VRS
Virginia
Retirement
System

Audit and Compliance Committee Meeting

1111 E. Main Street
Third Floor Board Room

Monday, 9/13/2021
1:30 - 4:00 PM ET

I. Welcome

II. Minutes of the June 3, 2021 Meeting

Meeting Minutes - Page 3

III. Matters for Discussion with the Auditor of Public Accounts

Matters for Discussion with the APA - September 2021 - Page 8

APA VRS Audit Committee Meeting Update - Page 9

A. Exit on the 2020 Employer Assurances Review

B. Update on VRS 2021 Annual Comprehensive Financial Report

IV. Audit Reports

A. Report 439: Hosted Systems - Administration

Audit Report 439 - Page 28

Management's Response to Audit Report 439 - Page 59

B. Report 440: Application Controls: VNAV and Enterprise Content Management

Audit Report 440 - Page 67

V. Quarterly Reports on the Modernization Program - Phase 4

A. Report from Management

Management's Report - Page 95

B. Report from Internal Audit

Internal Audit's Report - Page 105

VI. Annual Progress Reports for FY2021

A. Annual Report on Internal Audit

FY2021 IA Annual Report - Page 115

B. Annual Report on the Audit Recommendation Follow-up System - Management

Management's Annual ARFUS Report - Page 126

C. Annual Report on the Audit Recommendation Follow-up System - Internal Audit

Internal Audit's Annual ARFUS Report - Page 129

D. Annual Reports on FY2021 Audit Plan and FY2021-2024 Long Range Plan Status

FY2021 Annual Plan Progress - June 2021 - Page 131

FY2021-FY2024 Long-Range Plan Progress - June 2021 - Page 136

VII. Proposed FY2022 Annual Audit Plan

Proposed FY2022 Annual Plan - Page 142

A. RBA: Recommend Approval of the FY2022 Audit Plan

RBA - Approving FY2022 Annual Plan - Page 146

VIII. Quarterly Report on Fraud, Waste and Abuse Hotline Cases

Fraud Waste and Abuse Report - May 1, 2021 through July 31, 2021 - Page 148

IX. Miscellaneous Updates

A. Management's Quarterly Travel Expenses and Per Diem Report

Management's Travel Expense and Per Diem Report and Memo - Q4 - Page 152

B. Review of VRS APOs and Operational Measures

Internal Audit APO OM Memorandum - Page 157

C. Review of VRS Investment Compensation

Internal Audit Incentive Compensation Memorandum - Page 158

D. 2022 Committee Meeting Dates

2022 Confirmed Board and Committee Meeting Dates - Page 159

E. Next Scheduled Meeting Date: Monday, December 6, 2021 at 2:00 p.m.

X. Review of Audit Director's Performance (Closed Session)

Closed Session Language - Audit Director's Performance - Page 161

A. RBA: Review and Approve Internal Audit Director's Performance and Bonus

RBA - Review and Approve Internal Audit Director's Performance and Bonus - Page 162

Minutes

In accordance with Item 4-0.01 of Chapter 552 of the 2021 Special Session I Acts of Assembly of the *Code of Virginia* as it relates to conducting business during the COVID-19 pandemic, the Audit and Compliance Committee of the Board of Trustees convened electronically on June 3, 2021.

The following individuals participated electronically.

Audit and Compliance Committee Members:

Joseph W. Montgomery, Committee Chair
W. Brett Hayes, Committee Vice Chair

Other Members of the Board of Trustees:

J. Brandon Bell, II
John M. Bennett
William A. Garrett
Troilen G. Seward, Ed.S.

VRS Staff:

John Alouf, Patricia Bishop, Judy Bolt, Jeanne Chenault, Michael Cooper, Valerie Disanto, Barry Faison, Jonathan Farmer, Laurie Fennell, Joshua Fox, Jay Gentry, Krystal Groff, Kelly Hiers, Robert Irving, Curt Mattson, Vera Pleasants, Matthew Priestas, Denise Rasmussen, Mark Rein, Daniel Schlussler, Jennifer Schreck, Kristy Scott, Jillian Sherman and Cynthia Wilkinson

Auditor of Public Accounts: Zach Borgerding

Mr. Montgomery called the meeting to order at approximately 2:00 p.m. and noted that given the current circumstances related to COVID-19, the Audit and Compliance Committee (Committee) was unable to meet in person. However, utilizing electronic means, the Committee could hold this meeting in accordance with Item 4-0.01 of Chapter 522 of the 2021 Special Session I Acts of the Assembly of the *Code of Virginia* as it relates to conducting business during a pandemic.

Mr. Montgomery then completed a roll call of each Committee member for attendance purposes:

Senator Bell – present
Mr. Bennett – present
Chief Garrett – present
Mr. Hayes – present
Ms. Seward – present
Mr. Montgomery – present

PUBLIC COMMENT

Mr. Montgomery noted that no individuals registered to provide public comment to the Committee.

MINUTES

Upon motion of Senator Bell, seconded by Mr. Bennett, the Committee approved the minutes of the Audit and Compliance Committee meeting held on March 16, 2021 upon the following roll call vote:

Senator Bell – aye
Mr. Bennett – aye
Chief Garrett – aye
Mr. Hayes – aye
Ms. Seward – aye
Mr. Montgomery – aye

UPDATE ON THE 2020 EMPLOYER ASSURANCES REVIEW

Mr. Borgerding updated the Committee on the status of the Auditor of Public Accounts' (APA) separate examinations designed to provide participating employers and their auditors the assurances necessary to prepare their own annual financial statements in accordance with Governmental Accounting Standards Statements No. 68 and 75.

He noted these examinations are progressing as planned and the APA should conclude their work and issue the related opinions for the pension and OPEB plans by the end of July.

ENTRANCE CONFERENCE

The Committee proceeded to the scheduled entrance with the APA. The primary purpose of the entrance meeting was to review the approach and scope of the APA's annual examination of VRS' Annual Report for the fiscal year ending June 30, 2021. Mr. Borgerding noted the APA's primary responsibilities under Generally Accepted Auditing Standards are to provide reasonable assurance as to whether the financial statements are free of material misstatements. Mr. Borgerding also noted APA's responsibility to determine that VRS' financial information is accurately incorporated into the statewide annual comprehensive financial report (ACFR).

Mr. Borgerding further addressed the APA's use of materiality, responsibility for identifying fraud, as well as reporting on non-compliance items that could have a material direct or indirect effect on financial statements.

Finally, Mr. Borgerding shared a report on internal controls and compliance will be provided and any significant findings over internal controls would be included in the Statewide Single Audit (SSA) Report. Mr. Borgerding provided further information about the SSA and its related report and addressed the Committee's questions.

AUDIT REPORTS

The Committee received three audit reports from staff in the following order.

Audit Report 437

Mr. Fox presented audit report 437 – *Private Equity Program* which concluded due diligence and monitoring activities over the program are adequate and align with the Investment Policy Statement. There were no written recommendations resulting from the review. The Committee discussed the timing considerations of available financial data and external investment manager relationships.

Audit Report 436

Ms. Bolt presented audit report 436 – *Optional Retirement Plan for Higher Education*. The review evaluated the reasonableness and adequacy of monitoring activities and compliance activities performed by VRS and the accuracy of plan distributions, financial activities and system interfaces. There were no written recommendations resulting from the review.

Audit Report 438

Ms. Scott presented audit report 438 – *Internal Equity Management Program* which determined whether program activities are properly recorded and align with the Investment Policy Statement. In addition, other related processes reviewed are operating as intended. There were no written recommendations resulting from the review.

ACCEPTANCE OF AUDIT REPORTS

Upon motion of Mr. Bennett, seconded by Senator Bell, the Committee accepted audit reports 436, 437, and 438 as presented, upon the following roll call vote:

Senator Bell – aye
Mr. Bennett – aye
Chief Garrett – aye
Mr. Hayes – aye
Ms. Seward – aye
Mr. Montgomery – aye

MODERNIZATION QUARTERLY REPORT - MANAGEMENT

Ms. Rasmussen presented Management's report on the Modernization Program - Phase Four. Ms. Rasmussen provided a timeline highlighting the progress and accomplishments of the Modernization Program over the past 10 years and updated the Committee on the Phase Four progress. Ms. Rasmussen discussed the status of the rollout of software and VRS' implementation plan for the remaining features, including outreach and training, soft launch approach, and post wave business rollouts. The budget and cost updates as of March 31, 2021 were provided.

MODERNIZATION QUARTERLY REPORT – INTERNAL AUDIT

Mr. Priestas discussed Internal Audit's Review of the Modernization Program - Phase Four indicating agreement with management's representations regarding the overall schedule, budget and scope of Phase Four. Mr. Priestas acknowledged management's continued thoughtful and cautious planned approach through implementation and afterwards. Looking forward, VRS' risk averse approach tentatively indicates a full release of all features to all members in Fall 2021.

QUARTERLY REPORT ON FRAUD, WASTE AND ABUSE HOTLINE CASES

Ms. Schreck noted there were no Fraud, Waste and Abuse cases reported for the period February 1, 2021 through April 30, 2021.

MISCELLANEOUS UPDATES

Management's Quarterly Travel Expense and Per Diem Report
Ms. Schreck noted management's quarterly travel expense and per diem report was available in the meeting package for the Audit and Compliance Committee's review.

FY2022 Annual Audit Plan Assessment and Validation
Ms. Schreck noted that the risk assessment and validation of the Fiscal Year 2022 Annual Audit Plan was underway. Ms. Schreck reminded the Committee that the annual audit plan is derived from the long range plan. While it is the goal to focus on those projects included in the long range plan, the risks currently impacting the organization are considered when finalizing an individual fiscal year's annual audit plan. The proposed annual plan with any adjustments based on this feedback with consideration of the implications to the long-range audit plan will be presented to the Committee for its review and approval at the September meeting.

Next Committee Meeting Date
Ms. Schreck noted the next meeting of the Committee is scheduled for September 13, 2021 at 1:30 p.m.

MEETING ADJOURNMENT

There being no further business, Ms. Seward motioned to adjourn the meeting which was seconded by Senator Bell.

Mr. Montgomery adjourned the meeting at approximately 3:00 p.m. upon completion of the following roll call vote:

Senator Bell – aye
Mr. Bennett – aye
Chief Garrett – aye
Mr. Hayes – aye
Ms. Seward – aye
Mr. Montgomery – aye

Committee Chair

Secretary

Matters for Discussion with the APA

MATTERS FOR DISCUSSION WITH THE APA

GASB No. 68 RELATED REPORTS

VRS Management's Assertions Related to Census Data for the fiscal year ended June 30, 2019

State Employee Retirement Plan for the fiscal year ended June 30, 2020

Political Subdivision Retirement Plan for the fiscal year ended June 30, 2020

Teacher Retirement Plan for the fiscal year ended June 30, 2020

GASB No. 75 RELATED REPORTS

VRS Management's Assertions Related to OPEB Census Data for the fiscal year ended June 30, 2019

Disability Insurance Program for the fiscal year ended June 30, 2020

Group Life Insurance Plan for the fiscal year ended June 30, 2020

Line of Duty Act Program for the fiscal year ended June 30, 2020

State Health Insurance Credit Plan for the fiscal year ended June 30, 2020

Teacher Health Insurance Credit Plan for the fiscal year ended June 30, 2020

Political Subdivision Health Insurance Credit Plans for the fiscal year ended June 30, 2020

Exit on the VRS 2020 Employer Assurances Audit

The APA will exit with the Committee on the results of their 2020 Employer Assurances Audit for GASB No. 68 and 75. A listing of and hyperlink to the 11 reports issued by the APA as a result of this audit is provided for your convenience in the call out box to the left.

For reference purposes, a list of some types of questions posed to external auditors when exiting are provided below. However, exit meetings with the APA are typically informal, with questions posed as the Committee sees fit.

Typical Questions Posed to External Auditors when Exiting

- Were there any significant adjustments to the accounting records?
- Were there any significant accounting or auditing problems encountered during the examination? Do any remain unresolved?
- Were there any significant changes in accounting policies or principles during the year?
- Were there any indications of financial weaknesses, which should be addressed by the Committee?
- Did you detect any material errors, fraud, illegal acts, or significant deficiencies or material weaknesses in the internal control system?
- Are there any pertinent comments concerning operations in general?
- Did you review information furnished to others (e.g., actuaries)?
- Did the quality and quantity of personnel involved in the preparation and control of financial information appear adequate? Did personnel seem to be fulfilling their responsibilities in a conscientious and professional manner?
- Was the level of cooperation received from management and internal audit during the examination appropriate?
- Did you have enough time to complete all phases of your audit?

Update on the 2021 VRS Annual Comprehensive Financial Report Audit

The APA will provide an update on the status of their examination of VRS' 2021 Annual Comprehensive Financial Report, the final results of which are expected to be presented at the Committee's December meeting.

APA
AUDITOR OF PUBLIC ACCOUNTS
COMMONWEALTH OF VIRGINIA

Audit and Compliance Committee September Meeting

2020 VRS Employer Assurances Engagement

September 13, 2021

Zach Borgerding, Audit Director

Auditor of Public Accounts

Pension and OPEB Plan Types

Single Employer

- Single plan that covers the employees of a single employer

Agent Multiple Employer

- Single plan that covers the employees of multiple employers
- Plan assets are segregated for each participating employer and cannot legally be used to pay other employer’s pension or OPEB obligation

Cost Sharing Multiple Employer

- Single plan that covers the employees of multiple employers
- Plan assets are not legally segregated for each participating employer and can legally be used to pay other employer’s pension or OPEB obligation

Agent Multiple Employer Plans

- Pensions – Political Subdivisions

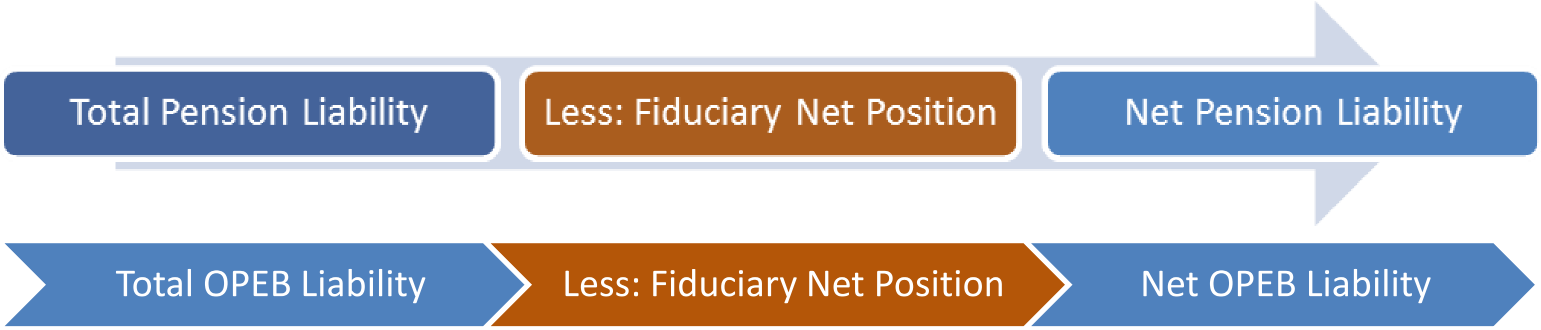
- Health Insurance Credit – Political Subdivisions

Agent Multiple Employer Plan Audit Assurances

Provide opinion on proper accumulation of census data by the plan

Provide opinion on fair presentation of changes in FNP by employer

Net Liability is the Residual Balance



Total Pension Liability

Less: Fiduciary Net Position

Net Pension Liability

Total OPEB Liability

Less: Fiduciary Net Position

Net OPEB Liability

VRS Cost Sharing Multiple Employer Plans

PENSION

- State Plan
- Teacher Plan

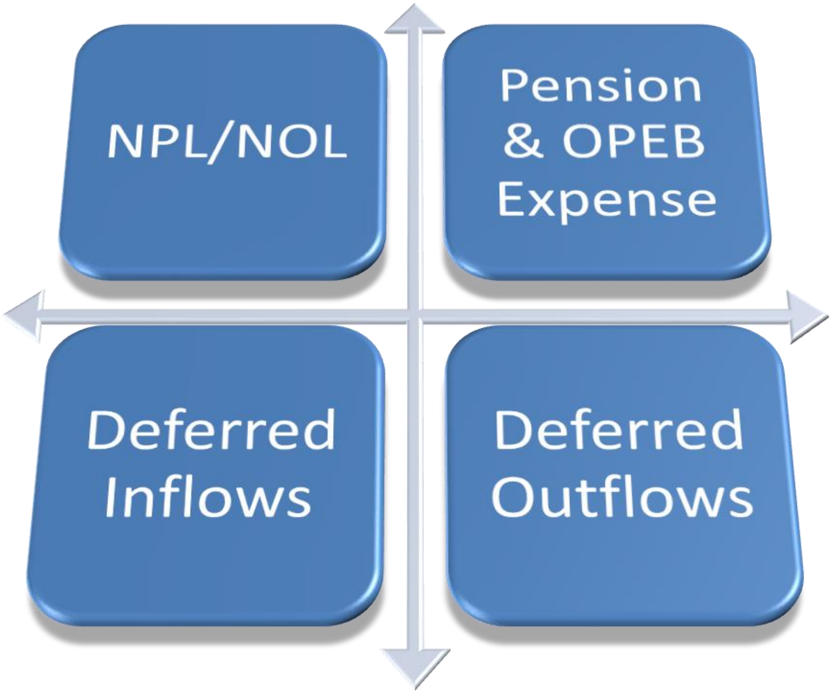
OPEB

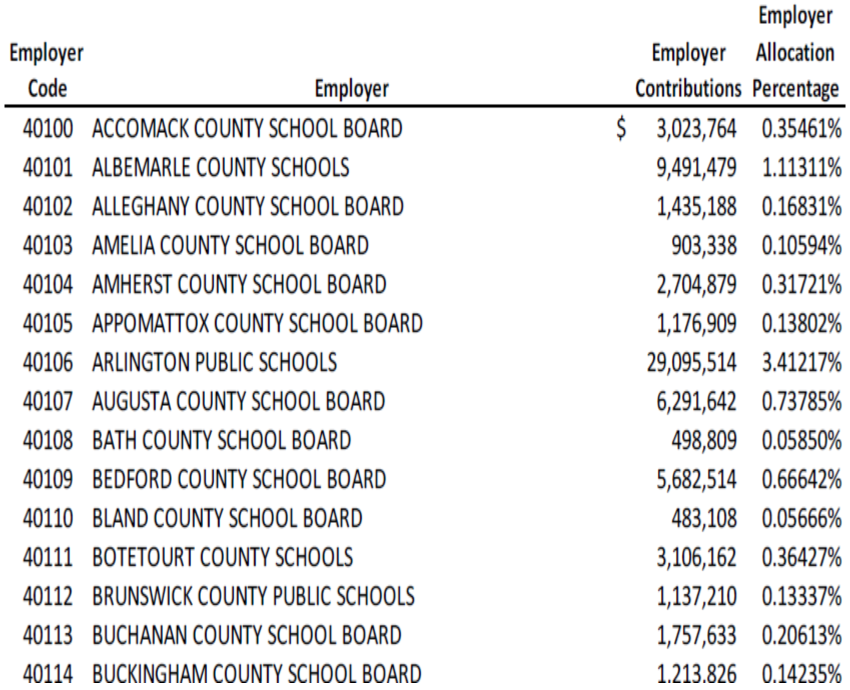
- Health Insurance Credit – Teacher
- Health Insurance Credit – State
- Group Life Insurance
- Line of Duty Act
- Virginia Sickness and Disability Program
- Virginia Local Disability Program (No opinions)

Cost Sharing Multiple Employer Audit Assurances

- Provide opinion on pension/OPEB amounts at plan level

- Provide opinion on employer allocation percentages





			Employer
Employer		Employer	Allocation
Code	Employer	Contributions	Percentage
40100	ACCOMACK COUNTY SCHOOL BOARD	$ 3,023,764	0.35461%
40101	ALBEMARLE COUNTY SCHOOLS	9,491,479	1.11311%
40102	ALLEGHANY COUNTY SCHOOL BOARD	1,435,188	0.16831%
40103	AMELIA COUNTY SCHOOL BOARD	903,338	0.10594%
40104	AMHERST COUNTY SCHOOL BOARD	2,704,879	0.31721%
40105	APPOMATTOX COUNTY SCHOOL BOARD	1,176,909	0.13802%
40106	ARLINGTON PUBLIC SCHOOLS	29,095,514	3.41217%
40107	AUGUSTA COUNTY SCHOOL BOARD	6,291,642	0.73785%
40108	BATH COUNTY SCHOOL BOARD	498,809	0.05850%
40109	BEDFORD COUNTY SCHOOL BOARD	5,682,514	0.66642%
40110	BLAND COUNTY SCHOOL BOARD	483,108	0.05666%
40111	BOTETOURT COUNTY SCHOOLS	3,106,162	0.36427%
40112	BRUNSWICK COUNTY PUBLIC SCHOOLS	1,137,210	0.13337%
40113	BUCHANAN COUNTY SCHOOL BOARD	1,757,633	0.20613%
40114	BUCKINGHAM COUNTY SCHOOL BOARD	1.213.826	0.14235%

APA Issued Unmodified Opinions for the Following

- Accurate and complete accumulation of census data to the actuary for pensions and OPEBs
- Fair presentation of the Schedules of Changes in Fiduciary Net Position at the employer level and related notes
- Fair presentation of pension/OPEB amounts and employer allocations and related notes

Census Data Opinion: Emphasis of Matter

- VRS does not have access to certain census data elements for retirees from an Optional Retirement Plan (ORP) who participate in HIC or GLI and have not claimed a benefit

- Actuary has applied assumptions in place of the data in accordance with Actuarial Standards of Practice

- Opinion was not modified in respect to this matter

Other Audit Results:

- No internal control weaknesses that we would consider significant deficiencies or material weaknesses
- No indications of non-compliance, fraudulent activity or illegal acts
- Proper treatment of accounting principles
- No material alternative accounting treatments
- No significant disagreements with management
- No material audit adjustments requiring the Committee's attention

Future Improvements to Group Life Census Data

Eligibility

- Certain ineligible employees currently included will be excluded
- Reduces total liability by $20.6 million (0.6%)

Rounding

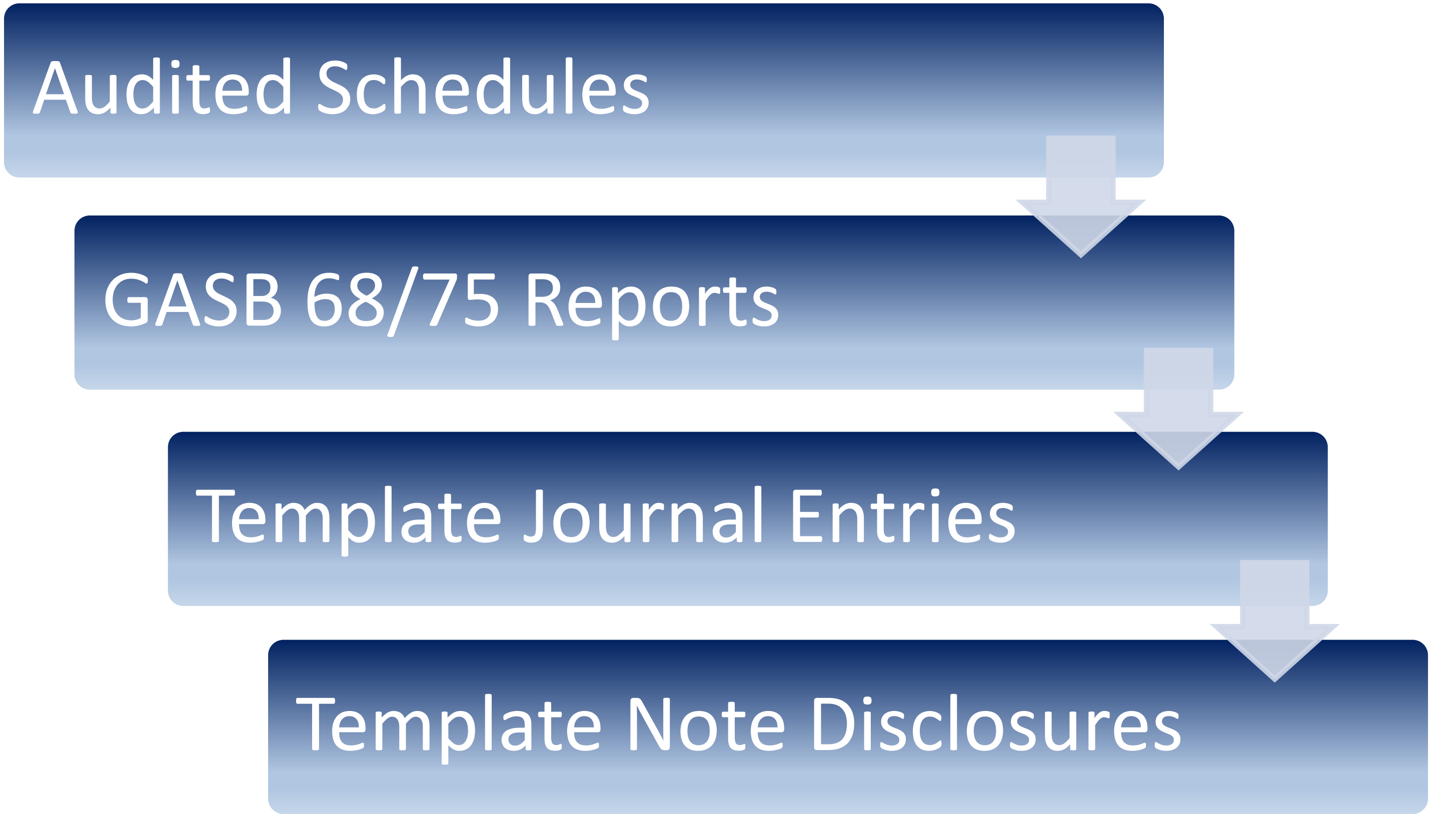
- Presenting service in months rather than rounding by year will increase accuracy
- Reduces total liability by $7.4 million (0.2%)

Future Improvements to VSDP Census Data

Eligibility	Recoveries
• Certain ineligible employees currently included will be excluded • Reduces total liability by $3.1 million (1.2%)	• New data element identified that will be provided to the external actuary for future valuations • Will assist in refining actuarial assumptions

Issuance of GASB 68 and 75 Resources

- Employers received the following pension and OPEB resources:



