools for system security, including, but not limited to, password management software, compliance software, a monitored IPS system to report anomalous behaviors, a

An Independent Agency of the Commonwealth of Virginia

SIEM tool for log aggregation and alerting, and a Security Configuration Management tool for file integrity monitoring. VRS will also publish baseline thresholds associated with monitoring specific database transactions.

VRS will be updating its framework in the near future, which will be designed to be compliant with current standards and best practices as applicable at that time. VRS is in the process of further identifying, documenting and implementing monitoring activities for required transactions and will continue to utilize compensating controls.

Improve Retirement Benefit Calculations

As previously noted in a memo dated October 12, 2023, VRS acknowledges the three improperly calculated benefits identified in the audit report and upon notification from APA immediately remedied each. One improper calculation resulted in a \$1,166 net underpayment of a member's partial lump sum payment and another resulted in a net underpayment of \$1,400. The other error did not result in any inaccurate payments. Although these three improper calculations resulted from unique and infrequent circumstances, VRS, nevertheless, instituted additional controls in its review of these types of scenarios.

Regarding the recommendation for process automation, VRS continuously works to identify opportunities to streamline processes, including the use of automation where appropriate. However, VRS must balance that benefit with the associated costs and risks. Therefore, VRS will continue to explore automation options for its benefit calculations, and where not feasible, in collaboration with the VRS internal audit team will further strengthen its manual process controls, particularly related to unusual and infrequent calculations.

Thank you again to you and your staff for your thoughtful review and for the opportunity to provide feedback.