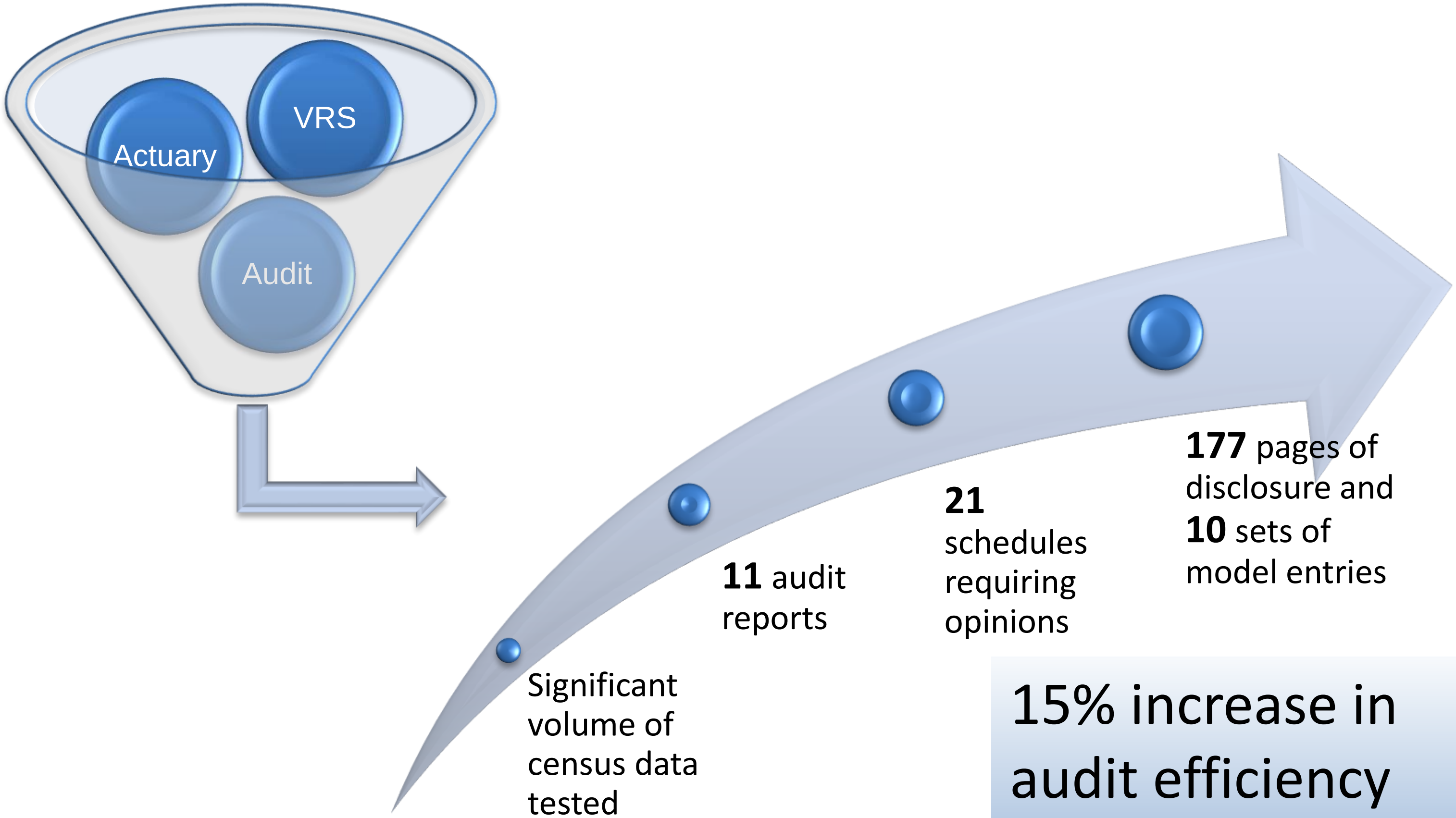
Audited Schedules

GASB 68/75 Reports

Template Journal Entries

Template Note Disclosures

GASB 68 and 75 Project Scope



Significant volume of census data tested

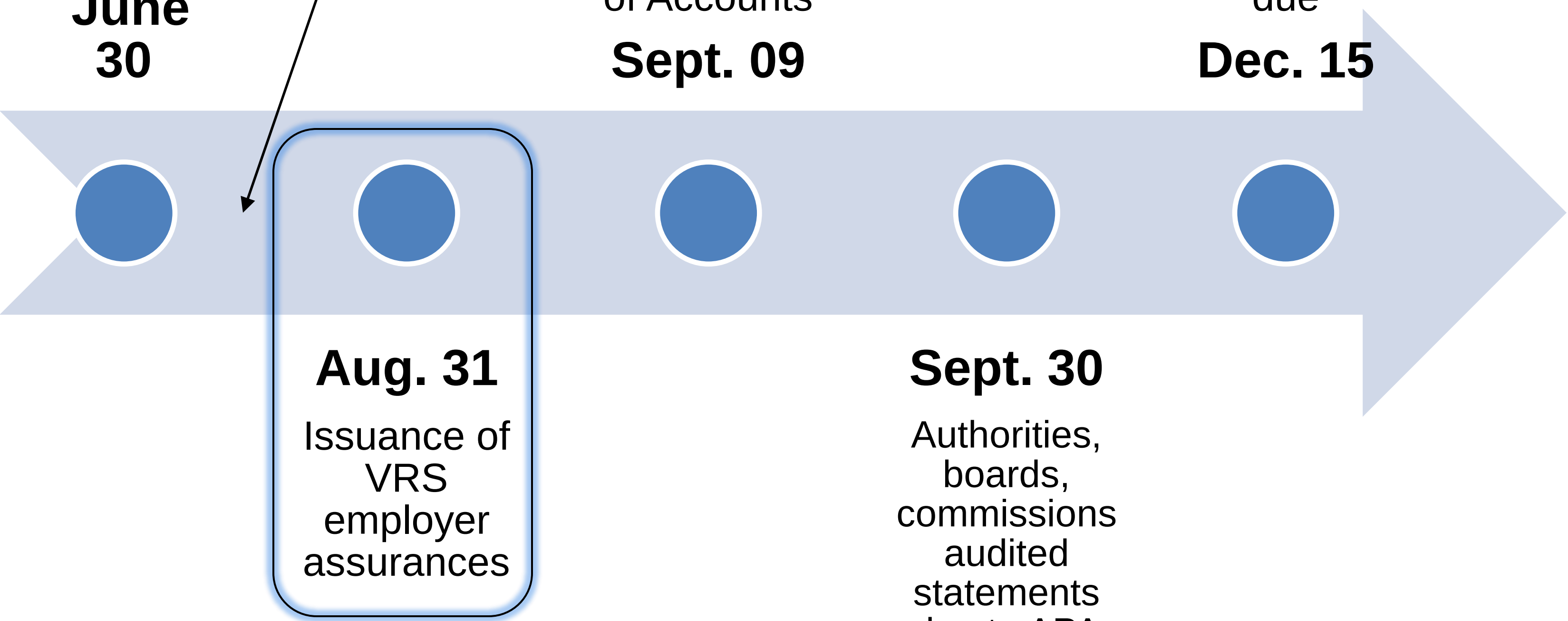
11 audit reports

21 schedules requiring opinions

177 pages of disclosure and **10** sets of model entries

15% increase in audit efficiency from the prior year

Issuance Timely with Room to Improve



Fiscal Year-end

June 30

Future Target Issuance Date: July 31

Aug. 31

Issuance of VRS employer assurances

VA component unit statements due to Department of Accounts

Sept. 09

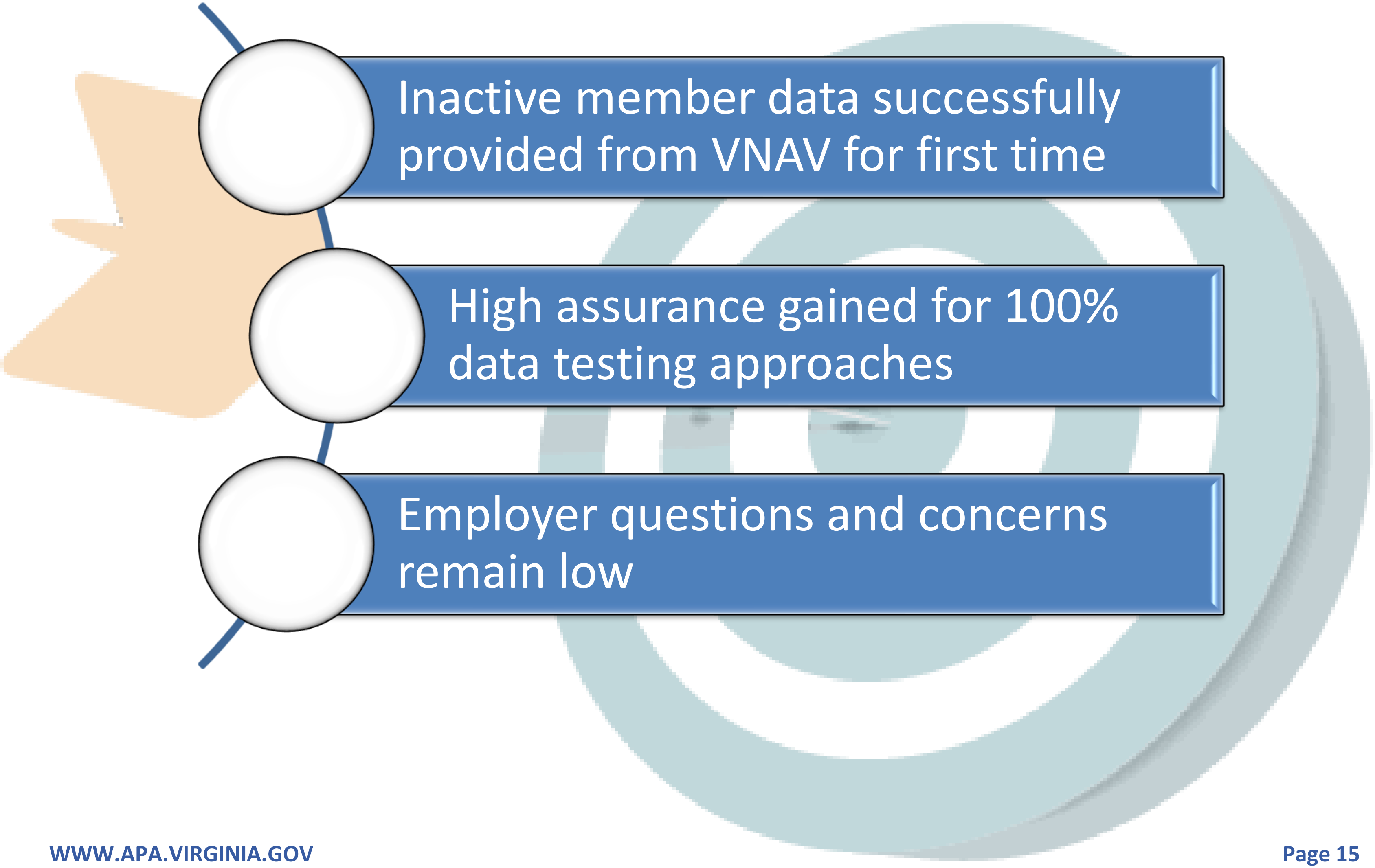
Sept. 30

Authorities, boards, commissions audited statements due to APA

VA, cities, towns, counties audited statements due

Dec. 15

Project Successes



- Inactive member data successfully provided from VNAV for first time
- High assurance gained for 100% data testing approaches
- Employer questions and concerns remain low

Employer Auditor Communications

- VRS audit team annually updates *Specifications for Audits of Counties, Cities, and Towns* and *Specifications for Audits of Authorities, Boards and Commissions* for GASB 68 and 75 requirements

- Local auditors must test active employee data and submit results to APA

- APA Local Government Audit Manager and the VRS audit team communicate with local employer auditors to address inquiries

VRS Annual Report Audit Update

- The audit is progressing adequately, and we are on schedule to complete the audit in advance of December 15th.

- We do not currently have any management recommendations or other issues of concern to bring to the Committee's attention

Intended Use Statement

This presentation is intended solely for the information and use of those charged with governance and management, and is not intended to be, and should not be, used by anyone other than these specified parties.

Audit Reports

Virginia
Retirement
System

INTERNAL AUDIT

Report No. 439

Vendor Hosted Systems in Administrative Operations

As of January 1, 2021

Highlighting VRS Core Values: *Integrity*, *Teamwork*, *Accountability* and *Agility* in Action

THIS REPORT IS INTENDED SOLELY FOR THE USE OF THE VRS BOARD OF TRUSTEES AND THE MANAGEMENT OF VRS AND IS NOT INTENDED FOR OTHER PURPOSES.

TABLE OF CONTENTS

VRS
Virginia
Retirement
System

TRANSMITTAL LETTER

August 2, 2021

Dear Members of the Audit and Compliance Committee,

We have completed audit number 439, “Vendor Hosted Systems in Administrative Operations.” The main purpose of our audit was to evaluate VRS processes for hosted systems used in Administrative Operations to determine if they adequately manage vendor risks.

We conducted our audit in accordance with the *International Standards for the Professional Practice of Internal Auditing*. These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the conclusions based upon our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

This report was distributed to the VRS Director and members of management for review and comment. Management expressed substantial agreement with our report and will issue a written response to the recommendations contained in this report.

We appreciate the cooperation and assistance of the Information Technology department throughout this audit.

Respectfully Submitted,

Jennifer P. Bell Schreck

Jennifer P. Bell Schreck, CPA, CISA, PMP
Audit Director

EXECUTIVE SUMMARY

We conducted an examination of vendor hosted systems used in Administrative Operations for the Virginia Retirement System (VRS) as of January 1, 2021.

Our review determined VRS has processes for managing vendor risks for hosted systems; however, opportunities to enhance these processes exist. These opportunities are described in the Recommendations section and focus on updating policies and procedures and promoting organizational awareness; enhancing risk monitoring of hosted system vendors; and evaluating vendor risk management considerations in the procurement process.

Our review focused exclusively on systems within administrative operations classified as sensitive through the VRS IT System and Data Sensitivity Classification process rather than all vendor hosted systems. The in-scope systems support ancillary activities of the agency. The review did not include sensitive vendor hosted systems used in Investment Operations. They will be considered through a separate review at a later date.

Subsequent to the audit period, management has implemented a new procurement workflow for IT goods and services and is in the process of evaluating additional tools to assist with recurring vendor risk management activities. Management has also implemented a new general ledger system which will bring additional changes to the procurement and payment authorization workflows.

SNAPSHOT

Based on VRS and Commonwealth **Standards,** system **sensitivity** is determined through a risk consideration of system **confidentiality**, **integrity** and/or **availability**. While a "**high**" risk assessment of **any** of the above **factors** will **result** in a system **designation** as sensitive, there are **degrees** of sensitivity and risk.

VRS has classified **four vendor hosted systems** which support ancillary business processes in its **Administrative Operations** as **sensitive**.

While VRS **contracts with vendors** to use these **systems**, VRS **retains accountability** for **protecting** its IT **environment**, including its **data**.

AUDIT ASSESSMENT

VRS has processes for managing vendor risks for hosted systems used in Administrative Operations; however, opportunities to enhance these processes exist.

Written Recommendations: 3

BACKGROUND

INTRODUCTION

Historically, technology vendors have offered products that can be installed on-premise on their customers' networks. This service model allowed customers to own and maintain all aspects of the operating systems, network and other infrastructure impacting these products, thereby having primary control over IT security and data protection. Technology goods and services have continued to evolve, with customers now able to access systems and data over the internet on a vendor's network, or "in the cloud". Cloud-based products allow customers to access software and other services hosted, or residing, outside of their organization's network.

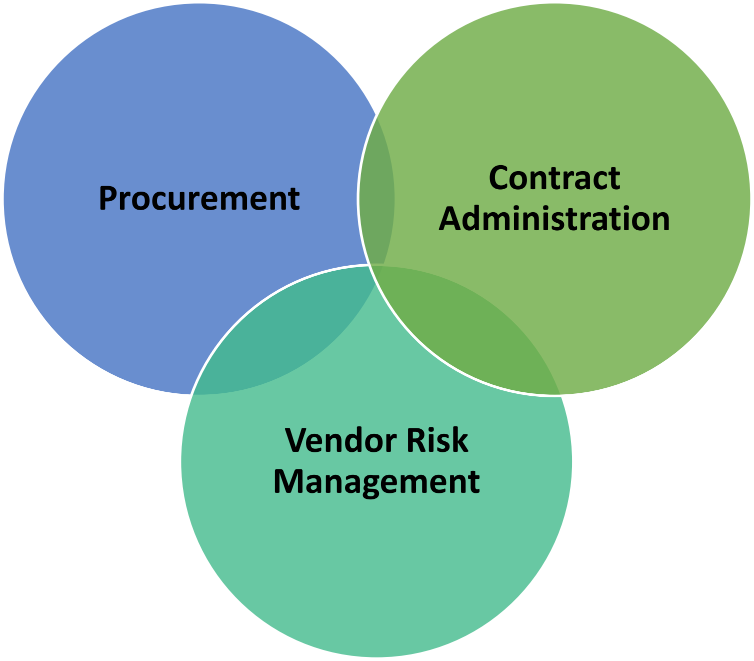
Cloud Service Models

Cloud products provide customers with new benefits such as: low fixed costs, remote access, rapid scalability, quicker deployment of IT strategies and enhanced resiliency and redundancy. Typically, cloud vendors provide their customers with one of the following three service models: infrastructure as a service (IaaS), platform as a service (PaaS), or applications, also known as software as a service (SaaS).

Cloud Service Models		
Infrastructure as a service (IaaS) provides consumers with the capability to use vendor processing, storage, networks and other fundamental computing resources, where the consumers can deploy and run software, including operating systems and applications. Consumers do not manage or control the underlying cloud infrastructure, but do have control over the operating systems, storage and deployed applications and possibly limited control of select networking components.	**Platform as a service (PaaS)** provides consumers with the capability to deploy onto a vendor cloud infrastructure, consumer-created or acquired applications. Consumers do not manage or control the underlying cloud infrastructure, but do manage or control the deployed applications and possibly configuration settings.	**Software as a Service (SaaS)** provides consumers with the capability to use a vendor's applications running on a cloud infrastructure. Consumers do not manage or control the underlying cloud infrastructure or the application, with the possible exception of limited user-specific application configuration and access settings.

As products and services have transitioned to cloud models, the IT security responsibilities and associated risks necessarily have shifted to be shared between VRS and its cloud vendors. These risks include data security, reliability and availability of services, integration with existing VRS systems and delegation of responsibilities to the vendor. VRS has demonstrated its *agility* by adapting its processes accordingly to address these risks. In this new environment, while VRS may delegate certain responsibilities to its vendors, VRS retains ultimate *accountability* for protecting its assets, including its data.

VRS' approach for vendor risk mitigation is governed by its adherence to applicable standards, policies and procedures in the following areas:



Coordinated Collaborative Processes

Business owners identify technology goods and services to meet their operational needs. While their respective processes are decentralized, and involvement is tailored to each relationship, VRS' IT, Procurement and Policy Planning and Compliance departments collaborate with these business owners to evaluate prospective vendors during procurement and then afterwards to support contract administration throughout the vendor relationship. The coordination, performance and *teamwork* of each area's responsibilities are critical with respect to reviewing contractual language, establishing a baseline understanding of vendors' controls through initial risk assessments and accomplishing ongoing vendor risk monitoring activities throughout the vendor partnership.

VRS' IT department serves an integral role in these processes by providing insights and expertise in analyzing vendor IT security and data management practices for compliance with applicable requirements before initial procurement and throughout the entire contract term. This gives VRS the opportunity to identify and preemptively address incongruities between each partner's control expectations. Business owners are assigned as the contract administrators for these relationships. VRS relies on the knowledge and insights offered by all three departments and assigned contract administrators to carry out vendor risk management activities.

Four SaaS systems in VRS' Administrative Operations' area are the focus of this review.

As a result, all cloud-based references from this point forward refer to SaaS platforms.

Vendor Hosted Systems in VRS' Administrative Operations

VRS uses various vendor hosted systems across its business processes. Four vendor hosted systems in VRS' Administrative Operations are SaaS and have been classified by VRS as sensitive. Each of these systems support business processes for which compromise with respect to confidentiality, integrity and/or availability could have an adverse effect on Board of Trustees (Board) and Board committee communications, human resources, timesheet capture, employee performance and employee alerts and notifications. These systems are governed by the accepted VRS standards, policies and procedures for SaaS products.

VITA's Information Security **Standard** for **Hosted Environments** became **effective** in June **2017**.

In response, **VRS** created its **Cloud Services** Information Security **Standard** in **2017** and finalized it in **2018**. This standard **adopts** the **VITA standard** by reference.

STANDARDS, POLICIES AND PROCEDURES

VRS Standards

VRS is subject to certain requirements of the Virginia Information Technologies Agency's (VITA) Information Technology Security Program. To address the mandatory VITA requirements, VRS has formulated its own IT Security Program, which meets and at times exceeds VITA's requirements, with supplemental information to clarify specific VRS procedures and processes.

In support of its IT Security Program, VRS created the VRS IT Security Program Policy and Standard, along with the VRS Cloud Services Information Security Standard, which notes VRS' adoption of VITA's Information Security Standard for Hosted Environments. The VRS Cloud Services Information Security Standard establishes minimum information security requirements for activities associated with engaging vendors for cloud products, as in these service models Commonwealth data is being stored at a data center not owned by a state agency.

Three of the four in-scope SaaS vendor relationships were initiated prior to the adoption of the VITA and VRS Cloud related policies, standards, guidance and services.

Annually, Internal Audit evaluates the conformance of VRS' Information Technology Security Program with the requirements set forth by VITA. Our most recent review, completed as of November 1, 2020, acknowledged VRS' continued conformance with VITA's requirements in the design of its security program.

While **VRS** must **comply with** the VITA **Information Security Standard** for **Hosted Environments**, VRS **does not** have to **obtain VITA approval** to engage a cloud vendor **nor** is VRS **required to use** VITA **services**.

However, as the Commonwealth's information technology agency, **VITA** is a **recognized resource** of accepted **industry practices** when **establishing** and **maintaining relationships** with cloud vendors for Commonwealth entities.

Other VITA Guidance and Services

VITA provides additional guidance and services to state agencies to support the Commonwealth in establishing and maintaining vendor relationships that comply with VITA's Information Security Standard for Hosted Environments. VITA's additional guidance and services include the Third-Party Use Policy and Procedures, IT Procurement Manual and Enterprise Cloud Oversight Service. While VRS is not required to follow this guidance or use these services, they generally are reflective of current best practices.

VITA Third-Party Use Policy and Procedures

The VITA Third-Party Use Policy and Procedures outline the requirements and responsibilities for state agencies, suppliers and VITA for acquisitions of and risk monitoring of cloud services. It supports the adoption of cloud service providers that comply with the VITA Information Security Standard for Hosted Environments and VITA's cataloging of cloud services used by the Commonwealth.

VITA IT Procurement Manual

The VITA IT Procurement Manual provides procurement methodologies and processes that comply with statutory requirements, but also are based on generally accepted government and industry best practices for the procurement of IT. The manual covers a variety of topics, including guidance specific to cloud service procurements including insurance and agency IT procurement security and cloud requirements for solicitations and contracts.

VITA Enterprise Cloud Oversight Service

VITA created the Enterprise Cloud Oversight Service (ECOS) to provide service level assessment and performance monitoring services for SaaS vendors on behalf of the Commonwealth. Executive branch state agencies are eligible to order services from ECOS which include assessment reviews, supply chain management consulting and oversight services for SaaS vendors and their products.

Being an approved ECOS vendor does not mean that VITA ECOS has assessed and is monitoring all products and services provided by a vendor. Rather VITA ECOS services extend only to the vendors and the SaaS products for which they have been engaged as reflected on the Approved Supplier Application List, which is publicly available on VITA's website. Three of the four SaaS vendors considered in-scope for this review are included on the VITA ECOS Approved Supplier Application List; however, one of the in-scope systems supplied by one of these three vendors is not.

As an independent agency, VRS can, at its discretion, purchase ECOS services to assist with the initial assessment and ongoing risk monitoring of its SaaS vendors. As of the report date, VRS has not purchased these services, but is working towards establishing an ECOS service account so that it can.

VRS' Approach

VRS is *accountable* for creating and adhering to its own policies and procedures to assess and manage risks for its cloud vendors and maintain compliance with its VRS Cloud Services Information Security Standard. To manage compliance during procurement and throughout the vendor relationship, VRS has developed a Technology Procurement Policy, Technology Procurement Procedures, Technology Procurement Purchase Request How-To Guide and Vendor Security Agreement Review Procedures. Additionally, the procurement of IT goods and services and related contract administration are subject to the general requirements of the VRS Purchasing Procedures maintained by the Procurement department.

SaaS VENDOR TECHNOLOGY PROCUREMENT PROCESSES

In 2018, management implemented the VRS Technology Procurement Policy which defines procedural and approval requirements for all technology-related acquisitions. The VRS Technology Procurement Procedures and VRS Technology Procurement Purchase Request How-To Guide lay out the internal workflows necessary to meet the VRS Technology Procurement Policy requirements.

New SaaS Acquisitions

For any IT good or service, a procurement request is created and goes through an internal workflow for technology procurements. Further, SaaS products undergo a VRS Cloud Vendor Security Review which includes completion and consideration of the following, as applicable:

Security Review Results Document

- Summarizes the business justification, designated VRS contacts, product information, research resources, identified risks and controls and vendor contact information.
- Provides a “security response”, including clearance/denial for the request and any additional steps the business owner and IT Security will need to take prior to and after the SaaS product is put into production.

Third-Party Assurance Reports Analysis

- Summarizes information gathered from third-party assurance report(s) within the vendor’s Security Review Results Document and Questionnaire for Hosted Solutions. Generally includes the document title and timeframe covered for each report.
- Provides any observations, issues, risks or mitigations from IT Security.
- Acknowledges deviations from the VRS Cloud Security Standard requiring follow-up and/or resolution.

Questionnaire for Hosted Solutions

- Captures the vendor's services and IT environment as described by the vendor.
- Uses the vendor’s third-party assurance reports as resources to validate compliance of the service with VITA’s Information Security Standard for Hosted Environments.
- Includes follow up with vendor for clarification and responses on any questions not addressed by the third-party assurance reports.

VRS Vendor IT Security Agreements

Based on the above, management will assess the need for various VRS vendor IT security agreements to be executed with the SaaS vendor, to ensure VRS, its environment and its data are appropriately protected. Those security agreements are described on the following page.

Interconnection Security Agreement*

- Necessary when VRS and a private sector vendor have a dedicated connection between IT systems. Applicability assessed based on whether a persistent connection with VRS systems exists.
- Documents the technical and security requirements of the connection, as well as understanding of the data being exchanged (classification as sensitive or not, storage practices, logical access, etc.), along with the data flow.

Security Conformance Agreement*

- Acknowledges the vendor’s agreement to comply with all provisions of the current VITA IT Security Program, including VITA’s Information Security Standard for Hosted Environments. The vendor’s compliance responsibilities extend to any subcontractors, also known as subservice organizations, it uses as well.
- When requirements in the VITA IT Security Program change, obligates the vendor to comply with any changes by the vendor by the compliance date of the updated standard or VRS to submit an exception request to VITA documenting the non-compliant aspects of the service.

Confidentiality and Non-Disclosure Agreement*

- Includes VRS’ definition of confidential information and how the vendor should use and share it.
- Requires the vendor to obtain VRS approval prior to disclosing any confidential information with subcontractors.
- Supplements the security conformance agreement by providing additional guidance on the vendor responsibilities related to VRS confidential information in the event of a data breach or termination of the contract.

*Alternatively, in practice, all or part of an agreement’s terms may be incorporated into the contract language or vendor terms and conditions, potentially eliminating the need for a standalone agreement. Depending on their extent and nature, these modifications may be subject to review by VRS’ Policy Planning and Compliance department.

For **small dollar procurements**, including those made with small purchase charge cards, **VRS follows** Commonwealth Accounting **Policies and Procedures** (CAPP) issued by the **Department of Accounts**.

Procurement Methods

VRS can procure technology-related goods and services by leveraging existing federal General Services Administration (GSA) contracts, VITA or other statewide and cooperative contracts; by going through the competitive bid process to establish its own contract with the vendor or by following small dollar purchase guidance.

When available for the requested goods and services, existing federal or statewide contracts may provide VRS the opportunity to obtain lower prices based on the aggregation of demand from multiple federal and/or state agencies. Additionally, since the contract is already in place, VRS saves time by reducing procurement activities normally associated with the competitive bid process.

Depending on the procurement method, VRS' ability to negotiate contract terms and successfully obtain executed VRS Vendor IT Security Agreements may be impacted.

Contract Renewals

Unlike new acquisitions, contract renewals do not have a procurement request created or go through the internal workflow for the technology procurement process. Instead, IT Security is notified of contract renewals and the associated purchase requisitions through email and coordinates with other areas within the IT department to provide approvals as needed.

A contract renewal also presents an important opportunity for VRS, the vendor, or both parties to modify contract and agreement terms. Specifically, in instances where VRS contracted with a vendor prior to the 2018 implementation of the VRS Technology Procurement Policy, documents supporting the Cloud Vendor Security Review process may not be present or may be inherently outdated and require updates. The contract renewal provides the best opportunity to address these documents. However, the extent of VRS' ability to do so may be limited depending on the nature of the contract vehicle as well as the vendor service being procured.

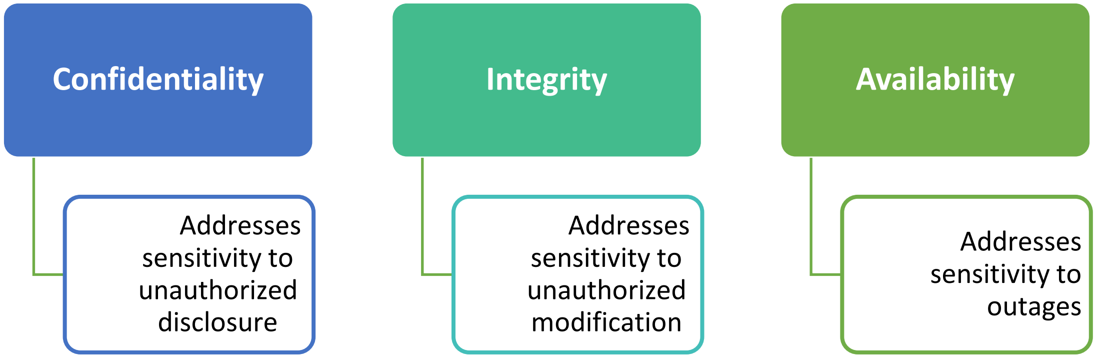
Other IT Approvals

All payments made to vendors are subject to the requirements included in the VRS purchase requisition process defined by VRS Purchasing Procedures. As a part of these procedures, payments to vendors for IT goods and services require pre-approval from members of the IT department.

IT SYSTEM AND DATA CLASSIFICATIONS AND RELATED RISK ASSESSMENTS

After the internal workflows defined by the VRS Technology Procurement Procedures are completed, the assigned IT Security Analyst will assess the IT System and Data Sensitivity Classification for the acquired product to determine the steps needed to protect the *integrity* of the application and the VRS information which resides within it. This classification is based on input from the business owners and an assessment of how the product will be implemented operationally and technically, including understanding the VRS owned data the business unit will be inputting to the system or providing the vendor.

This process is used to identify and classify IT system and data sensitivity with respect to:



Confidentiality

Addresses sensitivity to unauthorized disclosure

Integrity

Addresses sensitivity to unauthorized modification

Availability

Addresses sensitivity to outages

"Sensitive" systems or data are any for which compromise with respect to confidentiality, integrity and/or availability could have a material adverse effect on VRS operations. Once this classification is complete, it allows VRS to refine its security practices, placing the greatest focus on the highest risk or most sensitive systems.

The classification is completed before a system is put into production. Afterwards, the classification is reviewed annually and updated as needed to maintain accurate risk assessments in support of security plans and the Continuity of Operations Plan (COOP). The most recent full revision of the COOP was completed during fiscal year 2020.

Risk Assessments

VRS has adopted the VITA Information Security Standard for Hosted Environments within its VRS Security Cloud Standard. Per section 6.1 of the VITA Standard, it states that the risk assessment requirements define the steps VRS must take for each system classified as sensitive to:

- Identify potential threats to an IT system and the environment in which it operates;
- Determine the likelihood that threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

Further, section 6.2 of the VITA Standard specifies that the data-owning agency (VRS) shall conduct and document a risk assessment for each IT system classified as sensitive as needed, but not less than once every three years, and perform an annual self-assessment to determine the continued validity of the existing risk assessment.

For SaaS systems classified as sensitive, VRS retains ownership of its data. As the data-owning agency, VRS is required to perform these risk assessments.

VENDOR RISK MANAGEMENT

Contract Administration Responsibilities

Once VRS' initial contract with the vendor is finalized, a contract administrator is assigned and plays a key role in vendor risk monitoring. Generally, the assigned contract administrator works in the business unit which is the primary user of the vendor's product.

Contract administrator responsibilities in relation to IT Security include:

- Ensuring any limitations included in the security review are adhered to throughout the life of the good or service.
- Making certain the vendor meets security-related performance requirements specified in the initial approval and incorporated in the contract, with the assistance of VRS Procurement and IT departments. These include, but are not limited to:

  - All remediation required following contract signing occurs in a timely manner,
  - Any required periodic reviews or submissions happen in a timely manner throughout the life of the contract (including third-party assurance reports),
  - Security-related performance of the vendor is validated, and
  - IT Security approval is obtained prior to any contract renewal, including updating any necessary security-related provisions and requirements captured in the contract or supplemental agreements.
- Providing notification to IT Security in the event of changes in how the vendor’s product is being used (i.e., new services or additional products).

IT Related Responsibilities

After the initial procurement and IT System and Data Sensitivity Classification is complete, the vendor is subject annually to the VRS Vendor Security Agreement Review Procedures. In support of this, VRS adds the vendor to a tracking spreadsheet used by VRS’ IT Security Analysts to plan for and manage ongoing annual risk monitoring activities of vendors providing technology goods and services. Annually, IT Security reviews the identified VRS Vendor IT Security Agreements and determines if any updates are necessary.

Changes in how the vendor’s product is used or adjustments to the contractual arrangement may trigger IT Security to perform a review of the vendor earlier than the scheduled annual review and prompt changes to some or possibly all documents completed as part of the VRS Cloud Vendor Security Review. Due to the decentralized nature of VRS’ vendor management activities, IT Security is reliant on the contract administrator to promptly communicate these types of changes.

Annual Review of Third-Party Assurance Reports

IT Security’s annual monitoring of existing vendors also involves reviewing the most recent third-party assurance reports. Service Organization Controls (SOC) reports or other third-party assurance reports demonstrate the vendor’s ongoing compliance with the VITA Information Security Standard for Hosted Environments as well as changes in controls that may be significant to VRS as the customer, also known as the user entity.

Obtaining and reviewing third-party assurance reports may require collaboration among IT Security, business owners and assigned contract administrators. Business owners and assigned contract administrators are able to provide insight into how a vendor's system is used in VRS' operations and valuable input on any non-technical controls VRS needs in place to support the vendor. Vendor expectations regarding such user entity controls are included in service organization control reports discussed below and commonly known as complementary user entity controls.

IT Security's identification of control gaps or deviations in respect to the VITA Information Security Standard for Hosted Environments may result in a more detailed review of the vendor's hosted controls, and as needed, updating the Questionnaire for Hosted Solutions and the Security Review Results Document for the system. Ultimately, the vendor may be required to provide VRS with additional documentation as evidence of its compliance with the VITA Information Security Standard for Hosted Environments.

Service Organization Control Reports

Most often, third-party assurance is provided through a SOC report. While several versions of the SOC report exist, a SOC 2, Type 2 report generally is considered most beneficial when evaluating IT vendor service organizations. Such SOC reports provide management of the vendor's organization, user entities (i.e., potential and existing customers, such as VRS) and other intended recipients information about the effectiveness of the vendor's controls throughout a specified time period related to the security, availability or processing integrity of the service organization's system and the confidentiality and privacy of the data managed by that system.

A user entity's review of a cloud vendor's SOC report generally includes:

- Confirming the time period and scope
- Assessing the credentials of the auditor
- Evaluating the Auditor's Opinion and Management's Assertions
- Identifying significant subservice organizations excluded from the scope and assessing the need to obtain and review their available third-party assurance reports
- Understanding the controls tested and any exceptions identified and considering their impact relative to the requirements of the VITA Information Security Standard for Hosted Environments

When **assessing** the **risks introduced** by a **vendor relationship**, VRS should **also consider** the **services provided** to the vendor **by other organizations** which **may impact** VRS' overall control **environment**. These other organizations are **identified** as "**subservice organizations**" within **SOC reports**.

FedRAMP was established in 2011 to **provide** a **cost-effective**, **risk-based** approach for the **adoption** and use of **cloud services** by the **federal government**.

A FedRAMP security **package** provides **evidence** of an **in-depth examination** of a cloud solution's **data security** and data **governance capabilities** in relation to the **standardized** security **assessment**, **authorization** and **monitoring practices** developed by the federal government.

- Mapping vendor expected complementary user entity controls to the user entity to identify any gaps

Other Third-Party Assurance Reports

If a SOC report is unavailable, third-party assurance based on certain other frameworks can be used. Acceptable alternatives to a SOC 2, Type 2 report may include: the cloud vendor's Federal Risk and Authorization Management Program (FedRAMP) security package, penetration test results and any other reports or artifacts related to an independent third-party's assessment of a vendor's IT security and the related controls. Regardless, VRS is dependent on the information the vendor will share with them to perform their reviews, complete any necessary assessments and make any appropriate control adjustments.

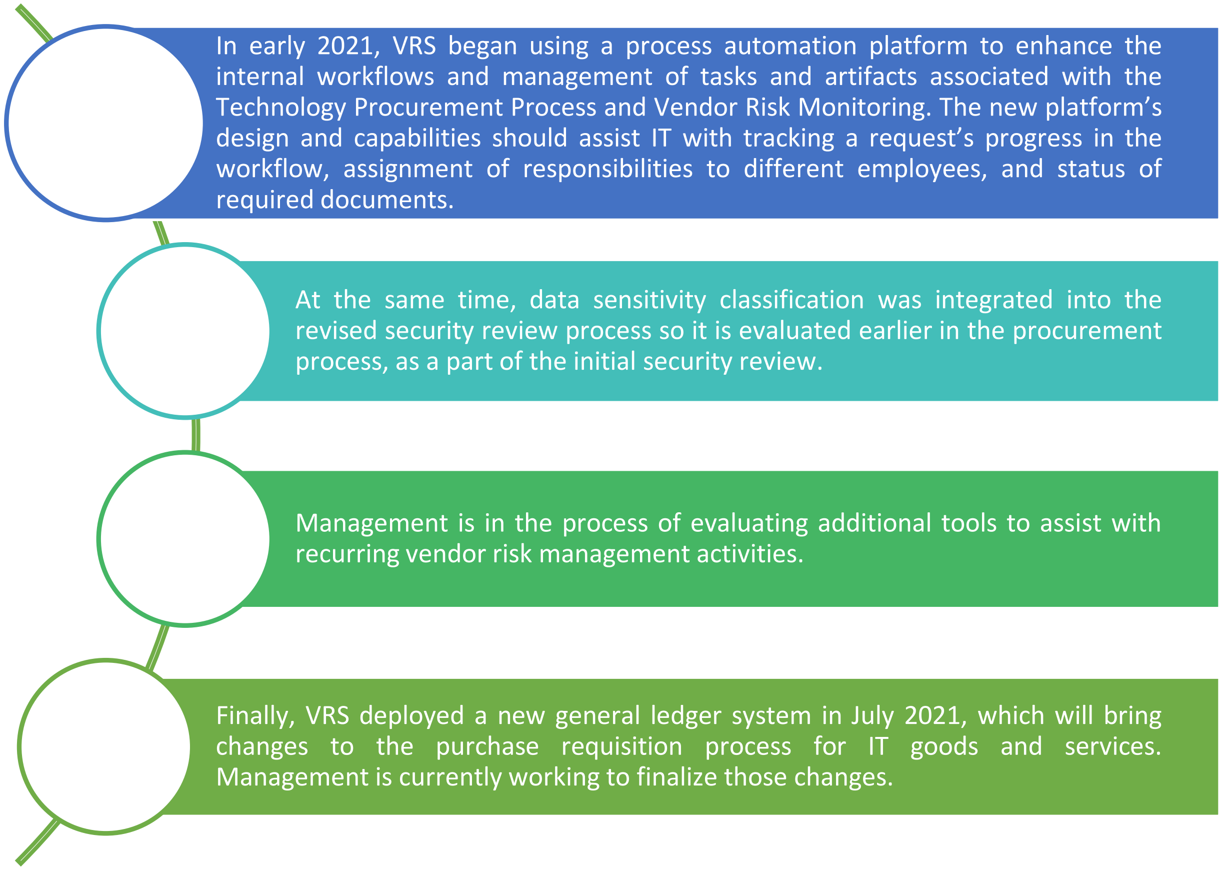
Frequency and Timing of Such Reviews

The VRS Cloud Services Information Security Standard specifies that for hosted systems *"Compliance will be verified, as defined by the VITA Information Security Standard for Hosted Environments, with an initial and an annual security review of the environment or review of their annual audit report of the environment conducted by an independent, third-party audit firm."*

Additionally, VITA Third-Party Use Policy and Procedures directs the agency to a perform a security audit within 90 days of being provided a recently completed third-party assurance report for a cloud vendor. As previously noted, the purpose of the security audit is to determine control gaps with the VITA Information Security Standard for Hosted Environments and to follow-up, as needed, on any deviations noted within the cloud vendor's or VRS' controls. Timely review of third-party assurance reports supports early identification of these control gaps as well as those between VRS and the vendor and the opportunity to respond to these gaps and their associated risks promptly.

Recent Changes to the Procurement Process and Vendor Risk Management

Several recent changes within the organization will support VRS' procurement and vendor risk management practices.



In early 2021, VRS began using a process automation platform to enhance the internal workflows and management of tasks and artifacts associated with the Technology Procurement Process and Vendor Risk Monitoring. The new platform's design and capabilities should assist IT with tracking a request's progress in the workflow, assignment of responsibilities to different employees, and status of required documents.

At the same time, data sensitivity classification was integrated into the revised security review process so it is evaluated earlier in the procurement process, as a part of the initial security review.

Management is in the process of evaluating additional tools to assist with recurring vendor risk management activities.

Finally, VRS deployed a new general ledger system in July 2021, which will bring changes to the purchase requisition process for IT goods and services. Management is currently working to finalize those changes.

SCOPE AND METHODOLOGY

The primary purpose of our examination was to determine whether VRS processes for hosted systems used in Administrative Operations adequately manage vendor risks.

Our examination did not include all vendor hosted systems, it focused solely on systems used in support of Administrative Operations classified as sensitive by VRS and its IT System and Data Sensitivity Classification process.

GENERAL ASSESSMENT AND UNDERSTANDING

We obtained a general understanding of the vendor hosted systems in Administrative Operations as well as the procurement and vendor risk management related controls by meeting with key individuals from each area and observing processes. We also reviewed the applicable policies and procedures and other relevant documents.

STANDARDS, POLICIES AND PROCEDURES

We obtained all relevant policies and procedures around the acquisition and management of cloud vendor environments, as a whole, to determine if VRS had appropriate governance and documentation in place, including an adequate control structure to provide reliance that controls were functioning as intended. To support this understanding, we obtained and reviewed the:

- VITA Information Technology Security Program;
- VRS Cloud Services Information Security Standard with the embedded VITA Information Security Standard for Hosted Environments;
- VITA's Third-Party Use Policy and Procedures;
- VRS Technology Procurement Policy and Procedures;
- VRS Vendor Security Agreement Review Procedures; and,
- VRS Purchasing Procedures.

Collectively, the VRS standards, policies and procedures were reviewed for relevancy compared to operational processes, for consistency relative to other organizational procurement policies and procedures and for adequacy in supporting vendor risk management activities, which included a consideration of guidance and resources published by VITA.

Further, once we understood VRS' hosted governance structure and requirements, we gathered information related to VITA ECOS and its services and the current ECOS approved supplier list.

Finally, we obtained and reviewed VITA's IT Procurement manual for guidance specific to cloud service procurements including insurance and agency IT procurement security and cloud requirements for solicitations and contracts. We reviewed the guidance relative to VRS practices.

SaaS VENDOR TECHNOLOGY PROCUREMENT PROCESSES

All procurement requests created and completed during calendar year 2020 for the in-scope systems were reviewed for compliance with the VRS Technology Procurement Policy and Technology Procurement Procedures. Specifically, each procurement request was reviewed for evidence of IT approvals captured as part of the internal workflow for technology procurements and completion of the VRS Cloud Vendor Security Review. All elements of the VRS Cloud Vendor Security Review were examined, which included the Security Review Results Document, Third-Party Assurance Report analysis, Questionnaire for Hosted Solutions and the applicable VRS vendor IT security agreements. This information was evaluated along with the selected procurement methods and contract language to collectively assess if they adequately support VRS' vendor risk management activities.

Additionally, all purchase requisitions and supporting documentation for procurement requests and contract renewals processed for the vendors during calendar year 2020 were reviewed to ensure approvals were obtained from the IT department as required by the VRS Technology Procurement Policy and Technology Procurement Procedures.

IT SYSTEM AND DATA CLASSIFICATIONS AND RELATED RISK ASSESSMENTS

IT System and Data Classifications

The IT System and Data Sensitivity Classifications for all in-scope systems were reviewed to confirm they were completed and evaluated in respect to the system's confidentiality, integrity and availability.

Risk Assessments

Further, based on each system's classification as sensitive, their initial or annual risk assessment, as applicable, was requested to review for compliance with the VRS Cloud Services Security Standard and the VITA Information Security Program, as necessary.

VENDOR RISK MANAGEMENT

Contract Administration Responsibilities

Responsibilities for contract administration included in the VRS Technology Procurement Policy and VRS Purchasing Procedures were reviewed for understanding and consistency.

Awareness of contract administration responsibilities included in the VRS Technology Procurement Policy was evaluated by making inquiries of the assigned contract administrators.

Finally, evidence of vendor performance monitoring submitted to the Procurement department by contract administrators was evaluated to assess their timeliness and adequacy in supporting vendor risk management activities.

IT Related Responsibilities

The tracking spreadsheet for the VRS Vendor Security Agreement Review Procedures was obtained and the completion of the annual review process during calendar year 2020 was evaluated. Further, we requested the Questionnaires for Hosted Systems for SaaS systems that had a relationship with VRS prior to the implementation of the VITA Information Security Standard for Hosted Environments.

Annual Review of Third-Party Assurance Reports

Evidence of IT Security's receipt and review of third-party assurance reports for the vendors was reviewed to evaluate timeliness, identification of control deficiencies and gaps relative to the VRS Cloud Services Security Standard and consideration of other significant report elements, including complementary user entity controls and their relationship to VRS controls.

Evidence of participation of contract administrators in the request and review of these reports was evaluated to assess their timeliness and adequacy in supporting vendor risk management activities.

CONCLUSIONS

GENERAL ASSESSMENT AND UNDERSTANDING

Our review found VRS has processes for managing vendor risks for hosted systems used in Administrative Operations; however, we have identified opportunities to enhance these processes related to updating policies and procedures and promoting organizational awareness; enhancing risk monitoring of hosted system vendors; and evaluating vendor risk management considerations in the procurement process. These opportunities are introduced below and discussed in further detail within the Recommendations section of this report.

STANDARDS, POLICIES AND PROCEDURES

Standards, Policies and Procedures

VRS has created appropriate standards, policies and procedures related to the hosted vendor environment which align with the required elements of VITA's standards and policies. However, these documents require integration and revisions to reflect current operational processes and provide a comprehensive and consistent depiction of the IT procurement process, contract administrator responsibilities and vendor risk management activities. These items are discussed further within the Recommendations section of this report. An additional item highlighted in the VITA's IT Procurement manual guidance for cloud service procurements was communicated separately to management for their consideration.

SaaS VENDOR TECHNOLOGY PROCUREMENT PROCESSES

IT Procurement Related Requests

IT Procurement related requests created and completed during the audit period for the in-scope systems did not fully comply with the VRS Technology Procurement Policy and Technology Procurement Procedures.

Approval of IT Procurement Requests

Evidence of all IT procurement requests approvals was not retained within the internal IT procurement workflow tool, as the workflow tool disposed of this information after 60 days. Alternative evidence for most approvals was obtained through review of purchase requisitions and/or the Security Review Results Documents.

VRS is in the **process** of migrating its **on-premise** infrastructure **systems** to the **cloud**.

One of VRS' four **Agency Performance Outcomes** focuses on this **cloud migration** project.

VRS' intentional **focus** on this area **highlights** the **importance** of sound **control processes** related to **cloud**-based **services** being placed into operation and **followed** to **protect** its **assets**.

When discussed with management, they indicated a new procurement workflow was implemented subsequent to the audit period. Management should assess and refine the approval retention period in the new tool, in coordination with VRS' current Records Management initiative, to ensure the most practical time period for retention of this information.

Completion of VRS Cloud Vendor Security Review

With respect to the two VRS Cloud Vendor Security Reviews performed during the audit period to support an initial procurement or when changes to services were made for an existing vendor, certain elements supporting this process were not available, as summarized in the chart below.

		System 1	**System 2**
Year Vendor Relationship Initiated		2020	2014
Contract Vehicle		VITA Contract	GSA Contract
Security Review Results Document		Completed	Updated in 2020, due to change in services
Available Third-Party Assurance Report Period		10/1/2018 – 3/31/2019	10/1/2018 – 9/30/2019 Bridge Letter thru 6/30/2020
Questionnaire for Hosted Solutions		Did not complete. Relied on VITA ECOS publication as an approved vendor. *	Completed
Vendor IT Security Agreements	Security Conformance Agreement	Relied on language included in VITA Contract	Vendor will not sign.
	Interconnection Security Agreement	Not Applicable	Vendor will not sign.
	Confidentiality and Non-Disclosure Agreement	Accepted and signed vendor's document in lieu of VRS Agreement.	Relied on language included in GSA Contract

* To date, VRS has not purchased VITA ECOS services nor has access to VITA's security artifacts, such as assessments or vendor provided third-party assurance reports. The assurances offered through VITA ECOS services do not carry over completely to VRS without added consideration of any identified control gaps, including those which may arise from each SaaS vendor systems' assumed complementary user entity controls. If such details cannot be obtained from VITA, VRS must request this information directly from the vendor for review and assessment.

Complementary User Entity Controls are controls that the **vendor** has **included** within its system and **rely** on the user entity (**VRS**) **to implement** in order **to achieve** the vendor's **control objectives**.

The selected procurement vehicles impacted VRS' ability to obtain executed VRS vendor IT security agreements and security artifacts to complete all elements of the VRS Cloud Vendor Security Review.

Collectively, these conditions impaired the effectiveness of the risk management activities for these vendors. Opportunities to enhance these processes and how they are used to support VRS' vendor risk management activities are discussed in further detail within the Recommendations section of this report.

Other IT Approvals

All purchase requisitions and supporting documentation, as applicable, processed for the vendors during calendar year 2020 included required approvals from the IT department.

IT SYSTEM AND DATA CLASSIFICATIONS AND RELATED RISK ASSESSMENTS

IT System and Data Classifications

The IT System and Data Sensitivity Classifications were completed for all systems reviewed and evaluated with respect to confidentiality, integrity and availability.

Risk Assessments

Risk assessments were not available for the in-scope hosted systems. Upon discussion, IT Security agreed risk assessments should be performed for all hosted systems classified as sensitive and noted they will be included as part of the 2021 risk assessment cycle, scheduled for completion by December 31, 2021.

VENDOR RISK MANAGEMENT

Contract Administration Responsibilities

VRS defines responsibilities for assigned contract administrators in the VRS Technology Procurement Policy and VRS Purchasing Procedures. We reviewed these duties in relation to the activities performed by the contract administrators of the four hosted systems reviewed. Overall, assigned contract administrators were not fully aware of certain contract administration responsibilities intended to support IT security vendor risk management. For the four hosted systems reviewed, VRS provided limited evidence of vendor performance monitoring activities and no evidence of submission of vendor performance reports to the Procurement department.

This is discussed in further detail within the Recommendations section of this report.

IT Related Responsibilities

All in-scope systems were included in the VRS vendor tracking spreadsheet as required by the VRS Vendor Security Agreement Review Procedures. However, the spreadsheet did not capture the completion of annual reviews during calendar year 2020 for these systems. Upon investigation, we found the following related to the annual reviews:

- One system reviewed was newly procured during the year and not subject to annual review.
- One system had a security review performed, initiated in response to a procurement request submitted for the rollout of new features; and,
- For the remaining two systems which pre-dated the implementation of the VITA Information Security Standard for Hosted Environments, certain artifacts were available, but there was no evidence that the required annual reviews were completed. Further, the Questionnaire for Hosted Solutions was not available for either system; however, VRS noted they relied on VITA ECOS approval for one system.

  In addition, it was noted one of these two systems has a longstanding relationship with VRS, initiated through a cloud subscription agreement, which has since expired. VRS has continued the relationship, procuring the same system through small dollar purchasing procedures. This procurement has not been resubmitted for security review and VRS is relying on the confidentiality language included within the original cloud subscription agreement instead of executing a new VRS confidentiality and non-disclosure agreement. This language has not been updated since the original agreement period.

Consequently, VRS has not met certain requirements surrounding continued assessment of the contracted vendors in-scope to this audit as elaborated in the Recommendations section below.

Annual Review of Third-Party Assurance Reports

For the two systems for which an annual review was not performed as noted above, third-party assurance reports were not received during calendar year 2020. Therefore, IT was unable to perform a timely review of the reports for these systems. VRS noted they relied on VITA ECOS approval in lieu of the third-party assurance report for one system.

Overall, the availability of documentation of IT Security's review of significant elements within third-party assurance reports was inconsistent, including the identification of control deficiencies and gaps with the VITA Information Security Standard for Hosted Environments. Furthermore, there was limited evidence of the consideration of significant report elements and their impact, including complementary user entity controls and their relationship to VRS controls.

Finally, evidence of contract administrator participation in the request and review of these reports was not available. Opportunities to enhance the request, receipt and review process for third-party assurance reports are discussed in further detail within the Recommendations section of this report.

FOLLOW-UP ON PRIOR REPORTS

There were no outstanding audit recommendations to consider.

RECOMMENDATIONS

We offer three recommendations as a result of our review, none of which are considered material issues.

Update Policies and Procedures and Promote Organizational Awareness

Multiple documents define VRS' IT procurement, contract administration and vendor risk management processes and responsibilities. Depending on the nature of the purchase and procurement method, one or more of these documents may be applicable and needed to effectively manage the procurement and administration of the resulting contract and vendor relationship. They include the following:

REPORTABLE CONDITION

Any observation included in the **Recommendations** section of the report is considered a "**Reportable Condition**." The **resolution** of a "Reportable Condition" merits **monitoring** in the Audit Recommendation Follow-Up System (**ARFUS**).

MATERIAL ISSUE

Certain recommendations may address a matter that poses such **significant risk** to VRS whereby **immediate measures** should be taken to mitigate the exposure. Other **long-term solutions** may also be appropriate for the permanent resolution of the matter. These recommendations are considered a "**Material Issue**."

All recommendations require a formal response from management.

- The VRS Purchasing Procedures describe all procurement methods and associated requirements including the purchase requisition process and contract administration.
- The VRS Technology Procurement Policy defines the requirements for all technology related acquisitions and responsibilities of purchasers and contract administrators.
- The VRS Technology Procurement Procedures and Technology Purchase Request How-To Guide provide instructions on how to submit a procurement request for an IT good or service and provide an overview of the workflow.

While accessible by all VRS staff, these policy and procedural documents are not cross-referenced to one another and are located in different online locations. The lack of integration of the policy, procedures and guides related to procurement and contract administration responsibilities for IT goods and services potentially weakens VRS employees' ability to consistently adhere to the accepted and expected organizational processes and perform assigned tasks. Additionally, this may result in inefficiencies in completing the procurement and contract administration processes.

For example, untimely acquisition of third-party assurance reports decreases the value of information contained therein as these reports only provide assurance for the specified period. Further, contract administrators did not consistently demonstrate familiarity with the referenced policy or procedures, especially relative to certain components of the contract administration responsibilities included therein. Additionally, VRS policy required quarterly performance reports for the in-scope hosted system vendors were not available for review, potentially making VRS susceptible to risks introduced by its vendors.

Management has recently implemented a new internal workflow to enhance the management of the procurement process for IT goods and services. Additionally, management is evaluating additional tools to assist with recurring vendor risk management activities. Interrelated to both, in July 2021 a new general ledger system was deployed, which is leading to modifications of the purchase requisition process. Further, an organizational working group is in the process of revising VRS' record management practices.

These changes and initiatives provide an apt time for management to re-evaluate all VRS procurement policies and procedures, consider ways to enhance how their requirements are communicated to employees and update related retention and disposition schedules to support records management.

While this review focused on IT-related purchases, the Procurement and IT departments should work collaboratively with other key business units, such as Policy, Planning and Compliance, Finance and Investments, to holistically evaluate and revise VRS' procurement policies and procedures to ensure they are reflective of the recently refined business practices and requirements and encompass both IT and non-IT procurement needs. Such policies and procedures should clearly define individual responsibilities throughout the entire vendor relationship life cycle and necessary interdepartmental communications.

Lastly, once these updates are completed, the Procurement and IT departments may wish to consider working together to create educational opportunities or other tools for employees who may initiate purchases to learn about VRS procurement processes and as applicable, for contract administrators and other responsible parties to gain an understanding of their ongoing responsibilities as part of VRS' vendor risk management practices.

Enhance Risk Monitoring of Hosted System Vendors

Third-party assurance reports were not received or reviewed during calendar year 2020 for two of the in-scope systems. In addition, VRS did not have the Questionnaire for Hosted Solutions for two systems.

To date, VRS has not purchased VITA ECOS services, yet relied on VITA ECOS approval in lieu of receiving and reviewing the third-party assurance report for one system as well as the Questionnaire for Hosted Solutions for two systems. Review of these documents by VRS when there are identified control gaps or defined complementary user entity controls is necessary to fully consider the risks introduced by the vendor relationship into the VRS environment.

Further, documentation of IT Security's review of significant elements within third-party assurance reports was limited, including:

- identification of control deficiencies and gaps with the VITA Information Security Standard for Hosted Environments and
- consideration of significant SOC report elements, including complementary user entity controls and their relationship to VRS controls, by IT Security and the assigned contract administrators. A vendor's desired control environment may be

impaired without VRS' employment of the IT driven and non-IT driven complementary user entity controls identified in the SOC report or appropriate alternative control mechanisms.

Compliance with the VRS Cloud Services Information Security Standard is required to be verified through an initial and an annual security review of the environment or a review of their annual audit report of the environment conducted by an independent, third-party audit firm. VRS' Technology Procurement Procedure Document and Vendor Security Agreement Review Procedures stipulate the initial and annual review of these documents. Collectively, certain incidents of non-compliance noted in the above referenced items potentially could increase the risk of compromise of the confidentiality, integrity and availability of VRS data and services as VRS activities indicated adherence to some, but not all, vendor review requirements defined by its accepted standard and procedures.

The IT and Procurement departments may wish to consider collaborating with key business areas across the organization using hosted systems to develop a more holistic approach to requesting, receiving, reviewing and responding to third-party assurance reports for IT vendors consistently. Contract administrators should be involved in the review of SOC reports for VRS to fully consider complementary user entity controls that are non-IT in nature. Monitoring practices should be incorporated for the annual review processes to ensure their timely completion. This collaboration will create a mutual understanding among the IT department, Procurement department and assigned contract administrators of the role each serves in organizational vendor risk management and offer standard guidance on reviewing significant elements of the third-party assurance reports. Management could also develop a clear responsibility matrix for such responsibilities to capture and communicate this information.

As of the report date, VRS has not purchased these services, but is in the process of evaluating the security review process to determine the level of reliance to place on VITA's ECOS service offering. VRS has contacted VITA to begin the process of acquiring a VITA service catalog account to enable ordering ECOS for specific services.

Additionally, VRS should assess the reasonableness of its reliance on VITA ECOS approvals without purchasing the associated services. While the inclusion of the vendor and its SaaS product on the Approved Supplier Application List gives limited assurance that VITA has assessed the vendor's compliance with VITA's hosted system requirements, it does not give VRS access to the security artifacts supporting this assessment and therefore impacts VRS' ability to consider any expected complementary user entity controls or control gaps which may need to be mitigated. VRS may gain value by purchasing initial assessment and ongoing monitoring services from VITA ECOS if the purchase will give it access to a vendor's security artifacts, including third-party assurance reports and VITA's Questionnaire for Hosted Solutions, which are needed to assess the vendor's controls and assumed user entity complementary controls relative to VRS' environment. Where VRS assesses ECOS services to be insufficient for its needs, VRS should obtain the required security artifacts directly from the vendor to ensure its comprehensive consideration of vendor risks within the VRS environment. If these security artifacts cannot be obtained from any source, then VRS should consider the ongoing viability of the vendor relationship given its impaired ability to fully assess the potential risks introduced by the vendor relationship.

Evaluate Vendor Risk Management Considerations in the Procurement Process

VRS used different procurement vehicles to obtain each of the four hosted systems reviewed. While reasonable and valid procurement choices, potentially unmitigated risks related to three of these procurements and ongoing relationships were noted. Specifically,

- Two of the hosted systems were procured by leveraging an existing contract (GSA, VITA). VRS did not or could not obtain fully executed versions of certain VRS Vendor IT Security agreements from one vendor. For certain agreements, VRS noted they relied on the language within the VITA or GSA contract, which may be reasonable, however VRS' current policies and procedures are silent regarding the acceptability of such departure from the requirements to obtain the applicable VRS Vendor IT Security agreements.
- One hosted system vendor relationship was initiated through a cloud subscription agreement, with appropriate confidentiality and non-disclosure language included at execution. The original agreement has since expired. However, VRS elected to continue this service and vendor relationship using small dollar purchasing guidance. When VRS shifted procurement methods, VRS continued to rely on the original confidentiality and non-disclosure language; however, evidence of an assessment of the viability of such reliance was not available.

The applicable VRS Vendor IT Security agreements are defined in the Technology Procurement Procedure Document and the Vendor Security Agreement Review Procedures. When supplemental agreements (or additional contractual language) are not executed, VRS' ability to enforce its desired terms may be impaired. While alternative avenues for protection may exist, they may not have the same strength as VRS having its own agreement(s). Further, changes in the procurement method over the life of a vendor relationship may impact the legal validity of agreements executed earlier in the relationship under a different procurement method.

When completing the updates to VRS’ policies and procedures VRS should consider also addressing alternative avenues for protection regarding interconnectivity, security conformance, and confidentiality and non-disclosure which are currently collectively addressed through the VRS Vendor IT Security agreements. As part of the initial procurement decisioning, VRS may wish to develop a collaborative process leveraging its IT, Procurement and Legal departments to evaluate the cost and benefit of available procurement methods relative to the inherent vendor risk management considerations of each method. Such a process should consider VRS’ ability to obtain desired terms relative to its IT security expectations under the selected method and determine appropriate compensating controls where traditional vehicles such as VRS Vendor IT Security agreements or contract language may not be feasible. Further, the IT, Procurement and Legal departments should assess the need to develop a process for reviewing and responding to the impact of changes to the procurement method over the life of a vendor relationship on existing contractual and agreement terms.

MANAGEMENT EXIT CONFERENCE

This report was distributed to Ms. Bishop and other members of VRS' management and staff for review and comment. They expressed substantial agreement with this report and will issue a written response to the recommendations contained in this report.

REPORT DISTRIBUTION

Submitted to the Audit and Compliance Committee at its meeting held September 13, 2021.

MEMBERS OF THE AUDIT AND COMPLIANCE COMMITTEE

Joseph W. Montgomery, Committee Chair
W. Brett Hayes, Committee Vice Chair
O'Kelly E. McWilliams, III, Board Chair

WITH COPIES TO:

OTHER MEMBERS OF THE BOARD OF TRUSTEES

J. Brandon Bell, II
John M. Bennett
Michael P. Disharoon
William A. Garrett
Susan T. Gooden
Troilen G. Seward

VRS EXECUTIVE LEADERSHIP

Patricia S. Bishop
Ronald D. Schmitz
Members of the Director's Executive Committee

AUDITOR OF PUBLIC ACCOUNTS

Staci Henshaw

JLARC

Kimberly A. Sarte
Jamie Bitz

PRINCIPAL AUDITOR IN-CHARGE

Kristy M. Scott, CPA, CISA, CIA

AUDIT SUPERVISOR

Matthew Priestas, CIA, CRMA, CISA, PMP

Virginia Retirement System

To: Jennifer P. Bell Schreck, Internal Audit Director

From: Patricia S. Bishop, Director

Date: September 8, 2021

Subject: Management's Response to Internal Audit Report No. 439 – "Vendor Hosted Systems in Administrative Operations"

We reviewed the above captioned Internal Audit Report on "Vendor Hosted Systems in Administrative Operations." We appreciate the Internal Auditor's thorough review of the agency's hosted systems and associated risk management processes for vendors. We also appreciate the professionalism and cooperation exhibited by internal audit staff throughout the audit process.

While there were no material findings, the Audit Report provided three recommendations for follow up. Below are the recommendations and management's response.

Update Policies and Procedures and Promote Organizational Awareness.

Multiple documents define VRS' IT procurement, contract administration and vendor risk management processes and responsibilities. Depending on the nature of the purchase and procurement method, one or more of these documents may be applicable and needed to effectively manage the procurement and administration of the resulting contract and vendor relationship. They include the following:

- The VRS Purchasing Procedures describe all procurement methods and associated requirements including the purchase requisition process and contract administration.
- The VRS Technology Procurement Policy defines the requirements for all technology related acquisitions and responsibilities of purchasers and contract administrators.
- The VRS Technology Procurement Procedures and Technology Purchase Request How-To Guide provide instructions on how to submit a procurement request for an IT good or service and provide an overview of the workflow.

While accessible by all VRS staff, these policy and procedural documents are not cross-referenced to one another and located in different online locations. The lack of integration of the policy, procedures and guides related to procurement and contract administration responsibilities for IT goods and services potentially weakens VRS employees' ability to consistently adhere to the accepted and expected organizational processes and perform assigned tasks. Additionally, this may result in inefficiencies in completing the procurement and contract administration processes.

For example, untimely acquisition of third-party assurance reports decreases the value of information contained therein as these reports only provide assurance for the specified period. Further, contract administrators did not consistently demonstrate familiarity with the referenced policy or procedures, especially relative to certain components of the contract administration responsibilities included therein. Additionally, VRS policy required quarterly performance reports for the in-scope hosted system vendors were not available for review, potentially making VRS susceptible to risks introduced by its vendors.

Management has recently implemented a new internal workflow to enhance the management of the procurement process for IT goods and services. Additionally, management is evaluating additional tools to assist with recurring vendor risk management activities. Interrelated to both, in July 2021 a new general ledger system was deployed, which is leading to modifications of the purchase requisition process. Further, an organizational working group is in the process of revising VRS' record management practices.

While this review focused on IT-related purchases, the Procurement and IT departments should work collaboratively with other key business units, such as Policy, Planning and Compliance, Finance and Investments, to holistically evaluate and revise VRS' procurement policies and procedures to ensure they are reflective of the recently refined business practices and requirements and encompass both IT and non-IT procurement needs. Such policies and procedures should clearly define individual responsibilities throughout the entire vendor relationship life cycle and necessary interdepartmental communications.

Lastly, once these updates are completed, the Procurement and IT departments may wish to consider working together to create educational opportunities or other tools for employees who may initiate purchases to learn about VRS procurement processes and as applicable, for contract administrators and other responsible parties to gain an understanding of their ongoing responsibilities as part of VRS' vendor risk management practices.

Management's Response:

VRS has a comprehensive IT procurement program that has well defined policies and procedures. IT procurement functions are a critical component of agency operations due to the rapid evolution of technology consumed by the agency to carry out its mission. With the recent surge in supply chain security breaches, notably starting with SolarWinds, IT procurement disciplines have been an increasing security focus. VRS Technology Security

Operations has been taking proactive steps over the past eight months to further improve the IT procurement program, including the following:

- Technology Security Operations recognized that the current SharePoint processes and office tools that were being utilized to support IT procurement functioned well but were not an optimized supply chain acquisition technology solution. Requirements were defined, multiple vendors were researched throughout Spring 2021, and a new Governance, Risk, and Compliance (GRC) tool that incorporates a vendor management module was acquired that will allow the agency to track compliance-related factors more effectively for vendors and service providers. This new tool provides the capability for in-depth questionnaires, supplemental document and artifact tracking, and compliance notifications to ensure that contract administrators or business owners are notified for compliance actions, such as annual security review requirements.

- The IT procurement workflow was refined in February 2021 to incorporate checkpoints that will prevent a procurement from moving forward without all required documentation. This is a continuous improvement effort where refinements will be made based on current best practices.

- Technology Security Operations continues to review and update all policies and procedures for IT procurement to ensure they continue to maintain compliance with Commonwealth Security Standards and industry best practices.

- In conjunction with the agency's procurement unit, Technology Security Operations is preparing to work with the VRS training department to strengthen current training related to procurement security and develop new role-based training for contract administrators.

- VRS is coordinating with VITA to establish the required accounts necessary to procure VITA ECOS services. Enrolling services in VITA ECOS will afford VRS efficiency in the oversight of those third-party services by leveraging the existing VITA governance processes.

- A new resource in the Policy, Planning and Compliance team is devoted to contract review.

It is important to note that the observations included in this recommendation, apart from the noted lack of quarterly vendor performance reviews required by VRS policy, are not defined requirements in VRS policy or Commonwealth Security Standards. VRS continues to improve the IT procurement process since early 2020 and has made significant strides in proactively addressing the observations noted in this report. VRS plans to address any backlog

associated with vendor quarterly reporting in calendar year 2022 through the above noted process improvement activities and the new GRC tool.

Enhance Risk Monitoring of Hosted System Vendors.

Third-party assurance reports were not received or reviewed during calendar year 2020 for two of the in-scope systems. In addition, VRS did not have the Questionnaire for Hosted Solutions for two systems.

To date, VRS has not purchased VITA ECOS services, yet relied on VITA ECOS approval in lieu of receiving and reviewing the third-party assurance report for one system as well as the Questionnaire for Hosted Solutions for two systems. Review of these documents by VRS when there are identified control gaps or defined complementary user entity controls is necessary to fully consider the risks introduced by the vendor relationship into the VRS environment.

Further, documentation of IT Security's review of significant elements within third-party assurance reports was limited, including:

- Identification of control deficiencies and gaps with the VITA Information Security Standard for Hosted Environments.

- Consideration of significant SOC report elements, including complementary user entity controls and their relationship to VRS controls, by IT Security and the assigned contract administrators. A vendor's desired control environment may be impaired without VRS' employment of the IT driven and non-IT driven complementary user entity controls identified in the SOC report or appropriate alternative control mechanisms.

Compliance with the VRS Cloud Services Information Security Standard is required to be verified through an initial and an annual security review of the environment or a review their annual audit report of the environment conducted by an independent, third-party audit firm. VRS' Technology Procurement Procedure Document and Vendor Security Agreement Review Procedures stipulate the initial and annual review of these documents. Collectively, certain incidents of non-compliance noted in the above referenced items potentially could increase the risk of compromise of the confidentiality, integrity and availability of VRS data and services as VRS activities indicated adherence to some, but not all, vendor review requirements defined by its accepted standard and procedures.

The IT and Procurement departments may wish to consider collaborating with key business areas across the organization using hosted systems to develop a more holistic approach to requesting, receiving, reviewing and responding to third-party assurance reports for IT vendors consistently. Contract administrators should be involved in the review of SOC reports for VRS to fully consider complementary user entity controls that are non-IT in nature. Monitoring practices should be incorporated for the annual review processes to ensure their timely completion. This collaboration will create a mutual understanding among the IT department, Procurement department and assigned contract administrators of the role each serves in organizational vendor risk management and offer standard guidance on reviewing significant elements of the third-party assurance reports. Management could also develop a clear responsibility matrix for such responsibilities to capture and communicate this information.

Additionally, VRS should assess the reasonableness of its reliance on VITA ECOS approvals without purchasing the associated services. While the inclusion of the vendor and its SaaS product on the Approved Supplier Application List gives limited assurance that VITA has assessed the vendor's compliance with VITA's hosted system requirements, it does not give VRS access to the security artifacts supporting this assessment and therefore impacts VRS ability to consider any expected complementary user entity controls or control gaps which may need to be mitigated. VRS may gain value by purchasing initial assessment and ongoing monitoring services from VITA ECOS if the purchase will give it access to a vendor's security artifacts, including third-party assurance reports and VITA's Questionnaire for Hosted Solutions, which are needed to assess the vendor's controls and assumed user entity complementary controls relative to VRS' environment. Where VRS assesses ECOS services to be insufficient for its needs, VRS should obtain the required security artifacts directly from the vendor to ensure its comprehensive consideration of vendor risks within the VRS environment. If these security artifacts cannot be obtained from any source, then VRS should consider the ongoing viability of the vendor relationship given its impaired ability to fully assess the potential risks introduced by the vendor relationship.

Management's Response:

The VRS IT procurement processes currently account for the requirements defined in both the VRS Cloud Services Information Security Standard and the VRS IT Procurement Policy. The VRS IT Procurement Policy, effective 7/23/2018, requires that purchasers and contract administrators, with assistance from VRS Procurement and Technology Security, ensure "that the vendor and contract continue to meet the security-related performance requirements specified in the initial approval and incorporated in the contract". This includes the documentation and artifacts that validate the continued conformance of the vendor with Commonwealth Security Standards. In addition, the VRS Cloud Services Information Security Standard aligns in whole with the Commonwealth's Hosted Environment Information Security Standard, SEC 525.

To further enhance and improve on the existing program, VRS Technology Security began process improvement actions in 2020 to enhance IT procurement processes and procedures to better ensure compliance with the aforementioned requirements. The improvement actions include the following:

- **Technology Security Operations researched and acquired a new Governance, Risk and Compliance (GRC) tool that incorporates a vendor management module that will allow VRS to effectively track compliance-related factors for vendors and service providers.**

This tool was requested through the procurement process in March 2021 and finalized in July 2021. Prior to this tool, VRS was reliant on SharePoint and Excel spreadsheets for tracking activities. This new tool provides the capability for in-depth questionnaires, supplemental document and artifact tracking, and compliance notifications to ensure that contract administrators or business owners are notified for compliance actions, such as annual security review requirements.

- **The IT procurement workflow was refined in February 2021 to incorporate checkpoints that will prevent a procurement from moving forward without all required documentation. This is a continuous improvement effort where refinements will be made based on current best practices.**

- **Technology Security Operations continues to review and update all policies and procedures for IT procurement to ensure they continue to maintain compliance with Commonwealth Security Standards and industry best practices.**

- **In conjunction with the agency's procurement unit, Technology Security Operations is preparing to work with the VRS training department to strengthen current training related to procurement security and develop new role-based training for contract administrators.**

- **VRS is coordinating with VITA to establish the required accounts necessary to procure VITA ECOS services. Enrolling services in VITA ECOS will afford VRS efficiency in the oversight of those third-party services by leveraging the existing VITA governance processes.**

It is important to note that the observations included in this recommendation, apart from the two systems missing third-party assurance reports and annual security reviews for 2020, are not defined requirements in VRS policy or Commonwealth Security Standards. Additionally, it is important to note that both systems were procured prior to the implementation of the VITA Information Security Standard for Hosted Environments. Work to improve the IT procurement process has been in progress since 2020 and we have made significant strides in proactively addressing the observations noted in this report. VRS plans to address any backlog associated with hosted system risk monitoring in calendar year 2022 through the above noted process improvement activities and the new GRC tool. All third-party audit reports will be updated in accordance with VRS policy as part of this initiative and tracked through the new GRC tool.

<u>Evaluate Vendor Risk Management Considerations in the Procurement Process.</u>

VRS used different procurement vehicles to obtain each of the four hosted systems reviewed. While reasonable and valid procurement choices, potentially unmitigated risks related to three of these procurements and ongoing relationships were noted. Specifically,

- Two of the hosted systems were procured by leveraging an existing contract (GSA, VITA). VRS did not or could not obtain fully executed versions of certain VRS Vendor IT Security agreements from one vendor. For certain agreements, VRS noted they relied on the language within the VITA or GSA contract, which may be reasonable, however VRS' current policies and procedures are silent regarding the acceptability of such departure from the requirements to obtain the applicable VRS Vendor IT Security agreements.

- One hosted system vendor relationship was initiated through a cloud subscription agreement, with appropriate confidentiality and non-disclosure language included at execution. The original agreement has since expired. However, VRS elected to continue this service and vendor relationship using small dollar purchasing guidance. When VRS shifted procurement methods, VRS continued to rely on the original confidentiality and non-disclosure language; however, evidence of an assessment of the viability of such reliance was not available.

The applicable VRS Vendor IT Security agreements are defined in the Technology Procurement Policy Procedures and the Vendor Security Agreement Review Procedures. When supplemental agreements (or additional contractual language) are not executed, VRS' ability to enforce its desired terms may be impaired. While alternative avenues for protection may exist, they may not have the same strength as VRS having its own agreement(s). Further, changes in the procurement method over the life of a vendor relationship may impact the legal validity of agreements executed earlier in the relationship under a different procurement method.

When completing the updates to VRS' policies and procedures VRS should consider also addressing alternative avenues for protection regarding interconnectivity, security conformance, and confidentiality and non-disclosure which are currently collectively addressed through the VRS Vendor IT Security agreements. As part of the initial procurement decisioning, VRS may wish to develop a collaborative process leveraging its IT, Procurement and Legal departments to evaluate the cost and benefit of available procurement methods relative to the inherent vendor risk management considerations of each method. Such a process should consider VRS' ability to obtain desired terms relative to its IT security expectations under the selected method and determine appropriate compensating controls where traditional vehicles such as VRS Vendor IT Security agreements or contract language may not be feasible. Further, the IT, Procurement and Legal departments should assess the need to develop a process for reviewing and responding to the impact of changes to the procurement method over the life of a vendor relationship on existing contractual and agreement terms

Management's Response:

As noted in the recommendation, VRS leverages authorized procurement vehicles to acquire the services in the scope period related to this report. Technology Security will work with the Procurement and Policy, Planning and Compliance departments to assess the best methods to incorporate standardized compliance language in future procurement agreements.

Inclusion of standardized language, such as that found in the VITA cloud terms, will help ensure that VRS vendors and suppliers are held to the same standards and contractual obligations for security compliance.

It is important to note that the observations included in this recommendation are not defined requirements in VRS policy or Commonwealth Security Standards. Work to improve the IT procurement process has been in progress since 2020 and we have made significant strides in proactively addressing the observations noted in this report.

Technology Security thanks the Internal Audit team for their recommendations for process improvement and will take them into consideration where those improvement activities are not already in progress.

Virginia
Retirement
System

INTERNAL AUDIT

Report No. 440

Application Controls: VNAV and Enterprise Content Management Systems

As of January 1, 2021

Highlighting VRS Core Values: *Integrity*, *Teamwork*, *Accountability and Agility* in Action

THIS REPORT IS INTENDED SOLELY FOR THE USE OF THE VRS BOARD OF TRUSTEES AND THE MANAGEMENT OF VRS AND IS NOT INTENDED FOR OTHER PURPOSES.

TABLE OF CONTENTS

Virginia
Retirement
System

TRANSMITTAL LETTER

August 6, 2021

Dear Members of the Audit and Compliance Committee,

We have completed audit number 440, “Application Controls: VNAV and Enterprise Content Management Systems.” The main purpose of our audit was to review the controls in place to protect the confidentiality, integrity and availability of VNAV, the Employer Portal and Enterprise Content Management applications’ inputs, processing and outputs.

We conducted our audit in accordance with the *International Standards for the Professional Practice of Internal Auditing*. These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the conclusions based upon our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report was distributed to the VRS Director and members of management for review and comment. As our review did not result in a written recommendation, management did not provide a written response but expressed substantial agreement with our report.

We appreciate the cooperation and assistance of the Information Technology Department throughout this audit.

Respectfully Submitted,

Jennifer P. Bell Schreck

Jennifer P. Bell Schreck, CPA, CISA, PMP
Audit Director

EXECUTIVE SUMMARY

We conducted an examination of the application controls within VRS' VNAV and Enterprise Content Management (ECM) systems as of January 1, 2021. Our review determined:

- Data or files entering into VNAV and ECM are accurate, authorized and stored completely;
- Data or files are processed as intended in VNAV and ECM, in an acceptable time period;
- Outputs, including interface files, are accurate, authorized and complete and protected from disclosure;
- Records are maintained to track the process of data from input to storage and to the eventual output and reports;
- Configuration management has been performed appropriately and completely to mitigate risks;
- High-risk transactions are authenticated to ensure transactions are authorized; and,
- Personnel access to VNAV's internal employer portal is restricted based on the principle of least privilege.

Management has established a broad foundation of application controls within the VNAV and ECM systems. Given the breadth of VRS business processes managed through these systems, this examination focused on application controls which had yet to be addressed through other reviews. Further, the general controls supporting these applications were not in scope as they are reviewed in a separate engagement known as the IT Client-Server General Controls Audit (Report No. 425).

Overall, our examination found the application controls examined surrounding the processing of transactions and data maintained within the VNAV and ECM systems at VRS reasonably minimize the risks associated with these systems. Member transactions are validated to provide necessary protections to the VNAV system, associated data and the member. As a result, there are no written recommendations resulting from our review.

APPLICATION CONTROLS SNAPSHOT

Application controls are designed to protect the **confidentiality**, **integrity** and **availability** of data managed within an information system. This review focuses on the application controls present within the VNAV and ECM systems to protect VRS member and employer information and support the associated business processes affecting that data.

For fiscal year 2020, VRS managed member, retiree and beneficiary accounts totaling **727,705** through the VNAV system. For fiscal year 2021, VRS imaged approximately **20,000** documents on average per month.

AUDIT ASSESSMENT

Overall, VNAV and ECM application controls are properly designed and operating correctly. Additionally, Employer Portal logical access was reasonable and follows the principle of least privilege.

Written Recommendations: **0**

BACKGROUND

INTRODUCTION

VRS has built business process-based application controls into its VNAV and Enterprise Content Management (ECM) systems to ensure the data captured satisfies specified criteria in conformance with all relevant business and Commonwealth parameters prior to processing and storage within the systems' databases. These controls significantly affect how VRS successfully achieves its business processes and associated objectives.

This examination applied to the application controls and the environment within VNAV and ECM, including the logical access control management of VNAV's employer portal for internal VRS representatives. However, we also reviewed VRS' additional authentication and validation processes surrounding high-risk transactions, which members and retirees conduct through the myVRS portal and thus could affect the integrity of the VNAV system and associated data.

Application controls provide accountability for meeting VRS business objectives, promoting operational efficiency, ensuring the reliability of financial statements, ensuring compliance with laws and regulations, and reducing the risk of asset loss due to fraud, waste or abuse.

The general controls of these applications and the rest of the IT client-server environment were exempted from this review as they are addressed separately, most recently in the IT Client-Server Audit (Report No. 425). The myVRS portal, which was previously reviewed with VNAV within this report's prior examination, Application Controls: VNAV and myVRS (Report No. 411), was exempt from this review as it will be addressed in a separate upcoming examination.

DATA ENTERING SYSTEMS

VNAV is the source system for the processing of member benefits at VRS. As of January 1, 2021, VNAV generally receives data in three ways:

- Manually input into VNAV directly by VRS or participating employer personnel;
- Automatically migrated into VNAV through an interface with another system; or,
- Manually input indirectly by a VRS member or retiree through the myVRS portal.

MEMBER BENEFITS ADMINISTRATION SYSTEMS

VNAV is VRS' **benefit** administrative **system** which **contains all** member and retiree **data**. This **system manages** and **stores** all associated account **transactions**.

ECM is comprised of **two** distinct **systems** which **work together** to transform **all types** of paper and electronic **documents** or **forms** into **actionable information** along with **storing** them securely. These two systems **communicate** regularly by **interface** transmission.

For each input mechanism, VRS uses various controls to ensure data is accurate, authorized and complete.

Since the commencement of our examination,
VRS has released additional features within the myVRS portal which allow members and retirees to update and input additional data into VNAV.

- Beneficiary Maintenance
- Health Insurance Maintenance
- Online Retirements
- Payment Maintenance
- Survivor Registration

Manual Data Entry into Systems

VRS allows members to submit paper forms to start all business processes, even automated ones. A member can submit paper forms directly to their participating employer or to VRS through the U.S. postal service or by physically dropping the document off at VRS. When submitted, VRS and participating employer personnel must enter data into VNAV on behalf of the member.

VRS provides specific VNAV roles based on employee job duties and responsibilities, which allow authorized personnel to input data. VRS makes certain that one person cannot perform an entire process by separating significant duties within a process into different roles. Essentially this means, if an employee performs one part of a process, another employee or supervisor must approve it prior to the process moving forward.

Participating employer personnel can enter member data from paper forms into VNAV either through ad-hoc or monthly reporting processes in the employer portal.

Paper forms received by VRS are scanned into ECM. When this occurs, VNAV is designed to provide an automated specific path or workflow, allowing business processes to follow an authorized and known review and approval through to completion. This ensures that an employee cannot dictate process flow and prevents processes from being handled in a silo.

SEPARATION OF DUTIES

A basic building block of sustainable **risk management** and **internal controls** for an agency, the principle of **Separation of Duties** is based on the shared responsibilities of a key process that **disperses** the **critical** function(s) of that process to **more than one person** or **department**.

VRS has developed a "**Separation of Duties Guideline**" to ensure duties are **managed** appropriately for **IT systems** along with **manual processes**, as required in the **VRS Security Standard**, section **AC-5**.

Incomplete or "Orphaned" Paper Forms

At times, forms arrive at VRS missing certain information to allow the system to direct the document to the appropriate business workflow. This could be caused by member error or a timing difference of the employer's reporting of the member. VRS manages these "orphaned" documents in two ways.

If the request is missing information required to be matched to an associated member account and there is enough information to respond to the member, then VRS will work with that individual to obtain the proper data. Documents with enough information to be processed, for which VRS has no existing member account, are directed to an exception workflow to allow VNAV and VRS personnel to research and locate the appropriate member process workflow.

Scanned Document Retention

After paper forms are successfully scanned into ECM, VRS batches them for retention in individually tracked storage boxes. VRS is *accountable* for these documents even after scanning and creating the electronic version. These documents are stored securely at VRS until picked up for retention by the Library of Virginia for a period of seven years. Once the retention period ends for a specific box, the Library of Virginia will contact VRS to approve its destruction.

Data Interfaces into VNAV or ECM

VNAV interfaces with internal VRS systems, such as ECM, along with external systems managed by outside agencies and other third-party partners to receive the data necessary to complete VRS business processes. Using interfaces to transfer data between systems provides VRS, participating employers, and its other partners with operational efficiencies by allowing large amounts of data to be entered into the system quickly and reducing redundant data entry into multiple systems. However, strong controls must be in place to ensure the input of accurate, complete and authorized data.

TEAMWORK

VRS worked with each **external partner** to develop an **agreed upon** and tested **interface design** that would allow **both systems** to **communicate** data regularly in both **transmission** directions.

Data Captured through myVRS

Members and retirees can interact with their VRS information directly through the myVRS portal. VRS manages the member-initiated data changes and transaction requests by using various application controls within myVRS and VNAV to ensure that inputted data fits particular parameters.

With the exception of additional authentication over higher risk transactions, the myVRS portal and its controls were specifically exempt from this review and will be studied in a future examination.

SYSTEM OUTPUTS

With respect to outbound transactions, VNAV interfaces internally with ECM. Also, VNAV transfers outbound files with external systems that are owned by other state agencies and third-party administrators. VRS has implemented various controls surrounding the transmissions to ensure the confidentiality, integrity and availability of the data as it is migrated. By implementing these controls, VRS ensures that only authorized data is released from VNAV or ECM.

In addition, when a user is granted access in VNAV and ECM, the user's associated role is limited to specific functions and reports that the user has the ability to initiate, produce and view. Users who are not granted access to certain functions or reports are unable to use or manipulate them. Roles and logical access are discussed further in the Logical Access section.

EXTRA AUTHENTICATION

Two-factor authentication is an **extra** layer of **security** designed to **validate** the **identity** of a **user** who is accessing or **attempting** to process a **material transaction**.

VRS performs this by **distributing** a **code** to the **user** through a **previously** authenticated **method** (phone number or email address).

MEMBER IDENTITY AUTHENTICATION

VRS uses several online authentication processes to ensure the person accessing or making changes within a member's account or initiating transactions on their behalf is authorized to do so.

Account Registration - Identity Authentication

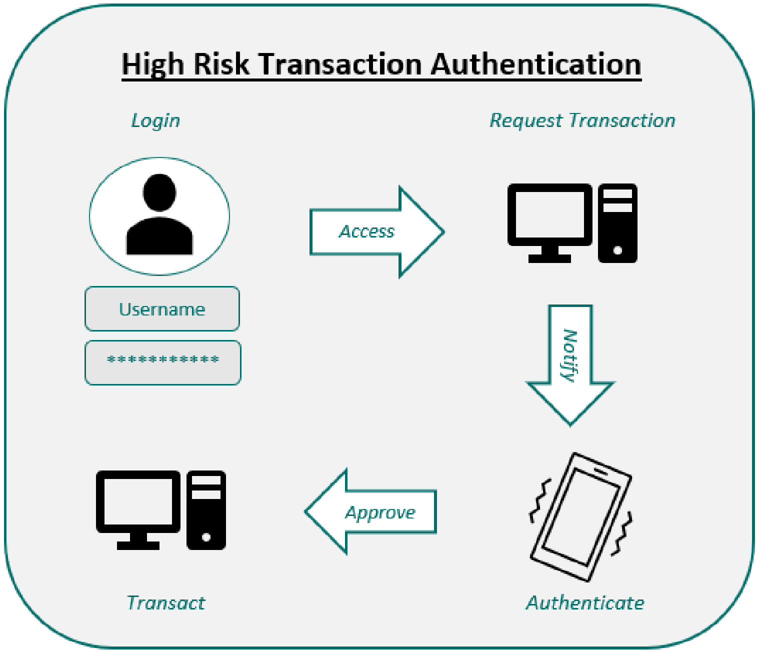
VRS has established a multi-layer risk model during registration to validate and authenticate a member's identity prior to accessing the myVRS member portal. Once their identity is established in myVRS, users must authenticate into their account with their associated username and password.

Higher Risk Transaction – Identity Authentication

For added security, coordinated with the implementation of the myVRS portal in 2016, VRS instituted a two-factor authentication for all higher risk transactions. Once authenticated into myVRS, if a member wishes to perform a transaction deemed higher risk, the user first must verify their identity through an additional authentication process. This is achieved through the provision of a unique one-time authorization code to the member's previously verified communication method, such as a phone number or email address. If the code is provided back to VRS successfully, the user identity is validated and the transaction can proceed.

As of January 1, 2021, the VRS transactions which equated to a higher risk category were identified as tasks related to changing a password, email address, mobile phone number or requesting a refund or Purchase of Prior Service (PPS).

The high-risk authentication process is diagramed below:



Two-factor authentication provides an **extra** layer of **security** to **validate** the **identity** of a **user** who is accessing or **attempting** to initiate a **high-risk transaction**.

VRS performs this by **distributing** a **code** to the **user** through a **previously** authenticated communication **method**.

Recent Authentication Enhancements

In early 2021, outside of our audit period, VRS expanded its authentication process to require the use of this two-factor authentication for all new myVRS account registrations and future log in attempts.

VRS currently offers this enhanced security as an optional choice for previously existing myVRS account holders. VRS plans to eventually transition this to a required security measure in the future.

This enhancement does not eliminate the requirement of authentication of high-risk transactions, but rather strengthens VRS security surrounding members' myVRS accounts and its associated transactions.

LOGICAL ACCESS

VRS manages VNAV and ECM security access through the Resource Access Management System (RAMS). RAMS is a role-based access management system designed to ensure the accurate administration of privileges, since most privileges are automatically assigned based on position and role. The foundation of these assigned roles is the principle of least privilege.

Management of the controls over VRS' user access to the VNAV and ECM systems' interface files as well as VRS' internal access to the VNAV employer portal and its processing applications are essential to protect the confidentiality, reliability and availability of data and application resources. These controls reduce the risk of information being disclosed, misused or destroyed, whether by accidental or intentional means.

As described in **VRS Security Standard** section **AC-6**, the **Principle of Least Privilege** requires **users** have **only** the **minimum access** rights **necessary** to **fulfill** their **responsibilities**.

VNAV and ECM Access

All VNAV and ECM roles are granted based on a business function position, as defined in the VRS position description, rather than based on an individual person. Position descriptions can be assigned one or more roles. Further, roles are not limited to a single position; rather they can be used across multiple positions in various units or departments.

A consistent and regulated approach is used to set roles since access is defined for a position, not an individual, and any approval of a role assignment approves the access for all individuals in the position. Brand new roles, as well as requests requiring a change to the roles set in the position description, must be approved by the VRS Data Owners Committee.

Since personnel logical control access for VNAV and ECM is assigned by position rather than a specific individual, access to these systems will be addressed separately in a future Logical and Physical Access Review.

Internally, VRS supervisors are responsible for ensuring position descriptions clearly identify the business responsibilities and required information system access privileges.

Externally, VRS requires its partners with system access, such as participating employers, to review their personnel's VNAV role assignments annually, making any necessary changes and confirming that access granted is still appropriate.

VNAV Employer Portal Access

Participating Employers

VRS relies on its participating employers to provide key demographic data about active members to support the calculation of their monthly contribution amounts. Employers use the VNAV Employer Portal to input, review and correct the submission of active member data for which they are responsible (e.g., members in covered positions, plan type, member salary and creditable compensation information, etc.). Employers paid approximately $3.0 billion in contributions for the fiscal year 2020 through this portal.

Employer logical control access for the VNAV Employer Portal was specifically exempted from this review and will be addressed separately in the upcoming myVRS examination.

VRS Personnel

VRS personnel also have access to the VNAV Employer Portal in two ways. First, VRS itself is an employer within the Virginia Retirement System. Similar to other participating employers, VRS must provide appropriate data to support the calculations of their monthly contribution amounts. Secondly, since VRS is the system owner of the VNAV Employer Portal and administrator of the pension system, personnel must have access to maintain the portal appropriately and manage the contribution process for all employers. Since these two roles are conflicting, VRS must ensure these duties are segregated appropriately between personnel.

VNAV and ECM Interface File Access

Protection of the information created by the system or received from another system transfer is vital to the integrity of the data and to ensure data cannot be manipulated prior to upload or transfer. VRS limits access to these file locations and interface management capabilities based on the principle of least privilege.

SYSTEMS PROCESSING

System Monitoring

VRS has set performance standards or metrics for certain processes within VNAV and ECM. VRS focuses its metrics on timely and accurate service retirement processing, timeliness of employer contribution confirmations and timeliness of workflow documentation being stored in ECM. Additionally, VRS tracks and monitors outages of these systems and their availability to users.

Further, VRS uses a multi-faceted approach across departments to monitor and alert appropriate personnel of system activity, including interface transmission activity, abnormal termination events or program crashes. This multi-faceted approach includes both automated and manual mechanisms. VRS uses an automated security information and event management tool to consolidate system performance or activity records and send out alerts for significant events or errors. This tool allows VRS to recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. Personnel review these alerts and associated information to investigate and address each occurrence appropriately. For manual monitoring, VRS has established specific and unique processes it performs in specific IT business units to remain cognizant of systems activities.

Finally, VNAV logs a chronological record of activity that provides documentary evidence of the sequence of events during any time, operation, procedure or event within the system in two main ways. These records are also known as audit or business trails. First, VNAV and ECM have internal audit logs tracking events related to a specific record at a high level. Additionally, in real-time, VRS has a separate tracking and logging mechanism external to VNAV and ECM that records all account activity and transactions for review and research, as necessary.

PUBLISHED VNAV & ECM CURRICULUM

VRS has **created** and **maintains** approximately **270** various **training products** to **demonstrate** relevant **processes** to users.

Assessments	Checklists	E-Courses
Job Aids	Process Guides	SharePoint Literature
Webinars	Webiste Literature	Videos

Systems Training

To perform their job duties within a system, users must be provided ample training within the environment. VRS has created and published approximately 270 training products to assist users in performing their job duties and to support system functionality. Management has strived to keep training up to date by establishing an internal standard of having all training products reviewed and updated within three years of being published or when an environmental change affects that product.

VRS has placed relevant trainings for particular job duties within the Virginia Learning Center to allow managers to train personnel prior to the assigned employees actually performing the duties. Additionally, as they work, authorized individuals can access VNAV help screens and internal SharePoint information which will provide necessary system documentation and job aids to assist with decision points, refreshers or clearer definitions to be able to complete a process within VNAV properly.

Application Changes

Periodic Change Management Requests

VRS uses Active Lifecycle Management or ALMs to make necessary changes or address defects within VRS’ systems. These are system or data changes that are necessary to fix an error or correct a unique situation once the system is live. In addition, technology related updates to systems are evaluated and applied on a periodic basis, such as system patches, upgrades to business software and operating system upgrades.

VRS logs all change management requests including, but not limited to, enhancement requests from business users, process re-engineering requests and productivity improvement opportunities. Further, an executable task list, including assignment, resources, time estimates and dependencies is created for each change management request. VRS regularly communicates status updates and reviews for all change management requests to applicable parties throughout the change process and ensures all changes are thoroughly tested prior to release.

An individual independent from the development activities releases new changes into production to safeguard against unauthorized changes being implemented. The production release authority is granted and controlled through the logical access roles previously discussed.

Application Hardening

When a new application, or a new version of an application, is implemented, personnel must review the application’s default configured settings to ensure only approved VRS settings are applied and unneeded functions are removed. To support knowledge transfer and ensure consistent application of settings, VRS creates procedure documents referred to as hardening guides, which allow personnel to configure the specific application to VRS specifications. These guides direct configuration of the application to establish appropriate logging of application activity, ensure the protection of data retained within the application and certify settings align with VRS IT Standards.

Routine Annual Change Requests

Additionally, at the end of the calendar and fiscal years, VRS performs separate but significant projects called the Calendar Year End and Fiscal Year End projects. These projects update any necessary processes, rates, data or functions within the VNAV or myVRS systems to set the foundational elements for various automated business processes within these systems for the upcoming year. While there is considerable commonality, the project tasks and software updates for each period are not identical each year.

Data Security

VRS protects the *integrity* of system data by converting or encrypting the stored or transferred information into a form that is unreadable to an unauthorized user or process. Encrypted data must be converted back to a readable form prior to use. Authorized systems are able to decrypt this data seamlessly through use of an encryption key. Further, VRS ensures data is encrypted when it is transferred to and from one of its business partners or employers to make certain the data is protected during transit. This encryption helps ensure that any information that has been misdirected, intercepted or otherwise improperly obtained will be extremely difficult to compromise.

VRS has instituted supplemental protections for data which during the course of business has been unencrypted and accessed properly by an authorized individual who becomes preoccupied while using the system. Specifically, once logged into a system, if a user steps away and fails to log-out or lock their workstation, a risk exists the system could be accessed by an unauthorized individual. Therefore, VRS configures its systems to prevent further access by initiating a “session lock” after 30 minutes of inactivity or upon receiving a request from a user, as stipulated in the VRS Security Standard section AC-11. As an added protection, VRS workstations also are automated to “screen lock” after 10 minutes of inactivity and require the user to re-authenticate to continue any activity.

VNAV DATA QUALITY MONITORING PRACTICES

Investigating data quality issues can lead to early identification of system design or coding oversights, needed enhancements or business processes that may not be working as anticipated. VRS strives to holistically ensure data within the VNAV system is and continues to be accurate.

To create and mature these processes for VNAV, in 2020, VRS hired a consultant to research existing data quality issues, with an end goal of identifying high-risk issues related to data quality, performing root cause analysis to determine the creation point of those issues and ultimately create a repeatable data quality monitoring process.

From this experience, a data quality dashboard was created and transitioned to VRS for future enhancements.

Data quality programs routinely monitor, maintain and ensure the data quality across a system, helping to lower operational risk, improve decision making and ultimately enhance member experiences and satisfaction.

SCOPE AND METHODOLOGY

The primary purposes of our examination were to determine if:

- Data or files entering into VNAV and ECM are accurate, authorized and stored completely;
- Data or files are processed as intended in VNAV and ECM, in an acceptable time period;
- Outputs are accurate, authorized and complete and protected from disclosure;
- Records are maintained to track the process of data from input to storage and to the eventual output and reports;
- Configuration management has been performed appropriately and completely to mitigate risks;
- High-risk transactions are authenticated to ensure transactions are authorized; and,
- Personnel access to the VNAV Employer Portal is restricted based on the principle of least privilege.

Given the breadth of VRS business processes managed through these systems, this examination focused on application controls not addressed through other examinations as well as those controls that support a significant number of business processes at one time. Additionally, we included a review of VRS personnel's logical access to the interface files and VNAV Employer Portal to ensure access was limited based on the principle of least privilege.

GENERAL ASSESSMENT AND UNDERSTANDING

We obtained a general understanding of the application controls over VNAV and ECM systems as well as the key application controls by reviewing the applicable system risk assessments, policies and procedures; system operational metrics, including system availability; and other relevant documents. We also met with key individuals from each area to discuss relevant processes. Afterwards, we validated application controls were functioning as stated and intended.

SCOPE EXCLUSIONS

VNAV **inbound** or **outbound** interfaces associated with **processes** supporting

- Virginia Sickness and Disability Program
- Virginia Local Disability Program
- Actuarial Data
- Defined Contribution and Cash Match Plans
- Group Life Insurance
- Long-term Care
- Retirement Payroll

were **not** reviewed during this **engagement** as they have been or will be addressed in **separate** examinations.

DATA ENTERING SYSTEMS (INPUTS)

We first gained an understanding of how data is entered or inputted into VNAV and ECM. We then substantiated VRS controlled inputted information to ensure its accuracy, completeness and authorization, no matter the path of input.

Then, within the VNAV system, we reviewed processes in which VRS personnel must input data into the system manually which were not previous reviewed or planned for review in risk-based business process examinations. We corroborated associated manual processes had proper separation of duties, as dictated in the VRS Security Standard section AC-5, and workflow mechanisms were in place to allow data to be input completely and accurately.

We gained an understanding of all systems, either internal or external to VRS, that interfaced with the VNAV or ECM systems to assess whether appropriate controls were in place to migrate only authorized data into VNAV accurately and completely. We determined whether interface transaction data confidentiality was protected with a widely accepted and robust security method. We then analyzed whether VRS was validating the *integrity* of the transfers by ensuring the entire population of transactions was received by the system. Where migrated data was received that could not be processed completely or was considered an exception within the system, we studied how these transactions were logged and reported and then evaluated the process of clearing items for reasonableness.

DATA EXITING SYSTEMS (OUTPUTS)

We first identified the outputs, such as transactions, reports and interface files that are created from the VNAV and ECM systems. Then we determined if outputs produced were accurate, complete and only authorized individuals could create them.

We gained an understanding of all systems, either internal or external, that received such information from VNAV or ECM through an interface or interface files to assess whether appropriate controls were in place to ensure only accurate and authorized data is released or transferred. We validated that proper checks of the data and approvals were given prior to the release of interface files during the audit period.

Finally, we reviewed the process for creating VNAV reports and gained an understanding of the present population of reports within the VNAV reports repository. We ensured proper controls were in place and reports were validated prior to the release for staff use.

MEMBER IDENTITY AUTHENTICATION

We gained an understanding of myVRS higher risk transactions requiring additional authentication and the process surrounding these verifications. We studied the processes and risk associated with these transactions. Then we analyzed the authentication and validation techniques and controls that were present during our audit period. Finally, we explored VRS' future plans surrounding the use or enhancements of this mechanism.

LOGICAL ACCESS

We studied the VRS account management processes for granting, changing and revoking access to VNAV's Employer Portal and interface files for VNAV and ECM. We reviewed the account management policies and procedures around these specific activities for all types of personnel (internal, external and contractors) who receive access to the VNAV Employer Portal or interface files. We evaluated the access of this population of users to determine if it was appropriately given based off the associated job description and principle of least privilege. We assessed these users' access for conflicting roles and proper separation of duties to confirm whether a single person could complete a full task.

Any further testwork surrounding VNAV and ECM logical access and account management processes are exempt from this review and will be evaluated in concert with the newly developed Resource Access Management System (RAMS) under the planned examination entitled "Logical and Physical Access."

Currently, there is **one** recommendation **outstanding** from the **previous report**, Audit Report 411. It pertains to **improving** VNAV's **procedures** for **assigning access** to users and **ensuring** they are accurately **defined** and **in alignment** with management's intended **practice**.

This is **discussed** further in the **Follow up on Prior Reports** section below.

SYSTEMS PROCESSING

System Monitoring

We first determined how the VNAV and ECM systems were intended to function by reviewing relevant design documentation and applicable Agency Operating Standards for VNAV and ECM business processes. We investigated any anomalies in results during the first half of the fiscal

SYSTEM AVAILABILITY FY2021 PERFORMANCE STANDARD

Critical systems are available to users at least **99.5%** of the time.

year 2021 to determine the reason why the systems were not functioning as intended, including any mitigation plans developed by management.

Then we reviewed the systems outage and availability statistics and determined management's process for identifying and addressing abnormal termination of software or program crashes.

Finally, we reviewed management's processes for tracking of transactions and activity within the systems. We determined whether logged activity was retained for a reasonable amount of time and documentation of activity could not be manipulated or deleted.

System Training

We obtained the master list of all training products published for these systems and determined what types of training information or products were provided to VRS personnel and other users of the VNAV and ECM systems to assist them in performing their job duties and support the systems' proper functioning. Then we gained an understanding of management's review and update process used to ensure training products are maintained and continue to be relevant.

Once we understood the sources of training, along with the population that was provided, we reviewed the master list and evaluated the application of these practices to the training products for these systems to ensure that all documentation was being maintained properly, investigating any discrepancies. Finally, we reviewed a sample of training documentation published to evaluate the relevance, completeness and reasonableness of the information.

Application Changes

We assessed VRS processes for updating applicable system information when there is a defect, change in the configuration or calculation of the business process by the General Assembly, VRS Board of Trustees, or other regulatory authority. We determined whether VRS had a set process in place to ensure only authorized changes were implemented and adequately tested prior to release. We also reviewed the systems' hardening guides and most recent hardening process performed to ensure systems have been configured and secured appropriately. Finally, we reviewed the most recent Calendar Year End and Fiscal Year End update projects to confirm that it was occurring, being completed timely, and encompassing all updates required for each year.

Data Security

We obtained VRS' system security plans for VNAV and ECM to understand how VRS is protecting the systems and data retain within the systems. We reviewed VRS' security protocols set within these two systems and assessed whether data was adequately protected at rest and in motion. We also ensured that data transferred to other systems confidentiality was protected during transit. Lastly, we ensured system data is protected to prevent further access to the systems after an identified period of inactivity or upon receiving a request from a user.

VNAV QUALITY MONITORING PRACTICES

Finally, we determined if VRS had created an overall data quality process for VNAV data. We reviewed the scope of these monitoring practices and any future plans to ensure VNAV data continues to be accurate and the system is functioning as intended.

CONCLUSIONS

GENERAL ASSESSMENT AND UNDERSTANDING

Management has designed an effective structure of application controls within the VNAV and ECM systems. Overall, for the elements in-scope to this examination, the application control environment surrounding processing of VNAV and ECM systems at VRS, reasonably minimizes risks associated with business transactions. Proper controls are in place that protect the confidentiality, integrity and availability of business processes as well as members' personal information.

DATA ENTERING SYSTEMS

Overall, data input into VNAV and ECM has sufficient controls in place to support its authorization, accuracy and completeness. Specifically, VRS has placed appropriate application controls within the systems to ensure that data entering into the system is meeting specified requirements and has been authorized by the associated member, retiree or appropriate employer or VRS designated personnel. Management has designed proper separation of duties and appropriate workflows so that no one individual can complete an entire process unaided and personnel must follow VRS approved paths to completion each time.

Further, interface transfers have been designed with appropriate approvals and controls to ensure the *integrity* of data. Management has designed data elements into the transfer process to regulate the specific data able to be transmitted and inputted.

SYSTEM OUTPUT

We reviewed VRS' report repository and process for creation of new reports in VNAV. We found newly created reports are vetted and validated to ensure accuracy and were functioning as intended prior to release.

For interface files produced or output from the VNAV system, we found the proper interface controls to be in place to ensure the *integrity* of the systems. All data released from the system through an outbound interface file is reviewed and authorized for release. Management has designed data elements into the transfer process to regulate the specific data able to be transmitted.

MEMBER IDENTITY AUTHENTICATION

Higher Risk Transaction - Identity Authentication

We found VRS has set forth a strong process for performing an additional validation and authentication process when members attempt to perform transactions which are inherently risky.

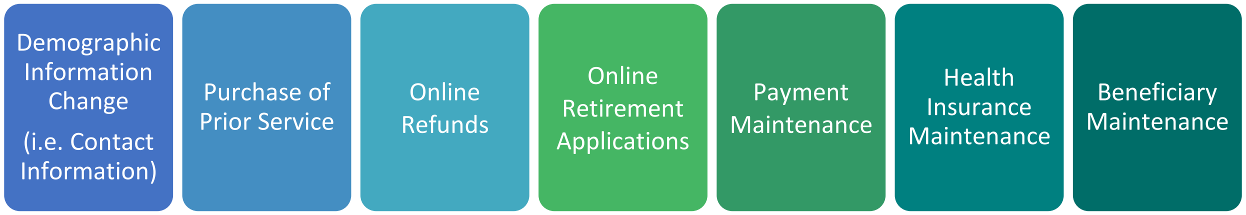
Authentication Enhancements

As previously noted, when VRS initially instituted this required authentication process, these one-time authentication codes were used to support the initiation of higher risk transactions which at the time the authentication code distribution was limited to demographic information changes (e.g., changing a password, email address or mobile phone number), requesting a refund or initiating a PPS.

The one-time authentication codes are distributed to members through SMS, commonly known as a text message, or alternatively through email. At the time of establishment, this distribution process was the most efficient method and made the most sense for the VRS population since members rarely performed these transactions, sometimes once in a lifetime. While widely accepted distribution methods, they introduce risk as the codes transfer in clear-text and are open to potential Subscriber Identification Module (SIM) manipulation. To mitigate these risks, VRS created a Data Analytics Program to monitor access attempts for all members logging into or registering at myVRS.

After our audit period, in early 2021, VRS expanded its authentication process to require the use of two factor authentication for all new myVRS account registrations and future login attempts. Additionally, VRS is now providing this enhanced security as an optional choice for current myVRS account membership, with the planned eventual transition of all members to this required security measure in the future. This enhancement strengthens VRS security surrounding a member’s myVRS account and its transactions.

Further, VRS adjusted its higher risk transactions listing due to the expanded functionality recently released in the final stages of the Modernization Program - Phase Four. Higher risk transactions now include the following:



- Demographic Information Change (i.e. Contact Information)
- Purchase of Prior Service
- Online Refunds
- Online Retirement Applications
- Payment Maintenance
- Health Insurance Maintenance
- Beneficiary Maintenance

VRS’ new and existing online transactional abilities represent leading-edge tools for members and retirees within the domestic public pension retirement industry. Currently, only one other public pension retirement system provides similar online functionality. We commend VRS for its ongoing monitoring and management of these risks as reflected in the expansion of the use of two-factor authentication.

Given the risks of being on the forefront of this transactional online functionality, we encourage management’s continued assessment and implementation of tools which will further enhance member identity validation and one-time use security code distribution. Currently, institutions with sensitive financial accounts already employ alternative robust authentication methods, but they may not be as user friendly for VRS’ member population. We recognize the balance required to provide exceptional customer service and secure authentication. We support management's continued work to mitigate risk and protect members' accounts and their associated benefits.

LOGICAL ACCESS

Logical access was appropriate for individuals authorized to receive access to the VNAV Employer Portal and related member and employer contributions transactions based on job duties, responsibilities and the least privilege principle.

Further, employees' access to interface files and their ability to modify or change interface parameters was protected appropriately and limited.

SYSTEM PROCESSING

System Monitoring

Overall, VRS regularly monitors VNAV and ECM and their associated processes to ensure the systems are working as intended.

Specifically, we found the Imaging department which inputs documents into ECM to be monitoring and using reconciliation techniques to ensure all documents scanned were in fact uploaded and tracked into the system. Additionally, paper documents received were managed appropriately, tracked and securely stored locally and remotely. Systems interface transmissions also were being monitored appropriately to ensure continued availability of the service and transmissions were functioning as intended.

VNAV was monitored appropriately through the VRS consolidated monitoring tool and processes. Additionally, ECM was monitored appropriately within the system; however, as a result of an audit request, management identified that ECM transaction activity was not being transferred and included in VRS' holistic monitoring program. Once identified, management immediately took action to correct the situation and ensured the system activity was transferred to the consolidated tool. Near the end of our engagement, we confirmed that ECM was included in the process and the issue had been corrected.

FY21 OPERATIONAL MEASURES

As of the **audit period**, January 1, 2021, we found that VNAV was available **99.99%** of the time during VRS **business hours**.

ECM workflow **documents** were **imaged** within **one business day** of receipt **100%** of the time.

System Training

The VRS Training Team is comprehensively tracking the training courses and information and job aids available to support all personnel performing VNAV and ECM processes, including the details of major changes and version history.

Our sample of materials reviewed were found to be consistent, complete and covering relevant topics and concepts. We also found training material to be easily located on the VRS website, internal SharePoint documentation, Virginia Learning Center and EKS/VNAV Help.

We commend management's documentation efforts surrounding the maintenance and history of these training products.

Application Changes

We found VRS' processes for updating applicable system information whenever there is a change in the configuration or calculation of the business process to be reasonable. VRS has a process in place to ensure only authorized changes are implemented and adequately tested. Finally, we reviewed the most recent completed Calendar Year End and Fiscal Year End update projects and found that they were occurring regularly, being completed timely and encompassing all updates required for each year.

Data Security

Our review found VRS is adequately protecting the systems and data retained within the systems. Specifically, we determined VRS' security protocols set within these two systems are reasonable and all data is adequately protected at rest and in motion. Interface transmissions were found to be secured with a robust and widely accepted encrypted method. Encryption keys were determined to be protected appropriately to prevent misuse.

We attempted to review the VRS System Security Plans for the VNAV and ECM and found that they had not been fully developed. Certain relevant artifacts of these plans exist in a decentralized form; however, assurance that all elements of these plans were created and available for review could not be provided. Management is currently in the process of executing a System Security Plan Development Project which is included in the Technology Services Roadmap. As part of this project, VRS will ensure system security plans are created for all sensitive systems, including VNAV and ECM.

The coordination of this process with its current infrastructure migration plan from on-premise to the cloud will allow VRS to align its security practices with the new and future environmental context. Once created, we encourage management to ensure these plans are regularly updated to monitor and mitigate the associated risks within the VRS environment and any changes to ensure these plans continue to be available and up to date.

We commend VRS for this tactical and efficient plan to align individual system security plans with the future environment.

Finally, we reviewed VRS systems configuration to prevent further access by unauthorized individuals if they fail to logout of their system account as stipulated in the VRS Security Standard, AC-11, which states that a system lock must occur after 30 minutes of inactivity. We found, in practice, VRS has chosen to be more stringent than their prescribed 30-minute maximum limit.

For ECM, the lock is achieved through the VRS workstation which disables access to the VRS account after 10 minutes of inactivity. The VNAV system is configured to prevent further access to the system by initiating a session lock after 20 minutes of inactivity. Once initiated for either mechanism, the session lock remains in place until the user reestablishes access using their established identification and authentication procedures. Even though the VNAV session lock is set at 20 minutes, this control is strengthened further by the VRS workstations lock at 10 minutes, effectively making both systems' accounts inoperable after 10 minutes of inactivity.

VNAV DATA QUALITY MONITORING PRACTICES

IT management continues to demonstrate *agility* through its development of quality monitoring practices for VNAV by establishing a data quality dashboard and introduction of necessary tools to identify VNAV transactions or ECM processes which are not appropriate or are not functioning as intended in the summer of 2020. IT personnel supplement these tools by working with business area representatives as necessary to identify potential data exception triggers or validate transaction misrepresentations. Due to the hiring freeze during the pandemic and competing operational priorities, VRS paused on its planned refinement of these practices in the fall of 2020. VRS hopes to bring on additional personnel in the near future to continue to mature and solidify them.

We commend VRS for their efforts to improve their quality monitoring processes and encourage VRS' continued efforts in this area as dedicated resources are able to be brought onboard. We also encourage continued empowerment of the key business areas to help drive potential data quality dashboard components.

FOLLOW-UP ON PRIOR REPORTS

In the previous review, Audit Report 411, one opportunity for improvement was identified to review and evaluate VNAV's security access procedures to ensure that the process for assigning access to users is accurately defined and in alignment with management's intended practice.

VRS represented this recommendation as implemented per management's status report within the Quarterly Audit Recommendation Follow-up System (ARFUS) as of December 31, 2020.

> *"All regular, test and domain admin accounts for all Administration and Investment business units were loaded into RAMS. The project team reviewed all privileges associated with regular, test and domain admin accounts, documented privilege descriptions, and obtained role & supervisor approvals for each privilege granted. RAMS enables managers/supervisors to assign only the privileges needed and approved for a given position. In addition, it enables to monitor and take appropriate actions to remove privileges that are no longer appropriate, facilitate period review of assigned privileges, and make necessary updates to reflect changes in job duties. Server admin, desktop admin, and service accounts that represent a small portion of technology related accounts remain to be loaded into RAMS. A process is in place to manage these accounts until they are implemented. We consider the recommendation regarding "Evaluate VNAV's Documented Security Procedures and Ensure Ongoing Monitoring of System Access Occurs" is implemented and closed."*

As is our practice, this recommendation will be reviewed during the fiscal year 2021 Annual Audit Recommendation examination. Once validated, it will be released from the Audit Recommendation Follow-up System (ARFUS). Due to this, this area was exempt from this review.

RECOMMENDATIONS

We have no written recommendations to offer as a result of our review.

MANAGEMENT EXIT CONFERENCE

This report was distributed to Ms. Bishop and other members of VRS' management and staff for review and comment. They expressed substantial agreement with this report.

As there are no written recommendations, a written response from management is not required.

REPORT DISTRIBUTION

Submitted to the Audit and Compliance Committee at its meeting held September 13, 2021.

MEMBERS OF THE AUDIT AND COMPLIANCE COMMITTEE

Joseph W. Montgomery, Committee Chair, Board Vice Chair
W. Brett Hayes, Committee Vice Chair
O'Kelly E. McWilliams, III, Board Chair

WITH COPIES TO:

OTHER MEMBERS OF THE BOARD OF TRUSTEES

J. Brandon Bell, II
John M. Bennett
Michael P. Disharoon
William A. Garrett
Susan T. Gooden
Troilen G. Seward

VRS EXECUTIVE LEADERSHIP

Patricia S. Bishop
Ronald D. Schmitz
Members of the Director's Executive Committee

AUDITOR OF PUBLIC ACCOUNTS

Staci A. Henshaw

JLARC

Kimberly A. Sarte
Jamie Bitz

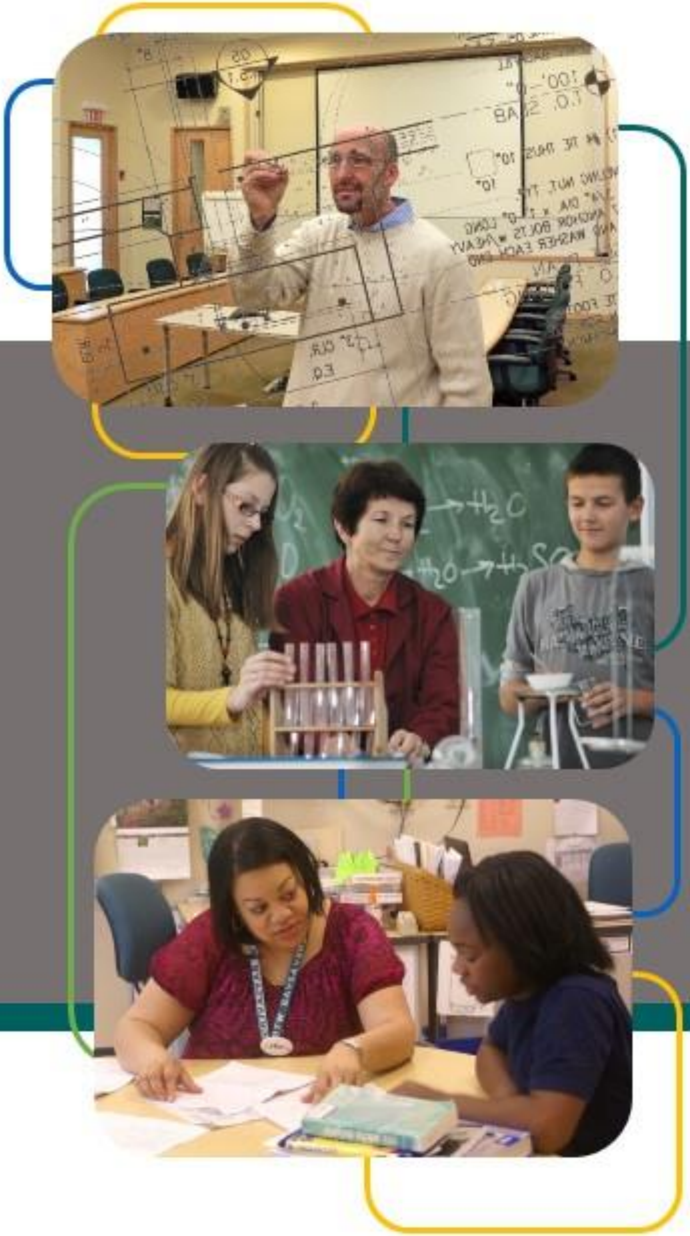
PRINCIPAL AUDITORS

Matthew Priestas, CIA, CRMA, CISA, PMP
Joshua Fox, CIA, CFE, CIDA

Quarterly Reports on the Modernization Program

- Phase 4

Virginia
Retirement
System

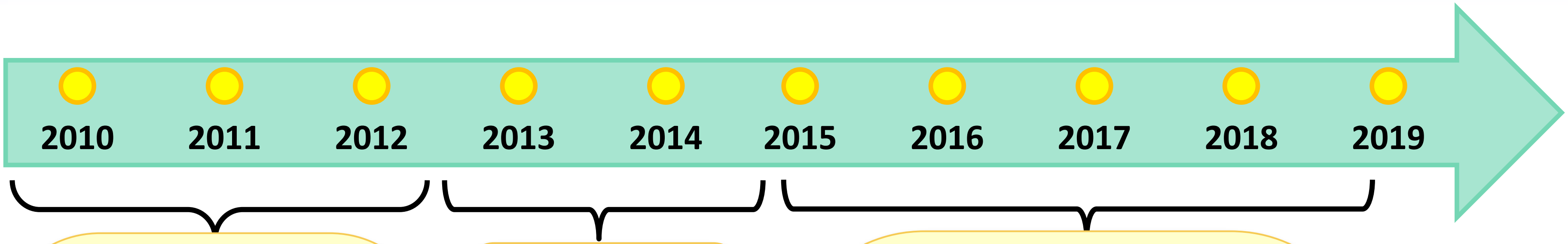


Modernization Phase 4

Audit Committee

September 13, 2021

Modernization



Infrastructure

- Data Center including Infrastructure and Security
- Imaging Solution
- Disaster Recovery Data Center
- Telephony Solution
- Centralized Print

Employer Functionality

- Employer Portal with Online Enrollment, Data Maintenance, Remittance, Contacts Management

Hybrid Plan for VNAV and RIMS

Member and Retiree Functionality

- Refunds Calculation Solution
- Refunds Disbursement Solution
- Member Portal with Enhanced Security and Online Refund Request
- Benefits Calculation Solution
- Online Retirement Planner
- Purchase Prior Service Solution
- PPS Online
- Retiree Portal
- ORPHE Solution
- Online ORPHE/ORPPA
- Online Financial Education
- Retirements/Disbursements Solution

Discontinue Use of Mainframe System (RIMS) 2019

Online Retirement 6/30/21

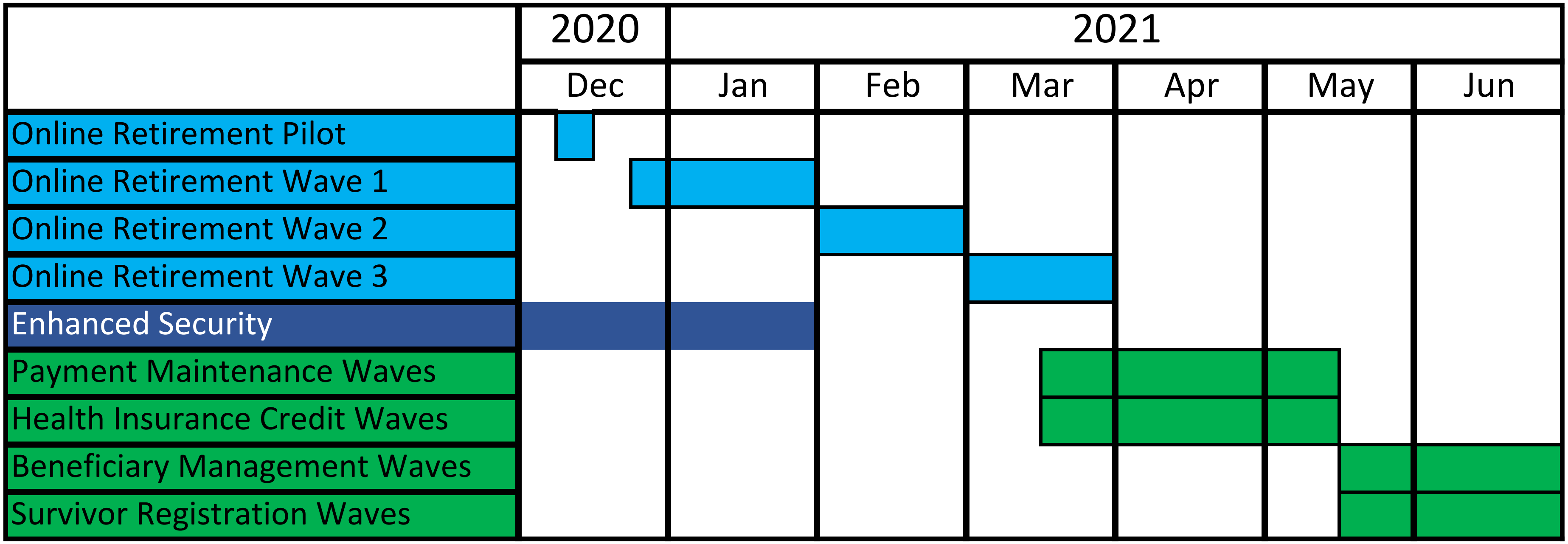
Background

- Modernization Program
  - The final deliverable under the Modernization Program is a set of new features for myVRS
    - Online retirement
    - Beneficiaries management
    - Retiree payment maintenance
    - Retiree health insurance credit maintenance
    - Survivor access
- This status report reflects progress as of 8/15/21

Current Software Status

myVRS Feature	Window Build	Integration Build	System Testing	Acceptance Testing
Online Retirement	Complete	Complete	Complete	Complete
Payment Maintenance	Complete	Complete	Complete	Complete
Beneficiary Management	Complete	Complete	Complete	Complete
Health Insurance Credit Maintenance	Complete	Complete	Complete	Complete
Survivor Access	Complete	Complete	Complete	Complete

Rollout Plan



All Rollouts are complete

Implementation Status

- Online Retirement – Complete
- Enhanced Security – Complete
- Payment Maintenance – Complete
- Beneficiary Management - Complete
- Health Insurance Credit – Complete
- Survivor Access - Complete

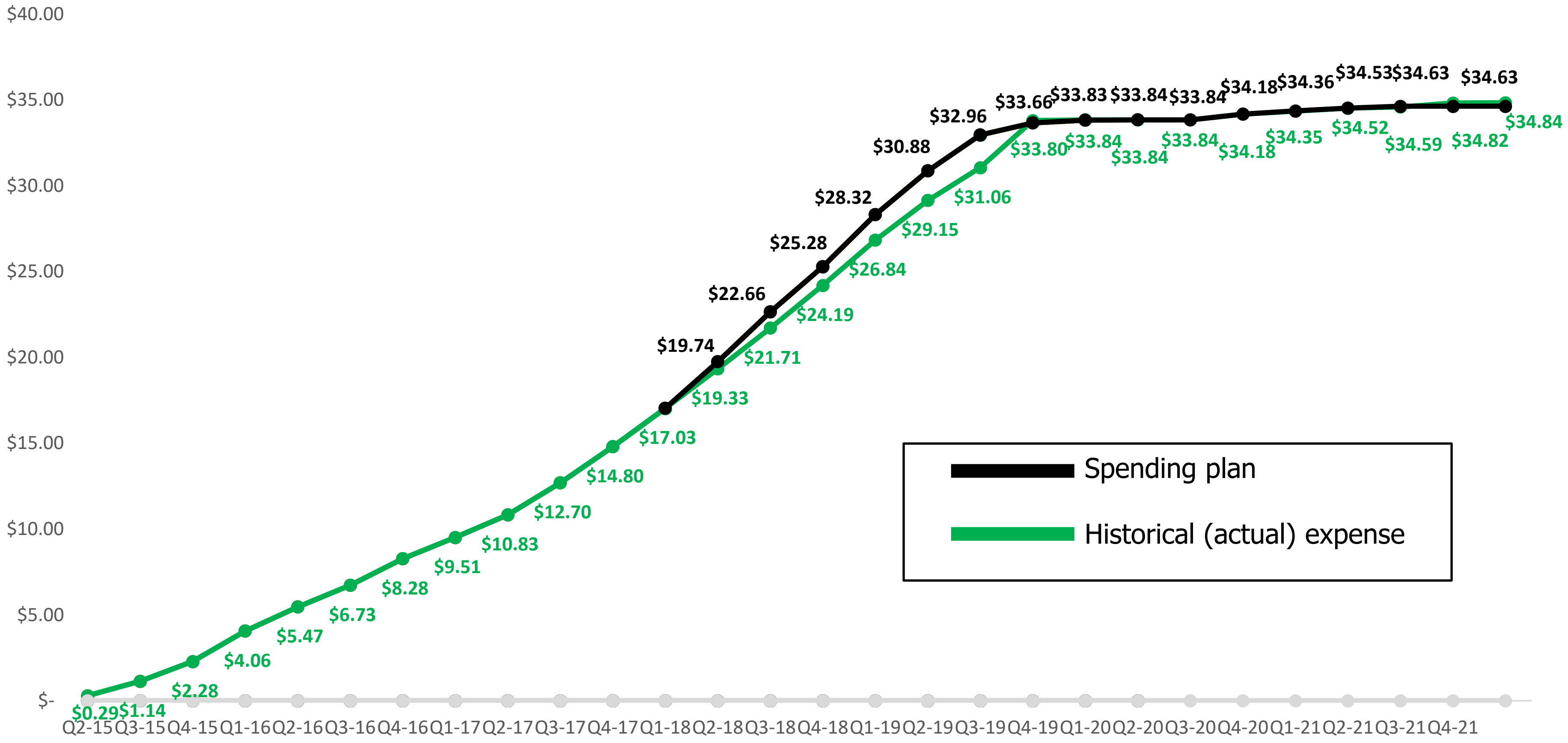
- Post wave business rollout – Complete 8/12/21
  - Risk mitigation approach during the May thru August time period
  - Control volume to ensure operations are not impacted by new processes

Online Retirement Production Update

Modules	Total Counts*
Online Retirement	• 320 requests successfully submitted online • 58 since it was turned on for all employers on 8/12/21
Payment Maintenance	• 1,009 requests successfully submitted online
Health Insurance Credit Maintenance	• 594 requests successfully submitted online
Beneficiary Management	• myVRS – 2,248 requests successfully submitted online
Survivor Registration	• 30 survivor registrations successfully completed online

**As of week of 8/26/2021*

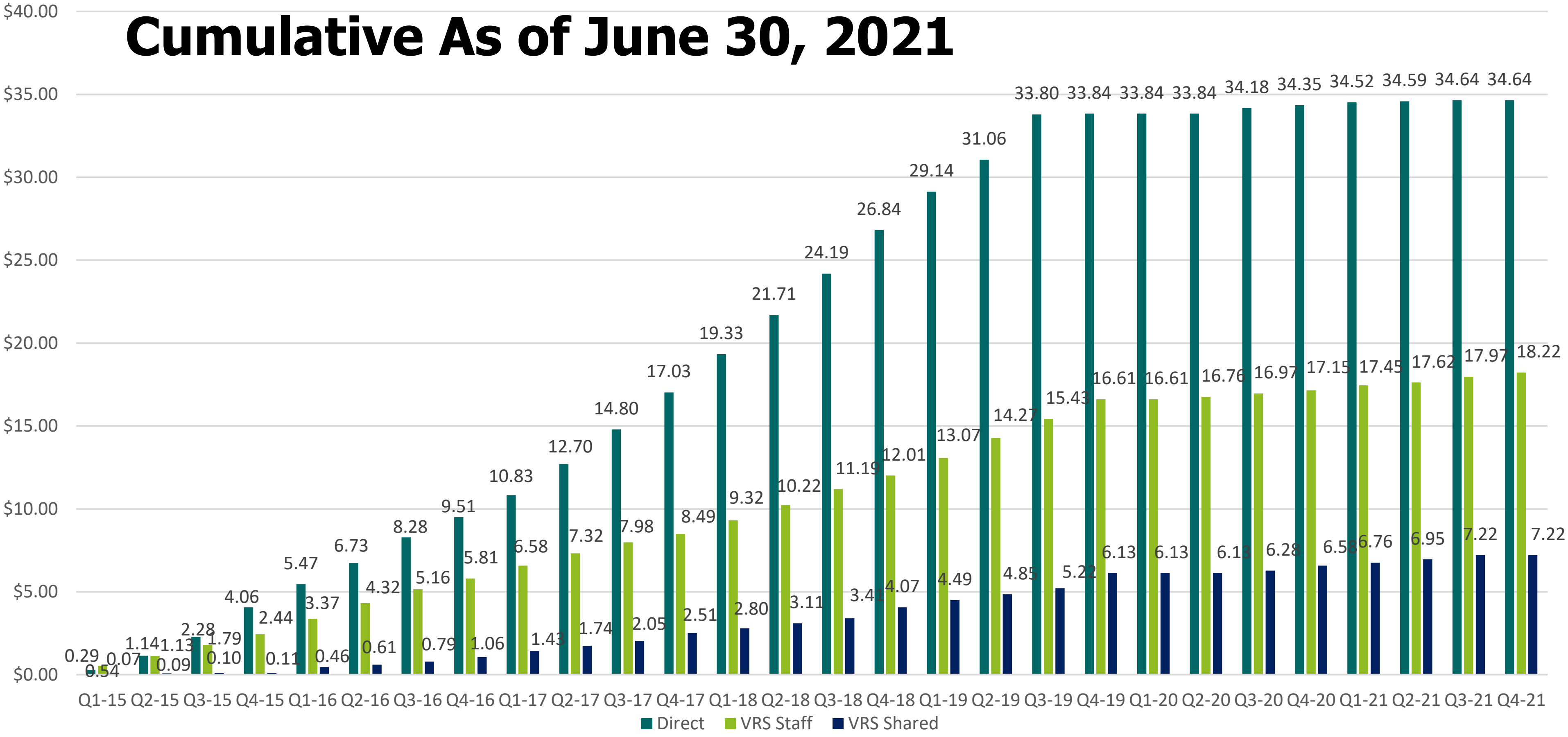
Budget as of 6/30/2021



Modernization Budget

- Modernization exceeded allocated funds by $201,774
    - 0.6% of the current budget
    - The exceeded amount is not included in the Total (Direct and Indirect) Cost slide as those numbers represent only the approved Modernization budget
- Technology Operations Funds Covered the Additional Cost
- Primarily Due to Complexity of the Enhanced Online Retirement and Security Initiatives

Total (Direct and Indirect) Cost



Cumulative As of June 30, 2021

Modernization Program Phase Four

Internal Audit's Quarterly Review

As of August 31, 2021

THIS REPORT IS INTENDED SOLELY FOR THE USE OF THE VRS BOARD OF TRUSTEES AND THE MANAGEMENT OF VRS AND IS NOT INTENDED FOR OTHER PURPOSES.

Phase Four's Scope

- To decommission the Retirement Information Management System (RIMS) by converting business functionality in RIMS over into VNAV. ☑

- To implement a new online customer portal for members and retirees. ☑

Phase Scope Changes

This Quarter

- *None.*

Previous Scope Changes

- *Quarterly Report as August 27, 2018 (reduction)*
  - Interactive Voice Response (IVR) Self-Service Replacement removal from phase scope.
- *Quarterly Report as of May 1, 2018 (reduction)*
  - Removal of Disability Retirement Case Management Functions. Case Management Functions will be handled by the new Medical Board vendor
- *Quarterly Report as of August 1, 2017 (increase)*
  - Incorporation of three individual projects under Phase Four scope for resource efficiencies.
    - ORPHE/ORPPA
    - Financial Education Resources within myVRS Portal
    - Retiree Portal Payment and Health Insurance Maintenance
- *Quarterly Report as of February 1, 2016 (increase)*
  - Addition of Online Assistance Tool for the Customer Contact Center within CSS #1 (Member Portal)

Observations

myVRS Functionality

- Full release of all features have been completed successfully.

Online Retirements

Soft Launch: April 2021
Full Release: Aug. 2021

Payment Maintenance

Full Release: June 2021

Beneficiary Management

Full Release: July 2021

HIC Maintenance

Soft Launch: June 2021
Full Release: Aug. 2021

Survivor Registration

Soft Launch: July 2021
Full Release: Aug. 2021

Phase Schedule

- Phase 4 has been successfully completed, with all planned scope and functionality implemented.

- We are in agreement with management's representation of Phase Four's overall status and progress to date.

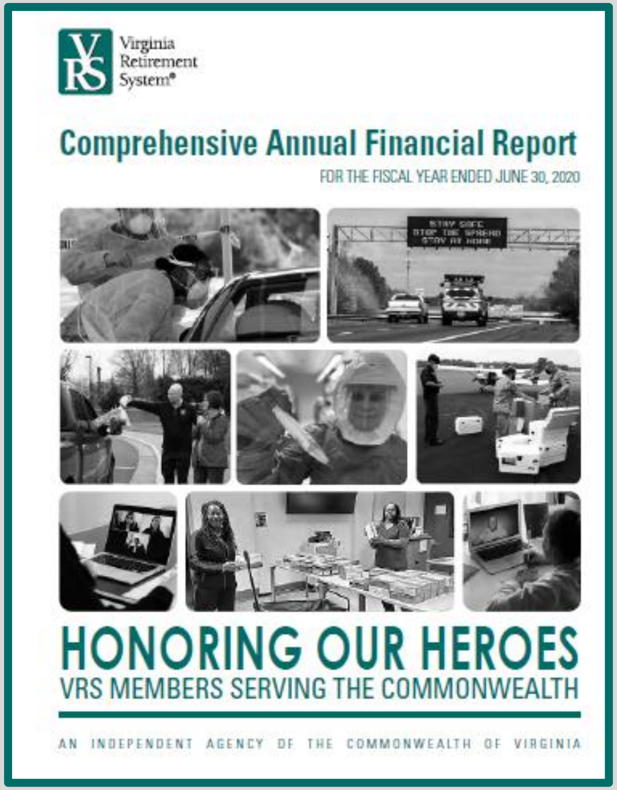
Phase Budget

- Phase Four has been completed over budget.

- Phase Four expenditures exceeded planned budget in total of just over $200,000.

- VRS has covered all overages with funds from the Technology Operations Department budget.

- We are in agreement with Phase Four expenditures to date represented in management's presentation.



VRS Virginia Retirement System®

Comprehensive Annual Financial Report

FOR THE FISCAL YEAR ENDED JUNE 30, 2020

HONORING OUR HEROES

VRS MEMBERS SERVING THE COMMONWEALTH

AN INDEPENDENT AGENCY OF THE COMMONWEALTH OF VIRGINIA

Methodology

Purpose

- To provide an objective assessment of the Modernization Program Phase Four’s progress, free from influence, guidance and control of the development effort.
- To provide validation of the accuracy of management’s quarterly status presentation.

Methodology continued…

Process

Gain an understanding of the purpose and progress of Phase Four through:

- Review of the Phase Four Microsoft SharePoint site or document management repository (applicable release documents)
- Interview of the Modernization Program Manager and other relevant personnel
- Attendance at ESC and other relevant meetings

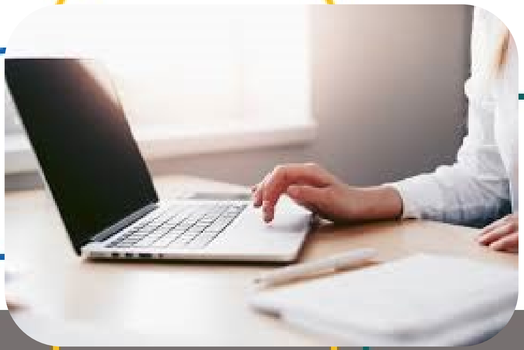
Approach and Timing

- Focus on specific areas active during the period of review
- Performed quarterly through the end of Phase Four

Questions

Annual Progress Reports for FY 2021

Virginia
Retirement
System



Internal Audit
FY2021 Annual Report
As of June 30, 2021

A look back and a look forward as the Internal Audit Department works to support the strategic goals and needs of this dynamic organization and to ensure appropriate avenues for oversight are provided to the Board of Trustees.

Virginia Retirement System

The Year in Review

Key Activities

Virginia Retirement System

Remaining agile, finding balance, and enhancing our partnerships in the ever-evolving Post-COVID world

Supporting VRS

Supporting agency initiatives including:

- VRS Commonwealth of Virginia Campaign
- Diversity Program
- Enterprise Risk Management
- Enterprise Performance Management
- Records Management

Dedicated to VRS' Commitment

"Serving those who serve others" by serving VRS

Continuous Improvement

Continued expansion of Internal Audit's access to data and business intelligence capabilities through cross-training and ongoing inter-departmental collaborative initiatives

Enhancement of audit tools and procedures supporting the audit process especially regarding communication and IT

Review and analysis of the Internal Audit Departmental Charter

Professional Growth

Emphasis on IT-related training opportunities to support growing responsibilities over IT assurance

New Certified Information Systems Auditor designation obtained

Key Activities

Issuing Informative Reports

Highlighting

- VRS' Core Values in Action
- Significant organizational initiatives and enhancements

Offering both formal and informal observations to support **VRS' Vision:**

To be the trusted leader in the delivery of benefits and services to those we serve

Focus on Independence and Objectivity

Maintaining our independence through routine Conflict-of-Interest certifications and communication in accordance with the IIA Standards and acknowledging responsibility for VRS' Code of Ethics and those of relevant professional organizations.

Providing Assurances regarding:

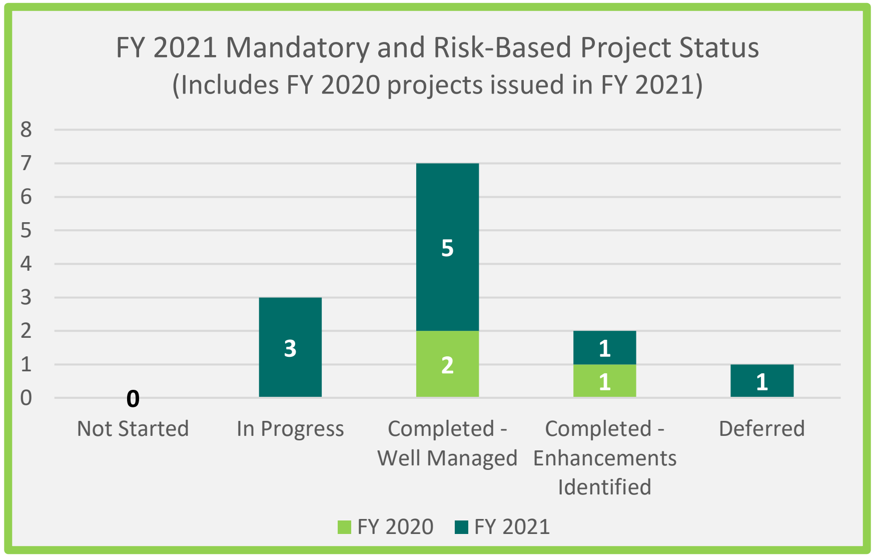
- Controls over VRS' investment research activities
- Management of the Line of Duty Act (LODA) program
- Oversight of the Multi-Asset Strategies Program (MAPS)
- Reliability of the application controls supporting member and employer contributions
- Administration of health insurance premiums and credit benefits
- Conformance of VRS' information security program with the Virginia Information Technologies Agency's (VITA) standards
- Accuracy of cost-of-living allowances recommended by the VRS actuary
- Management of the Optional Retirement Plan for Higher Education
- Controls over the Private Equity program
- Administration of Internal Equity Management
- Accuracy of Investment Incentive Compensation
- Fulfillment of VRS' Performance Outcomes

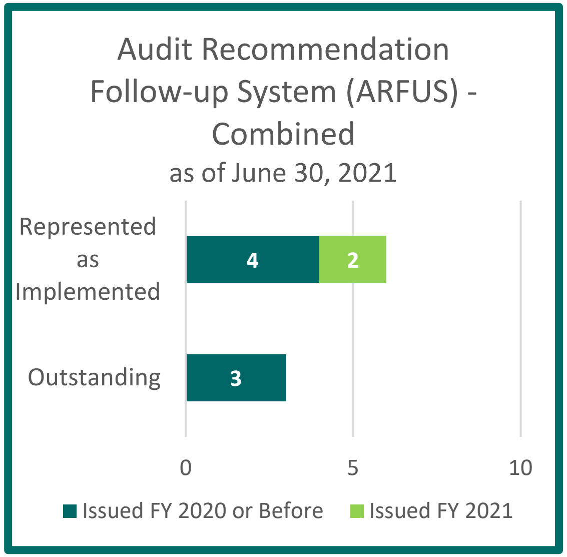
Quarterly Reporting on Modernization

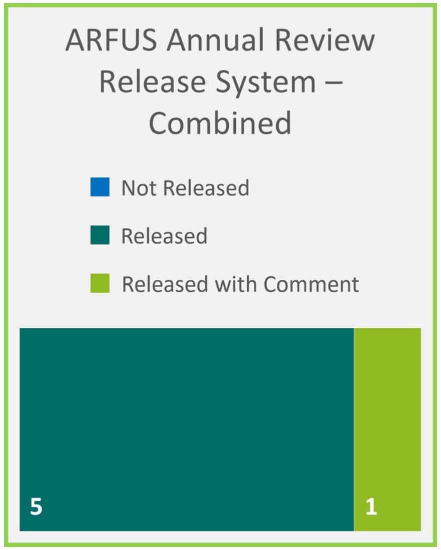
Quarterly Reporting on Fraud, Waste and Abuse Hotline Cases

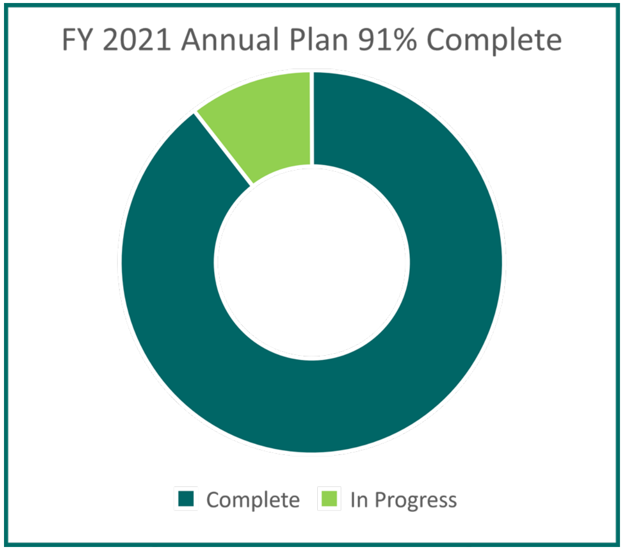
Annual ARFUS Review

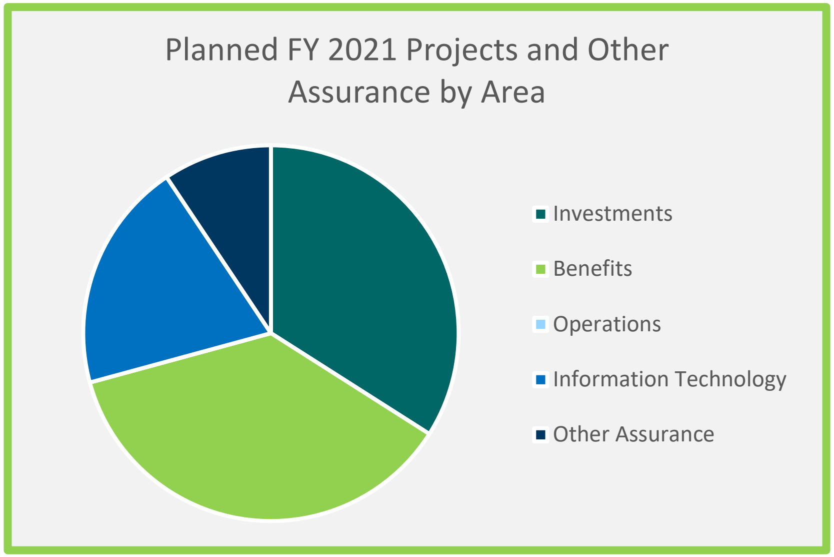
FY 2021 Annual Plan Dashboard











FY 2021 Projects In-Progress

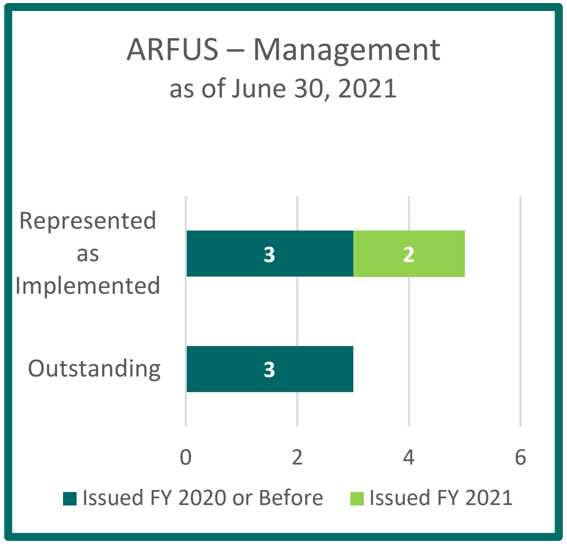
Reporting out in September

- Hosted Systems – Administration
- Application Controls – VNAV and ECM
- Review of Agency Performance Outcomes
- Annual ARFUS Review

Reporting out in December

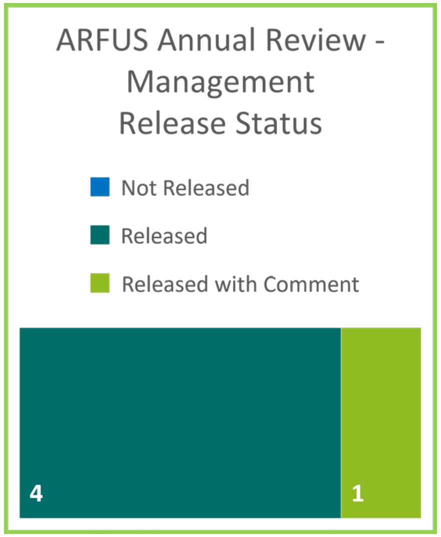
- Retiree Payroll – Processing and Changes

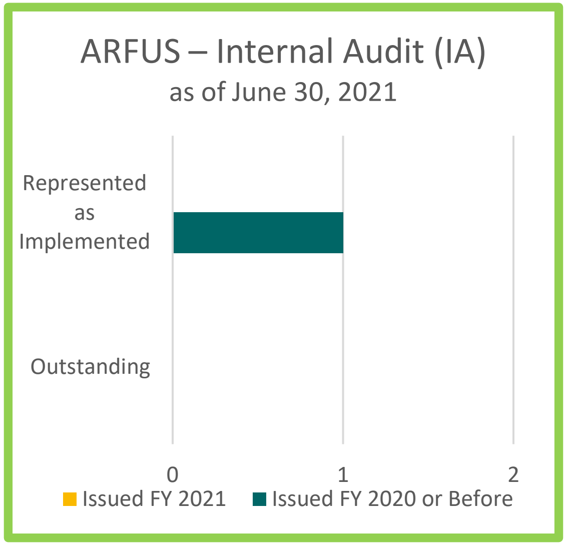
FY 2021 Annual Audit Recommendation Follow-up System (ARFUS) Review Results



ARFUS Review Results Management

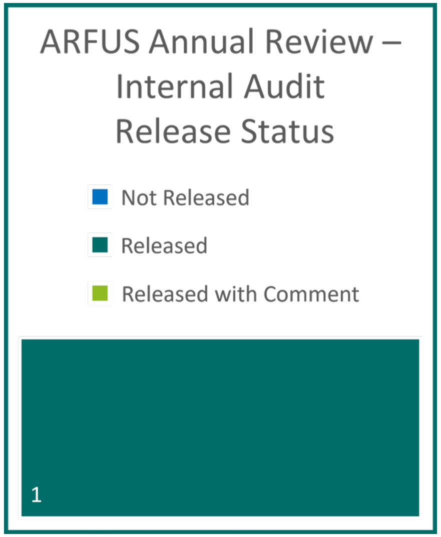
- As of June 30, 2021, Management's ARFUS included eight recommendations.
- Management represented five as implemented.
- Upon review, all five were released, one with comment.



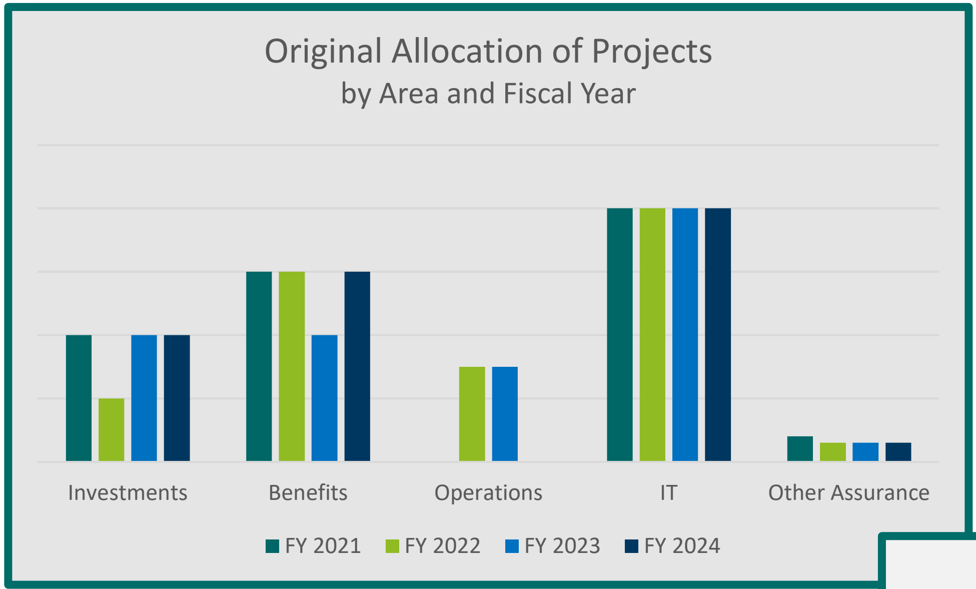


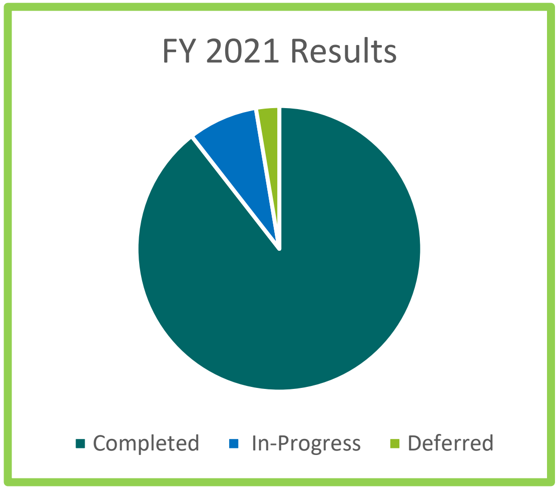
ARFUS Review Results Internal Audit

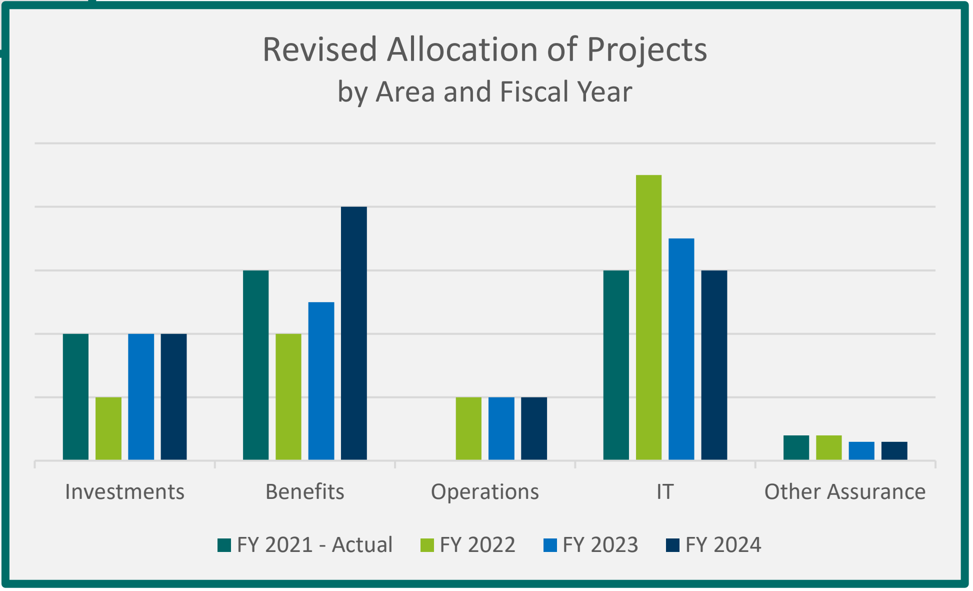
- As of June 30, 2021, Internal Audit's ARFUS included one recommendation.
- Internal Audit represented one as implemented.
- Upon review, it was released.



FY 2021 – FY 2024 Long-Range Plan Dashboard







- Considering FY 2021's results and VRS' changing risk landscape, the timing and execution of the remaining approved projects have been adjusted.
- Additional growth is anticipated in the IT area due to enhanced risk assessment activities by VRS IT to support VRS' move into the Cloud. These risk assessments will be leveraged to continuously assess the approach for and timing of our IT work.

Virginia
Retirement
System

A Look Forward

Proposed FY 2022 Annual Plan

Derived from Approved Long-Range Plan. Adjusted for revised risk assessment and operational considerations.

Carry Over

- Retiree Payroll – Processing and Changes (Reporting in Dec)
- Hosted Systems Review – Administration (Reporting in Sept)
- VNAV and Related Systems Review (Reporting in Sept)

Investments

- Fixed Income Program and Securities Lending

Benefits

- Disability Retirements
- Long-Term Care Program (Deferred)
- Refunds (Deferred)
- Retirement Application Processing (Deferred)

Operations

- Cash Assets and Cash Management (Administration and Investments)
- Procurement and Contract Management (Deferred)

Information Technology

- Conformance of VRS Information Security Program with VITA Standards
- General Controls Review of VRS' Operating Environment
- General Ledger Review
- myVRS

- Modernization Program Monitoring
- Report on Fraud, Waste and Abuse Hotline Cases
- Review of Investment Incentive Compensation Plan
- Review Results of Agency Performance Outcomes
- Verification of Cost of Living Adjustment
- Special Initiative to develop IT Audit Augmentation Program ahead of FY 2023

Maintaining Quality Audit Staffing

Virginia Retirement System

- Given the complexity of VRS' operations, the department does not employ entry level auditors
- Combined, the current team has almost 100 years experience in the auditing profession
- Each member holds two or more professional designations

- Continuing professional education is required to maintain professional designations and helps to ensure the continued quality of the work performed by the team by honing their knowledge, skills and abilities.

Professional Designations

CIA
(Certified Internal Auditor)

CISA
(Certified Information Systems Auditor)

CPA
(Certified Public Accountant)

PMP
(Project Management Professional)

CIDA
(Certified Investments & Derivatives Auditor)

CFE
(Certified Fraud Examiner)

CRMA
(Certified in Risk Management Assurance)

Growing our Bench Strength for the Future

Given VRS' intentional and thoughtful move to the Cloud over the next several years, the knowledge, skills and abilities needed to adequately support our VITA-mandated audit responsibilities in the future will inherently grow in complexity. We are actively participating in training to prepare the team for the changing landscape but recognize we will benefit from additional technically trained resources in the IT audit space.

Team Members and Qualifications

Matt Priestas

Principal Auditor for Information Technology, Security, Systems Development and Project Management

CISA, CIA, PMP, CRMA

B.S. in Management Information Systems, East Carolina University

Joined VRS in 2008, previously worked for the APA

Newscenter SharePoint Site Administrator, APPFA liaison

Judy Bolt

Principal Auditor for Benefits, Operations and Quality Assurance

CPA, CIA, CFE, CISA

B.S. in Accounting, Virginia Commonwealth University (VCU)

Joined VRS in 2012, previously worked for the APA and Owens and Minor

Lead for the Quality Assurance and Improvement Program

Josh Fox

Principal Auditor for Investments and Operations

CIA, CIDA, CFE

B.S. in Finance and Management, Virginia Polytechnic Institute and State University (Virginia Tech)

Joined VRS in 2014, previously worked for the APA

Lead for Investments, training as business intelligence back-up

Krystal Groff

Principal Auditor for Business Intelligence

CIA, CISA

B.S. in Computer Science, University of Mary Washington; M.S. in Nursing Informatics, Duke University

Joined VRS in 2015, previously worked for the Federal Reserve Bank of Richmond, Capital One and Circuit City

Experience with various technologies and programming languages including: SQL, Tableau, Ab Initio, UNIX and C

Kristy Scott

Principal Auditor for Governance and Program Administration

CPA, CISA, CIA

B.B.A., Roanoke College; Post-Baccalaureate Certificate in Accounting, VCU; holds COSO Enterprise Risk Management Certificate

Joined VRS in 2018, previously worked for the APA

Team SharePoint Site Administrator, training as business intelligence back-up

Jennifer Schreck

Internal Audit Director

CPA, CISA, PMP

B.S. in Accounting, College of William and Mary

Joined VRS in 2015, previously worked for the APA

Holds an Associates Certificate in Project Management and a Master's Certificate in IT Project Management

Virginia Retirement System

ANNUAL REPORT ON THE AUDIT RECOMMENDATION FOLLOW-UP SYSTEM As of June 30, 2021

BACKGROUND

The Audit Recommendation Follow-Up System (ARFUS) is a reporting mechanism for monitoring the status of audit recommendations issued by Internal Audit, the Auditor of Public Accounts (APA) or other external entities. Internal Audit maintains the information recorded in ARFUS with the cooperation and assistance of management.

On a quarterly basis, Internal Audit requests and receives progress reports from management on outstanding recommendations, which describe the status of the actions taken in response to the recommendations. While compiled by Internal Audit, the information included in the quarterly summary reflects the representations of the responsible party and are not subject to verification by Internal Audit at that time. Recommendations represented as "implemented" remain in ARFUS until Internal Audit performs its review to obtain reasonable assurance that the essence of the recommendation has been implemented.

Annually, Internal Audit conducts a limited review on all recommendations represented as implemented to obtain assurance that management has in fact reasonably addressed these recommendations. Where reasonable implementation is confirmed, the recommendation is released from ARFUS and is no longer subject to monitoring by Internal Audit. Further, Internal Audit identifies the addition and removal of any audit recommendations issued by the APA within ARFUS based upon a review of APA reports.

ARFUS Activity during FY 2021

ARFUS Components	Internal Audit	APA*	Total
Total Outstanding Recommendations as of June 30, 2020	6	–	6
Recommendations Added during FY 2021	2	–	2
Total Recommendations for FY 2021 (available for remediation)	8	–	8
Informational: Recommendations Represented as Implemented during FY 2021	*5*	–	*5*
Represented Recommendation(s) tested and released by Internal Audit (see page 2)	(5)		(5)
Represented Recommendation(s) tested and released by APA (see page 3)	–	–	–
Total Outstanding Recommendations as of June 30, 2021 (see page 3)	**3**	–	**3**

* Recommendations issued by the APA are listed separately from the Internal Audit activity above, as the decision to issue or release such findings rests with their office.

The purpose of this report is to convey the results of our review regarding the audit recommendations represented as implemented as of June 30, 2021.

RECOMMENDATION VALIDATION AND RELEASE FROM ARFUS

During fiscal year 2021, management represented five recommendations as implemented. Internal Audit reviewed these recommendations to validate that they were reasonably addressed. This review was not designed to test the operational effectiveness of the implemented controls. The testing of these controls will be considered within the scope of future audits. Our review found all five recommendations have been sufficiently implemented and no longer warrant oversight. Accordingly, Internal Audit is releasing these recommendations from ARFUS. (One recommendation was released with comment as reflected in the "Status of Recommendations Represented as Implemented" summary found below.)

THIS REPORT IS INTENDED SOLELY FOR THE USE OF THE VRS BOARD OF TRUSTEES AND THE MANAGEMENT OF VRS AND IS NOT INTENDED FOR OTHER PURPOSES.

STATUS OF RECOMMENDATIONS REPRESENTED AS IMPLEMENTED

The table below reflects the status of each recommendation represented as implemented (with explanatory comments as appropriate). Please note that the "Audit # - Audit Name" has been hyperlinked to the applicable audit report and management response within Directors Desk.

Audit # - Audit Name	Recommendation Represented as Implemented	Management's Target Date	Completion Date	Audit Comments
367 - IT Client-Server	Modify Procedures in Three Areas to Ensure Full Compliance with the VRS Security Standard	12/31/2020* ~~12/31/2019~~ ~~07/01/2019~~ for Project 2 01/01/2018 for Project 1 (Project 1 is complete)	12/31/2020	**Released with Comment** *Timely Training of COOP Team Replacements* Management successfully developed processes to ensure compliance with the VRS Security Standard. While the processes are established, opportunities for enhancements in the execution of COOP training within 30 days of an individual assuming a COOP role, as dictated in CP-3 of the VRS Security Standard, were discussed with management. *AD Monitoring & Annually Review and Renew Administrative Privilege Exceptions* Fully Implemented
411 – Application Controls: VNAV and myVRS	Evaluate VNAV's Documented Security Procedures and Ensure Ongoing Monitoring of System Access Occurs	12/31/2020* ~~12/31/2019~~ ~~07/01/2019~~	12/31/2020	**Released without Comment** Fully Implemented
429 – Conformance with VITA's Security Program	Address the ISO Relationship to the VRS Director	06/30/2021	3/31/2021	**Released without Comment** Fully Implemented
430 – Investment Research	Enhance the Investment Department's Communication and Reporting of IT-Related Acquisition Activity to the IT Department	6/30/2021	6/30/2021	**Released without Comment** Fully Implemented
434 – Health Insurance Premiums and Credits	Implement Ongoing Monitoring Techniques over Health Benefits Area	6/30/2021	6/30/2021	**Released without Comment** Fully Implemented

*The Director's Executive Committee approved revisions to the original target date as reflected in the table above.

OUTSTANDING AUDIT RECOMMENDATIONS AS OF JUNE 30, 2021

The following is a list of outstanding recommendations remaining in ARFUS as of June 30, 2021. Please note that the “Audit # - Audit Name” has been hyperlinked to the applicable audit report and management response within Directors Desk.

Audit # - Audit Name	Recommendation	Report Date	Management's Target Date
412 – Hybrid Plan	Improve the Expected versus Actual Contributions Reconciliation Review Process	11/01/2017	TBD* (Part of Post-Phase 4 work. Revised Phase 4 schedule is still pending.) ~~12/31/2019~~
425 – Review of the General Controls within the IT Client-Server Environment	Enhance Management of Policy and Procedure Documents	08/01/2019	12/31/2021* ~~6/30/2021~~ ~~12/31/2020~~
425 – Review of the General Controls within the IT Client-Server Environment	Update Retention and Disposition Schedules to align with Library of Virginia Standards as well as VRS’ Actual Practice	08/01/2019	TBD* ~~06/30/2021~~

*The Director’s Executive Committee approved revisions to the original target date as reflected in the table above.

RECOMMENDATIONS ISSUED BY THE APA

Recommendations issued and released by the APA are captured based on the results reflected in their reports and are included below for informational purposes. Please note that the “Audit Name” has been hyperlinked to the applicable audit report on the APA’s website.

Audit Name	Recommendation	Represented as Implemented? (Y/N)	Management's Target Date	Completion Date	Audit Comments
–	–	–	–	–	–

Virginia
Retirement
System

ANNUAL REPORT ON THE AUDIT RECOMMENDATION FOLLOW-UP SYSTEM FOR INTERNAL AUDIT As of June 30, 2021

BACKGROUND

The Audit Recommendation Follow-Up System (ARFUS) is a reporting mechanism for monitoring the status of audit recommendations issued by Internal Audit, the Auditor of Public Accounts (APA) or other external entities. Internal Audit maintains the information recorded in ARFUS with the cooperation and assistance of management.

This specific report reflects the status of Internal Audit related recommendations issued as a result of our external quality assurance review performed once every five years, most recently completed in the fall of 2019 and reported to the Committee December 12, 2019.

Of note, while recommendations were added to ARFUS as a result of this review, they represented opportunities to enhance existing processes rather than a reflection of any deficiencies relative to the *Standards* issued by the Institute of Internal Auditors.

ARFUS Components	Total
Total Outstanding Recommendations as of June 30, 2020	1
Recommendations Added during FY 2021	0
Total Recommendations for FY 2021 (available for remediation)	1
Informational: Recommendations Represented as Implemented during FY 2021	*1*
Represented Recommendation(s) tested and released by Internal Audit (see page 2)	(1)
Total Outstanding Recommendations as of June 30, 2021 (see page 2)	**0**

On a quarterly basis, Internal Audit staff requests and the Internal Audit Director provides progress reports on such outstanding recommendations, which describe the status of the actions taken in response to the recommendations. The information included in the quarterly summary reflects the representations of the responsible party and are not subject to verification by Internal Audit at that time. Recommendations represented as "implemented" remain in ARFUS until Internal Audit performs its review to obtain reasonable assurance that the essence of the recommendation has been implemented.

Annually, Internal Audit conducts a limited review on all recommendations represented as implemented. Where reasonable implementation is confirmed, the recommendation is released from ARFUS and is no longer subject to monitoring by Internal Audit.

The purpose of this report is to convey the results of our review regarding the recommendations from the external quality assurance review represented as implemented as of June 30, 2021.

RECOMMENDATION VALIDATION AND RELEASE FROM ARFUS

During fiscal year 2021, the Internal Audit Director represented one recommendation as implemented. Internal Audit reviewed this recommendation to validate that the recommendation was reasonably addressed. Our review found the recommendation has been sufficiently implemented and no longer warrants monitoring. Accordingly, Internal Audit is releasing this recommendation from ARFUS.

THIS REPORT IS INTENDED SOLELY FOR THE USE OF THE VRS BOARD OF TRUSTEES AND THE MANAGEMENT OF VRS AND IS NOT INTENDED FOR OTHER PURPOSES.

STATUS OF RECOMMENDATIONS REPRESENTED AS IMPLEMENTED

The table below reflects the status of each recommendation represented as implemented (with explanatory comments as appropriate). Please note that the "Report Name" has been hyperlinked to the applicable report within Directors Desk.

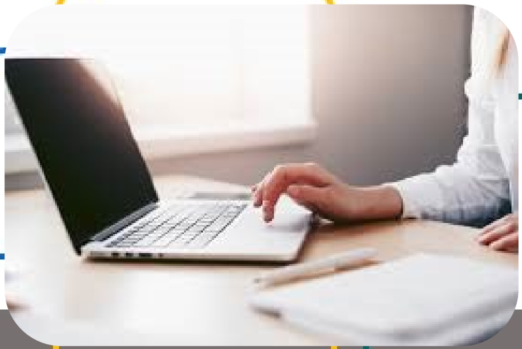
Report Name	Recommendation Represented as Implemented	Internal Audit's Target Date	Completion Date	Audit Comments
VRS External Quality Assurance Review Report Date: 10/31/2019	Consider establishing a joint data analytics initiative with IT to enhance IAD's capability.	6/30/2021	6/30/2021	**Released without Comment** Fully Implemented

OUTSTANDING RECOMMENDATIONS AS OF JUNE 30, 2021

The following is a list of outstanding recommendations remaining in ARFUS as of June 30, 2021. Please note that the "Report Name" has been hyperlinked to the applicable report within Directors Desk.

Report Name	Recommendation	Report Date	Internal Audit's Target Date
-	-	-	-

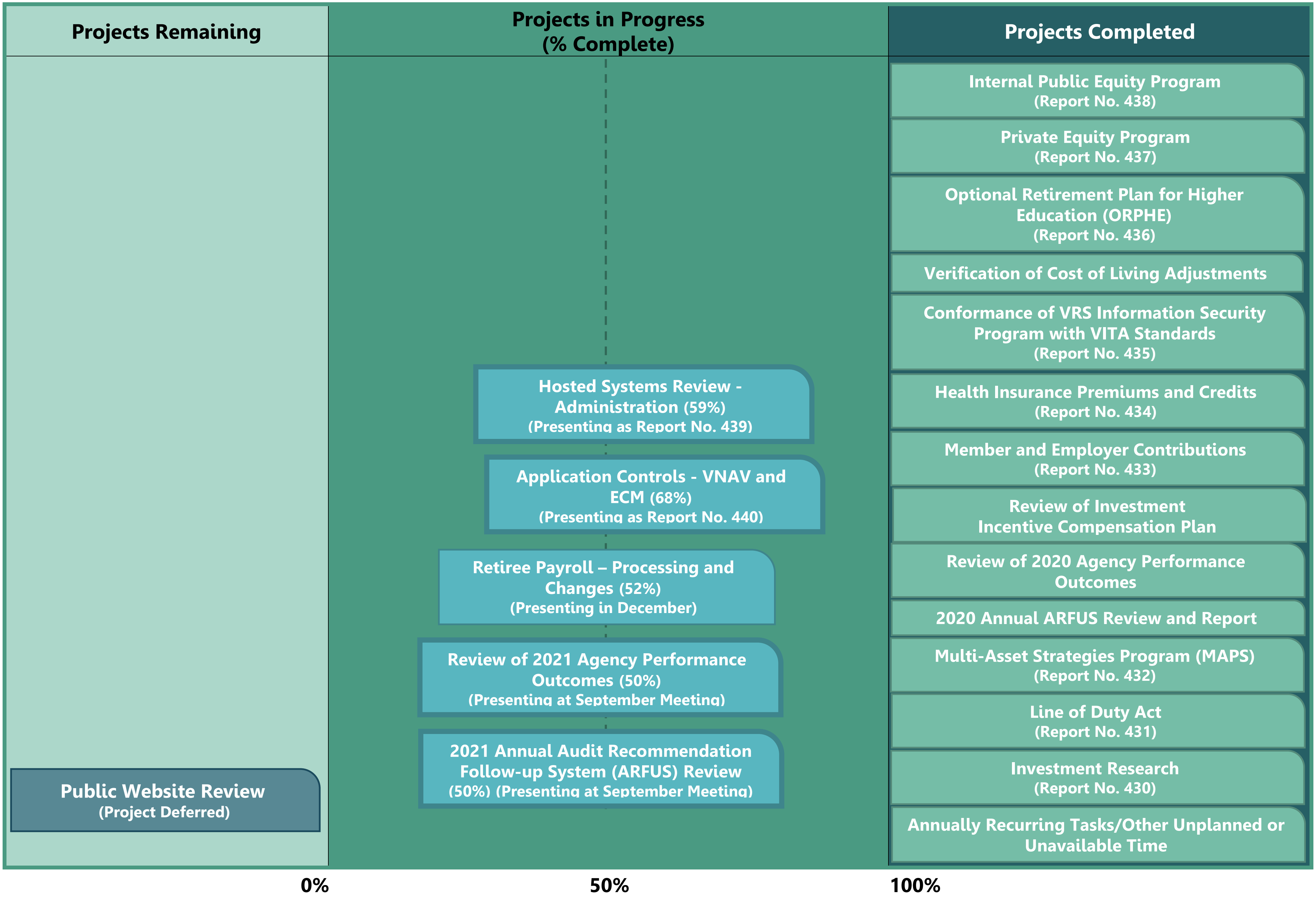
Virginia
Retirement
System



Internal Audit
FY2021 Annual Audit Plan
Progress Report

As of June 30, 2021

Fiscal Year 2021 Annual Audit Plan Progress Summary – as of June 30, 2021



Projects Remaining

Public Website Review
(Project Deferred)

Projects in Progress (% Complete)

Hosted Systems Review - Administration (59%)
(Presenting as Report No. 439)

Application Controls - VNAV and ECM (68%)
(Presenting as Report No. 440)

Retiree Payroll – Processing and Changes (52%)
(Presenting in December)

Review of 2021 Agency Performance Outcomes (50%)
(Presenting at September Meeting)

2021 Annual Audit Recommendation Follow-up System (ARFUS) Review (50%)
(Presenting at September Meeting)

Projects Completed

Internal Public Equity Program
(Report No. 438)

Private Equity Program
(Report No. 437)

Optional Retirement Plan for Higher Education (ORPHE)
(Report No. 436)

Verification of Cost of Living Adjustments

Conformance of VRS Information Security Program with VITA Standards
(Report No. 435)

Health Insurance Premiums and Credits
(Report No. 434)

Member and Employer Contributions
(Report No. 433)

Review of Investment Incentive Compensation Plan

Review of 2020 Agency Performance Outcomes

2020 Annual ARFUS Review and Report

Multi-Asset Strategies Program (MAPS)
(Report No. 432)

Line of Duty Act
(Report No. 431)

Investment Research
(Report No. 430)

Annually Recurring Tasks/Other Unplanned or Unavailable Time

91% of the planned work was completed during the work plan year based on the adjusted budgets.

FY2021 Annual Audit Plan - Progress Report - Detailed Analysis

Budget vs. Actual - As of June 30, 2021

	Budgeted Hours	Status	Total Actual Hours to Date	Estimated Remaining Hours	Actual or Estimate of Total Hours Needed	Estimated Variance Over/ (Under)
RISK BASED PROJECTS						
Carry Over from Prior Long-Range Plan						
Line of Duty Act	50	Complete	61	-	61	11
Member and Employer Contributions	200	Complete	261	-	261	61
Investment Research (Portfolio Intelligence Team)	100	Complete	127	-	127	27
Investments						
Internal Public Equity Program [1]	550	Complete	974	-	974	424
Private Equity Program	600	Complete	747	-	747	147
Benefits						
Health Insurance Premiums and Credits	400	Complete	474	-	474	74
Optional Retirement Plan Higher Education (ORPHE) [2]	600	Complete	741	-	741	141
Retiree Payroll - Processing and Changes [3]	800	In Progress	645	600	1,245	445
Operations						
Information Technology						
Conformance of VRS Information Security Program with VITA Standards	150	Complete	137	-	137	(13)
Hosted Systems Review - Administration [4]	500	In Progress	431	300	731	231
VNAV and Related Systems Review [4]	800	In Progress	536	250	786	(14)
VRS Public Website Review [5]	500	Deferred	-	-	-	(500)
OTHER AUDIT REPORTING AND SUPPORT						
Other Reporting						
Audit Quality Assurance Improvement Program	150	Complete	180	-	180	30
Audit Recommendation Follow-Up System Annual Review [6]	150	FY20 Complete	64	-	64	(86)
Audit Recommendation Follow-Up System Quarterly Monitoring	25	In Progress	51	-	51	26
Modernization Program Monitoring	200	In Progress	282	50	332	132
Report on Fraud, Waste and Abuse Hotline Cases	75	In Progress	36	-	36	(39)
Review of Investment Incentive Compensation Plan	75	Complete	76	-	76	1
Review Results of Agency Performance Outcomes (APOs) [6]	75	FY20 Complete	102	-	102	27
Verification of Cost of Living Adjustments (COLAs) [6]	20	Complete	15	-	15	(5)

FY2021 Annual Audit Plan - Progress Report - Detailed Analysis

Budget vs. Actual - As of June 30, 2021

	Budgeted Hours	Status	Total Actual Hours to Date	Estimated Remaining Hours	Actual or Estimate of Total Hours Needed	Estimated Variance Over/ (Under)
OTHER AUDIT REPORTING AND SUPPORT, Continued						
Audit Support						
Coordination with the APA	40	Ongoing	18	-	18	(22)
Data Analytics and Support	900	Ongoing	866	-	866	(34)
Develop and Update Annual and Long-Range Plans	125	Ongoing	83	-	83	(42)
Monitor Annual and Long-Range Plan Progress	100	Ongoing	95	-	95	(5)
Audit and Compliance Committee Support						
Review, Compile and Publish Meeting Materials	300	Ongoing	369	-	369	69
Attend Audit and Compliance Meetings	80	Ongoing	64	-	64	(16)
Prepare Committee Report and Meeting Minutes	80	Ongoing	60	-	60	(20)
ONGOING ACTIVITIES						
Risk Monitoring Activities						
Attend Board and other Committee Meetings	170	Ongoing	160	-	160	(10)
Attend Executive Team Meetings (DEC, Roadmap, C-suite)	100	Ongoing	108	-	108	8
Monitor and Review Professional Literature	90	Ongoing	96	-	96	6
Participate in Professional Organizations	90	Ongoing	36	-	36	(54)
Other Administrative Activities						
Continuing Professional Education	360	Ongoing	438	-	438	78
Continuing Professional Education Administration	150	Ongoing	93	-	93	(57)
External Reporting and Other Interactions (OSIG/VITA)	10	Ongoing	28	-	28	18
Internal Audit Staff Meetings and Mentoring	300	Ongoing	385	-	385	85
Manage Budget, Departmental Files, SPCC, and Purchasing	100	Ongoing	58	-	58	(42)
Participate in VRS Events/Committees	150	Ongoing	158	-	158	8
Performance Standards and Evaluations	60	Complete	54	-	54	(6)
OTHER TIME						
Annual Leave	750	Ongoing	858	-	858	108
Holidays	648	Ongoing	696	-	696	48
Other Leave (Sick, Personal, Volunteer, etc)	660	Ongoing	814	-	814	154
Unplanned Hours [7]	1,197	Ongoing	1,059	-	1,059	(138)
TOTAL TIME [8]	**12,480**		**12,536**	**1,200**	**13,736**	**1,256**

Fiscal Year 2021 - Annual Audit Plan Progress – Detailed Analysis

Budget vs. Actual – as of June 30, 2021

Explanatory Notes:

[1] This program was last reviewed in 2014. Overages are due to expanded scope and testwork over operational activities closely aligned to this program not originally envisioned for the project. Given the duration since the last audit, the enhancements to the program and changes in leadership and focus for the program, these expansions are not unusual and help to enrich our audit coverage and address additional audit risks within the program and administration of investments.

[2] This program was last reviewed in 2010. Overages are due to expanded scope and testwork over operational activities closely aligned to this program not originally envisioned for the project. Given the duration since the last audit, the adjustments to the program and changes in leadership, these expansions are not unusual and help to enrich our audit coverage and address additional audit risks within the program.

[3] This program was last reviewed in 2015. Overages are due to expanded scope and testwork over operational activities closely aligned to this program not originally envisioned for the project. Given the duration since the last audit, the modernization of the systems supporting this process, these overages and expansions are not unusual and help to enrich our audit coverage and address additional audit risks. This project also started lanter than originally anticipated to address organizational resource considerations and needs and will therefore carry over into the next audit plan year for reporting at the December Audit and Compliance Committee meeting. Adjustments will be made when developing the proposed audit plan for FY2022 to accommodate this time.

[4] These projects started later than originally anticipated either to address internal or organizational resource considerations and needs and will therefore carry over into the next audit plan year to be reported at the September Audit and Compliance Committee meetings. Adjustments will be made when developing the proposed audit plan for FY2022 to accommodate them.

[5] This project has been deferred for consideration in a future period.

[6] These projects reflect annually recurring tasks which require testwork to be initiated in one audit plan year and the conclusion and reporting to occur in the next. The actual hours to date reflect time spent completing the FY2021 projects and initiating the FY2022 projects.

[7] The unplanned hours reported reflect departmental items not explicitly planned for in our original budget, such as

- [A] Administrative and computer issues;
- [B] VRS provided training;
- [C] Internal Audit's involvement in VRS' Enterprise Risk Management and Enterprise Performance Management Initiative;
- [D] Internal Audit's support of the development of an agency performance objective and operational measure dashboard;
- [E] Review and enhancement of departmental policies and procedures and supporting tools; and
- [F] Continued enhancement of SharePoint capabilities to store and manage audit documentation.

[8] Total time for the year was budgeted based on the average of 2080 man hours being available in a year; however in FY 2021 there were actually 2088 man hours available based on the timing of the weekdays verses weekends. In addition, staff work various "flex" schedules, the timing of those flex schedules allowed for 8 additional hours to be worked during the period. Therefore, 56 additonal hours were worked over the budgeted hours.

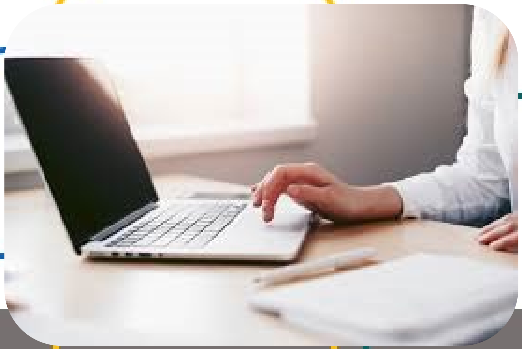
Acronyms (Not defined elsewhere):

APA	Auditor of Public Accounts
ARFUS	Audit Recommendation Follow-Up System
C-suite	Chief Executives for VRS, including the Executive Director and Chief Investment Officer
DEC	Director's Executive Committee
IIA	Institute of Internal Auditors
ISACA	Information Systems Audit and Control Association
OSIG	Office of the State Inspector General
Roadmap	Program management tool used by VRS management to monitor critical organizational activities
SPCC	Small Purchase Charge Card
VITA	Virginia Information Technologies Agency

Virginia
Retirement
System

Internal Audit
FY 2021 – FY 2022
Long-Range Plan
Progress Report

As of June 30, 2021



Virginia Retirement System

Approved Long-Range Plan FY2021 - FY2024 - Progress and Adjustments as of June 30, 2021

Approved Projects	Approved Total Budgeted Hours	Actual	Approved Budgets			Total	Variance	Comments
		FY2021	FY2022	FY2023	FY2024			
RISK BASED PROJECTS								
Carry Over from Prior Long-Range Plan								
Line of Duty Act	50	60				60	10	**Complete**
Member and Employer Contributions	200	220				220	20	**Complete**
Portfolio Intelligence Team	100	120				120	20	**Complete**
Investments								
Credit Strategies Program and Private Investment Partnerships (PIP)	600			600		600	-	
Fixed Income Program and Securities Lending	600		600			600	-	
Global Public Equity Program	600				600	600	-	
Internal Public Equity Program	550	900				900	350	**Complete - See FY 2021 Annual Plan Progress Report**
Investment Balances, Performance Reporting and Investment Manager Compensation	750				750	750	-	
On-Site Review of Bank of New York Mellon	600			600		600	-	
Private Equity Program	600	750				750	150	**Complete - See FY 2021 Annual Plan Progress Report**
Benefits								
Deferred Compensation, Cash Match Plans, ORPs, VOLSAP and the Benefit Restoration Plan	700				-	-	(700)	Project deferred for consideration in a later period as the risk profile for the audit area has changed.
Disability Retirements	700		700	-		700	-	Pushed forward to FY 2022 to better accommodate other project timing.
Health Insurance Premiums and Credits	400	400				400	-	**Complete**
Long-Term Care Program	400		-		400	400	-	Moved to FY2024 to accommodate adjustments to IT and other project timing.
Managed Disabilities Programs (VSDP and VLDP)	800			800		800	-	
Member and Employer Contributions	700				700	700	-	
Optional Retirement Plan Higher Education (ORPHE)	600	600				600	-	**Complete**
Purchase of Prior Service	700				700	700	-	
Refunds	800		-	200	600	800	-	Moved to begin in FY 2023 and carry over to FY 2024 to accommodate adjustments to IT and other project timing.
Retiree Payroll - Processing and Changes	800	650	600			1,250	450	Increased project hours and to address expanded scope and process changes since previous audit, resulting in carry over.
Retirement Application Processing	800		-	800		800	-	Pushed back to FY 2023 to better accommodate project timing.
Operations								
Cash Assets and Cash Management (Administration and Investments)	600		600			600	-	
Human Resources, Internal Payroll and Leave Administration	600			600		600	-	
Procurement and Contract Management (Administration and Investments)	600		-	-	600	600	-	Moved from FY 2022/FY 2023 to FY 2024 to accommodate adjustments to IT and other project timing.

Virginia Retirement System
Approved Long-Range Plan FY2021 - FY2024 - Progress and Adjustments as of June 30, 2021

Approved Projects	Approved Total Budgeted Hours	Actual	Approved Budgets			Total		
		FY2021	FY2022	FY2023	FY2024			
RISK BASED PROJECTS, Continued								
Information Technology [1]								
Conformance of VRS Information Security Program with VITA Standards	600	150	150	150	150	600	-	Complete
General Controls Review over VRS' Operating Environment (Infrastructure Systems, excluding Physical Access)	800		800			800	-	
General Ledger Review	600		300	300		600	-	Adjusted to start later in FY 2022 to better allocate available resources. As a result, anticipate the project to carryover to FY 2023.
Hosted Systems Review - Administration	1,000	400	300		700	1,400	400	Adjusted FY 2021 to reflect actual experience and carry over of hours to FY 2022. Anticipate similar duration for the next cycle due to merge with Hosted Systems - Investments project.
Hosted Systems Review - Investments	600			-		-	(600)	Adjusted to merge Hosted Systems - Investments project into the next cycling of the Hosted Systems - Administration project. Both follow same process, resulting in a net budgetary savings across the two projects.
Investment Decision Systems Review	600			600		600	-	
Logical and Physical Access Review (RAMS and Physical Access Infrastructure Systems)	700			700		700	-	
myVRS Review	500		500			500	-	
VNAV and Related Systems Review	1,600	500	250		600	1,350	(250)	Adjusted FY 2021 to reflect actual experience and carry over of hours to FY 2022. Planned initiation within a similar timeframe in FY 2024 with completion by October 2024.
VRS Public Website Review	1,000	-			-	-	(1,000)	Project deferred for consideration in a later period as the risk profile for the audit area has changed.
OTHER AUDIT REPORTING AND SUPPORT								
Other Reporting								
Audit Quality Assurance Improvement Program	600	150	150	150	150	600	-	
Audit Quality Assurance Review - External (1 every 5 years)	10				10	10	-	
Audit Recommendation Follow-Up System Annual Review	600	150	150	150	150	600	-	
Audit Recommendation Follow-Up System Quarterly Monitoring	100	25	25	25	25	100	-	
Modernization Program Monitoring	200	280	60			340	140	Modernization Phase Four project schedule extended. Adjusted to include final reporting of the Modernization Program.
Report on Fraud, Waste and Abuse Hotline Cases	300	75	75	75	75	300	-	
Review of Investment Incentive Compensation Plan	300	75	75	75	75	300	-	
Review Results of Agency Performance Outcomes (APOs)	300	75	75	75	75	300	-	
Verification of Cost of Living Adjustments (COLAs)	80	20	20	20	20	80	-	

Virginia Retirement System

Approved Long-Range Plan FY2021 - FY2024 - Progress and Adjustments as of June 30, 2021

Approved Projects	Approved Total Budgeted Hours	Actual	Approved Budgets			Total		
		FY2021	FY2022	FY2023	FY2024			
OTHER AUDIT REPORTING AND SUPPORT, Continued								
Audit Support								
Coordination with the APA	160	40	40	40	40	160	-	
Data Analytics and Support	3,600	900	900	900	900	3,600	-	
Develop and Update Annual and Long-Range Plans	600	125	125	125	225	600	-	
Monitor Annual and Long-Range Plan Progress	400	100	100	100	100	400	-	
Audit and Compliance Committee Support								
Review, Compile and Publish Meeting Materials	1,200	300	300	300	300	1,200	-	
Attend Audit and Compliance Meetings	320	80	80	80	80	320	-	
Prepare Committee Report and Meeting Minutes	320	80	80	80	80	320	-	
ONGOING ACTIVITIES								
Risk Monitoring Activities								
Attend Board and other Committee Meetings	680	170	170	170	170	680	-	
Attend Executive Team Meetings (DEC, Roadmap, C-suite)	400	100	100	100	100	400	-	
Monitor and Review Professional Literature	360	90	90	90	90	360	-	
Participate in Professional Organizations (APPFA, IIA, ISACA, Tableau User Groups)	360	90	90	90	90	360	-	
Other Administrative Activities								
Continuing Professional Education	1,440	360	360	360	360	1,440	-	
Continuing Professional Education Administration	600	150	150	150	150	600	-	
External Reporting and Other Interactions (OSIG/VITA)	40	10	10	10	10	40	-	
Internal Audit Staff Meetings and Mentoring	1,200	300	300	300	300	1,200	-	
Manage Budget, Departmental Files, SPCC, and Purchasing	400	100	100	100	100	400	-	
Participate in VRS Events/Committees	600	150	150	150	150	600	-	
Performance Standards and Evaluations	240	60	60	60	60	240	-	
OTHER TIME								
Annual Leave	3,000	900	850	850	800	3,400	400	Adjusted to reflect actual staff leave trends given tenure.
Holidays	2,496	696	648	600	600	2,544	48	
Other Leave (Sick, Personal, Volunteer, etc)	2,640	850	660	660	660	2,830	190	
Unplanned Hours	4,524	1,229	1,687	1,245	735	4,896	372	Adjusted based on other adjustments and to accommodate certain strategic initiatives.
TOTAL TIME	**49,920**	**12,480**	**12,480**	**12,480**	**12,480**	**49,920**		

Virginia Retirement System

Approved Long-Range Plan FY2021 - FY2024 - Progress and Adjustments as of June 30, 2021

Legend - See explanatory notes provided in the "Comments" column.

Project complete.

Project "In Progress" at fiscal year end. Will require carry over hours in the next annual plan to be completed.

Project deferred.

Proposed project hours adjusted.

Other Notes:

[1] These approved projects are subject to VITA's mandated 3-year audit cycle. Therefore, projects scheduled in FY 2021 will be repeated in FY 2024, unless their VITA reported risk assessment is changed during the annual IT risk assessment update process.

Acronyms not Described Elsewhere:

APA - Auditor of Public Accounts

APPFA - Association of Public Pension Fund Auditors

ARFUS - Audit Recommendation Follow-Up System

C-suite - Chief Executives for VRS, including the Executive Director and Chief Investment Officer

DEC - Director's Executive Committee

IIA - Institute of Internal Auditors

ISACA - Information Systems Audit and Control Association

IT - Information Technology

myVRS - web-based portal for members developed through the Modernization program

OSIG - Office of the State Inspector General

Roadmap - program management tool used by VRS management to monitor critical organizational activities

SPCC - Small Purchase Charge Card

VITA - Virginia Information Technologies Agency

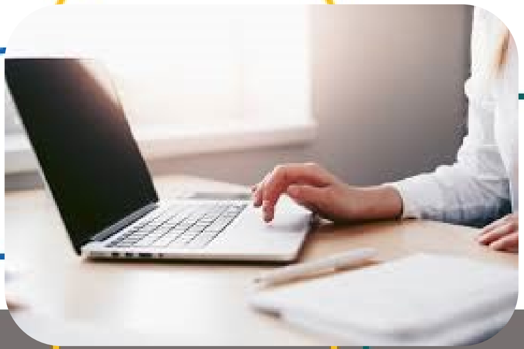
VNAV - myVRS Navigator, administrative system developed through the Modernization program

Proposed

FY 2022 Annual Plan

Virginia Retirement System

Internal Audit Proposed FY 2022 Annual Plan



Virginia Retirement System

Proposed FY 2022 Annual Plan

Approved Projects	Original FY 2022 Budget	FY 2021 Plan Carry Over	Other Proposed Changes	Proposed FY 2022 Plan
RISK BASED PROJECTS				
Carry Over from Prior Annual Plan [1]				
Retiree Payroll - Processing and Changes	-	600		600
Hosted Systems Review - Administration	-	300		300
VNAV and Related Systems Review	-	250		250
Investments				
Fixed Income Program and Securities Lending	600			600
Benefits				
Disability Retirements [2]	-		700	700
Long-Term Care Program [2]	400		(400)	-
Refunds [2]	800		(800)	-
Retirement Application Processing [2]	800		(800)	-
Operations				
Cash Assets and Cash Management (Administration and Investments)	600			600
Procurement and Contract Management (Administration and Investments) [2]	200		(200)	-
Information Technology				
Conformance of VRS Information Security Program with VITA Standards	150			150
General Controls Review over VRS' Operating Environment (Infrastructure Systems, excluding Physical Access)	800			800
General Ledger Review [3]	600		(300)	300
myVRS Review	500			500
OTHER AUDIT REPORTING AND SUPPORT				
Other Reporting				
Audit Quality Assurance Improvement Program	150			150
Audit Recommendation Follow-Up System Annual Review	150			150
Audit Recommendation Follow-Up System Quarterly Monitoring	25			25
Modernization Program Monitoring [4]	-		60	60
Report on Fraud, Waste and Abuse Hotline Cases	75			75
Review of Investment Incentive Compensation Plan	75			75
Review Results of Agency Performance Outcomes (APOs)	75			75
Verification of Cost of Living Adjustments (COLAs)	20			20

Virginia Retirement System

Proposed FY 2022 Annual Plan

Approved Projects	Original FY 2022 Budget	FY 2021 Plan Carry Over	Other Proposed Changes	Proposed FY 2022 Plan
OTHER AUDIT REPORTING AND SUPPORT, Continued				
Audit Support				
Coordination with the APA	40			40
Data Analytics and Support	900			900
Develop and Update Annual and Long-Range Plans	125			125
Monitor Annual and Long-Range Plan Progress	100			100
Audit and Compliance Committee Support				
Review, Compile and Publish Meeting Materials	300			300
Attend Audit and Compliance Meetings	80			80
Prepare Committee Report and Meeting Minutes	80			80
ONGOING ACTIVITIES				
Risk Monitoring Activities				
Attend Board and other Committee Meetings	170			170
Attend Executive Team Meetings (DEC, Roadmap, C-suite)	100			100
Monitor and Review Professional Literature	90			90
Participate in Professional Organizations (APPFA, IIA, ISACA, Tableau User Groups)	90			90
Other Administrative Activities				
Continuing Professional Education	360			360
Continuing Professional Education Administration	150			150
External Reporting and Other Interactions (OSIG/VITA)	10			10
Internal Audit Staff Meetings and Mentoring	300			300
Manage Budget, Departmental Files, SPCC, and Purchasing	100			100
Participate in VRS Events/Committees	150			150
Performance Standards and Evaluations	60			60
OTHER TIME				
Annual Leave [5]	750		100	850
Holidays	648			648
Other Leave (Sick, Personal, Volunteer, etc)	660			660
Unplanned Hours [6]	1,197		490	1,687
TOTAL TIME	**12,480**	**1,150**	**(1,150)**	**12,480**

Virginia Retirement System

Proposed FY 2022 Annual Plan

Notes:

(1) Due to unforeseen circumstances impacting the timing of work, certain audit projects will initiate in one fiscal year and be reported out in the next fiscal year. Typically they are reported out at the September Audit and Compliance Committee meeting. These projects are identified as a part of planning for the upcoming fiscal year annual audit plan and their impact is considered when determining the extent of available resources.

(2) As noted in the FY 2021 – 2024 Long-Range Plan Progress report, these projects have been moved to accommodate adjustments in IT and other project timing and appropriately consider operational needs.

(3) As noted in the FY 2021 – 2024 Long-Range Plan Progress report, this project is being adjusted to start later in FY 2022 to better allocate available resources and appropriately consider operational needs. As a result, hours will carry over to FY 2023.

(4) The Modernization Phase Four project schedule was extended to the end of FY 2021. As a result, these hours are proposed to accommodate the final reporting on the Modernization Program.

(5) Given the maturity of the Internal Audit Department staff, the use of annual leave balances have trended higher than originally budgeted. This is to acknowledge the actual behavior.

(6) Proposed increase in unplanned hours to accommodate development of information technology staff augmentation approach and other strategic initiatives.

Acronyms not Described Elsewhere:

APPFA	Association of Public Pension Fund Auditors
C-suite	Chief Executives for VRS, including the Executive Director, Chief Investment Officer and Internal Audit Director
DEC	Director's Executive Committee
IIA	Institute of Internal Auditors
ISACA	Information Systems Audit and Control Association
myVRS	Web-based portal for members developed through the Modernization Program
OSIG	Office of the State Inspector General
Roadmap	Program management tool used by VRS management to monitor critical organizational activities
SPCC	Small Purchase Charge Card
VITA	Virginia Information Technologies Agency
VNAV	myVRS Navigator, administrative system developed through the Modernization Program

Virginia Retirement System

Request for Board Action
RBA 2021-09-____

Approval of FY2022 Annual Audit Plan.

Requested Action

The VRS Board of Trustees approves the proposed FY2022 Annual Audit Plan.

Description/Background

The Audit Director has developed a comprehensive risk assessment process to identify and prioritize the work of the Internal Audit Department in line with organizational and operational risk priorities of the Board of Trustees and VRS management. The process is applied against a universe of potential audit projects within the limitations created by the available audit resources and results in the creation of a Long-Range four-year audit plan.

Annually the Audit Director looks to the guidance provided by the Long-Range plan and develops the Annual Audit plan. FY 2022 is the second year in the Long-Range plan, as a result certain adjustments have been proposed based on the changing risk environment within the organization.

Rationale for Requested Action

The proposed Annual Audit Plan, derived from the approved Long-Range plan is brought forward annually for Board consideration and approval, ensuring the work of the Internal Audit Department remains in alignment with organizational and operational risk priorities.

Authority for Requested Action

Section V.C.6 of the VRS Board of Trustees' Governance Policy delegates the responsibility of developing a comprehensive annual audit plan to the Audit Director and providing that plan to the Audit and Compliance Committee and the Board of Trustees for review and approval.

The above action is approved.

______________________________________ ______________________________

O'Kelly E. McWilliams, III, Chair Date
VRS Board of Trustees

Page 1 of 1
September 21, 2021

Quarterly Report on Fraud, Waste and Abuse Hotline Cases

Virginia Retirement System

INTERNAL AUDIT

Report of Alleged Fraud, Waste and Abuse Hotline Cases

For Complaints Received During the Period May 1, 2021 through July 31, 2021

SUMMARY OF CASES REVIEWED AND CLOSED

During the period May 1, 2021 through July 31, 2021, we received no cases of potential Fraud, Waste and Abuse from the Office of the State Inspector General.

Background

Fraud, Waste and Abuse relating to VRS can be comprised of any number of concerns. Such items can be reported to VRS' Internal Audit Department directly or through the Office of the State Inspector General (OSIG) State Employee Fraud, Waste and Abuse Hotline. (A majority of complaints are received through OSIG.)

All matters that relate to Fraud, Waste and/or Abuse reported are reviewed to determine the proper protocol for investigation.

Committee Reporting

Cases of a serious and/or significant nature will be reported to the VRS Audit and Compliance Committee immediately. At a minimum, a summary of all Hotline cases will be reported to the Audit and Compliance Committee on a quarterly basis.

Retention

Hardcopy documents, including hand-written notes, are stored in a secure location until the case is closed, upon which they are shredded. Electronic files are stored on Internal Audit's secured drive. Documentation containing case details are labeled "***CONFIDENTIAL – STATE FRAUD, WASTE AND ABUSE HOTLINE DOCUMENTS***" and sensitive items are labeled FOIA Exempt. As appropriate, files are disposed of in accordance with the Library of Virginia's retention policy.

FRAUD, WASTE AND ABUSE CASE MANAGEMENT

PROCESSING OF COMPLAINTS

When received, the Audit Director and Hotline Auditor perform a preliminary review of the complaint. After initial discussion, the Hotline Auditor determines whether a formal response is required by OSIG (cases referred by OSIG may or may not require a formal response, depending on the nature of the complaint) and adds the case to Internal Audit's Hotline Tracking System.

The Hotline Auditor sets up a case file on Internal Audit's secured and restricted drive to maintain confidentiality. The Hotline Auditor then evaluates the case details and may review information available in VRS' systems to obtain further details about the subject of the complaint. Additionally, the Hotline Auditor may forward the details of the case to other VRS personnel for review. The Hotline Auditor also notifies the VRS Director of the case.

Complaints regarding disability benefits constitute the large majority of the Hotline cases received by VRS. The Hotline Auditor will meet with appropriate VRS staff, as necessary, to discuss details of the case in order for all parties to proceed forward with their portion of the investigation. Complaints forwarded to others are monitored for resolution. Actions and determinations for cases are reviewed for reasonableness by the Hotline Auditor. Once a determination of appropriate action has occurred, such action is documented in the Internal Audit case file and on the Hotline Tracking System. The Internal Audit Director is apprised of all actions and determinations.

For other complaints, such as internal fraud, waste or abuse (examples could include abuses of various types of leave, teleworking policies, employee theft, etc.), the Hotline Auditor investigates the allegation and obtains supporting documentation from management, as needed. If a determination is made that there is a reasonable possibility of fraud, waste or abuse, management is notified of the allegation by the Audit Director and given a reasonable timeframe in which to report back to the Audit Director any actions taken regarding the allegation. The Audit Director determines the reasonableness of such action, reports the actions and resolution of the complaint to the Hotline Auditor who documents the results in the case file and on the Hotline Tracking System.

All investigation results are reported to the VRS Director and members of the VRS Audit and Compliance Committee once a case is resolved, regardless of the outcome.

Miscellaneous Updates

Virginia
Retirement
System

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

Patricia S. Bishop
Director

MEMORANDUM

To: Jennifer P. Schreck, Internal Audit Director

From: Patricia S. Bishop, Director

Date: September 1, 2021

Subject: Summary of Travel Related Expenses

I am attaching the following:

1. Summary of Travel Related Expenses Paid During the Quarter of and Fiscal Year-to-Date Through June 30, 2021.

2. Summary of Other Sponsored Travel Related Expenses Paid During the Quarter of and Fiscal Year-to-Date Through June 30, 2021. Because of the COVID-19 travel restrictions, there was no reportable Other Sponsored Travel Related Expenses for the period.

3. Schedule of Selected Travel Related Expenses Paid During the Quarter of and Fiscal Year-to-Date Through June 30, 2021.

4. Record of Attendance and Per Diems for the Quarter Ended June 30, 2021.

This information should be shared with the Audit & Compliance Committee.

If you have any questions, please do not hesitate to ask.

PSB/lbk

Attachments

Schedule of Selected Travel Related Expenses
(Board and Committee Members, VRS Executive Staff, and VRS Professional Investment Staff)
Paid During the Quarter Ended June 2021

Name of Traveler	Voucher Number	Date(s) of Travel	Location	Sponsor	Purpose	Sponsor Provided	VRS Provided	Total
Board and Committee Members								
Staff								
Coleman, Thomas J.	102909	6/1/21	Washington, DC		Due Diligence for Pritzker	-	143.32	143.32
Totals						**-**	**143.32**	**143.32**

Virginia Retirement System
Summary of Other Sponsored Travel Related Expenses
(Staff Not Otherwise Includable in Quarterly Reporting)
Fiscal Year-To-Date Through June 2021

	Current Quarter		Fiscal Year-To-Date	
Name of Traveler	Value Provided	Sponsor	Value Provided	Sponsor
	-		-	
Totals	-		-	

Virginia Retirement System
Summary of Travel Related Expenses
(Board and Committee Members, VRS Executive Staff, and VRS Professional Investment Staff)
Fiscal Year-To-Date Through June 2021

	Current Quarter Costs											Fiscal Year-To-Date Prior Report					Fiscal Year-To-Date				
	Total Travel Expenses			Out of State Travel								Total Travel Expenses			Out of State Travel		Total Travel Expenses			Out of State Travel	
						Purpose															
Name of Traveler	Sponsor Provided	VRS Provided	Total	Number of Trips	Cost	Due Diligence	Conference	Advisory/Assoc Mtg	Mger Mtg	Site Visit	Training	Sponsor Provided	VRS Provided	Total	Number of Trips	Cost	Sponsor Provided	VRS Provided	Total	No. of Trips	Cost
Board of Trustees & Committee Members																					
Staff																					
Bishop, Patricia S.	-	-	-									-	-	-	-	-	-	87.03	87.03	-	-
Coleman, Thomas J.	-	143.32	143.32	-	-							-	-	-	-	-	-	143.32	143.32	-	-
Totals	**-**	**143.32**	**143.32**	**-**	**-**							**-**	**-**	**-**	**-**	**-**	**-**	**230.35**	**230.35**	**-**	**-**

VRS BOARD OF TRUSTEES AND COMMITTEES
RECORD OF ATTENDANCE & PER DIEMS
FOR 2Q2021

	Month Paid:	Apr-21						Jun-21				Total Days Attended	Per Diem Rate	Per Diem Payments			Total
		3/24/21	4/14/21	4/15/21	4/19/21	4/19/21	4/20/21	6/2/21	6/3/21	6/9/21	6/10/21			April	May	June	
Member	Area	IPC	IAC	DCPAC	A&P	B&A	BOT	A&P	A&C	B&A	BOT						
J BRANDON BELL, II	BOT	X	X	X	-	X	X	X	X	X	X	9	$ 300.00	$ 1,500.00	$ -	$ 1,200.00	$ 2,700.00
JOHN M. BENNETT	BOT	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	X	X	X	X	4	300.00	-	-	1,200.00	1,200.00
MICHAEL P. DISHAROON	BOT	X	X	X	-	X	X	-	-	X	X	7	300.00	1,500.00	-	600.00	2,100.00
WILLIAM A. GARRETT	BOT	X	X	X	X	X	X	X	X	X	X	9	300.00	1,500.00	-	1,200.00	2,700.00
SUSAN GOODEN	BOT	-	-	X	-	-	X	-	-	-	X	3	300.00	600.00	-	300.00	900.00
WALLACE G. HARRIS	BOT	X	X	-	X	X	X	[redacted]	[redacted]	[redacted]	[redacted]	4	300.00	1,200.00	-	-	1,200.00
W. BRETT HAYES	BOT	X	X	-	-	-	X	X	X	-	X	6	300.00	900.00	-	900.00	1,800.00
O'KELLY E. MCWILLIAMS, III	BOT	X	X	X	X	X	X	X	-	X	X	8	300.00	1,500.00	-	900.00	2,400.00
JOSEPH W. MONTGOMERY	BOT	X	X	-	X	X	X	X	X	X	X	8	300.00	1,200.00	-	1,200.00	2,400.00
TROILEN G. SEWARD	BOT	X	X	-	X	X	X	X	X	X	X	8	300.00	1,200.00	-	1,200.00	2,400.00
RIVINDRA DEO	DCPAC	-	-	X	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
SHANNON T. IRVIN	DCPAC	-	-	X	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
RICK LARSON	DCPAC	-	-	X	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
BRENDA O. MADDEN	DCPAC	-	-	X	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
KATHERINE T. SEAY (2)	DCPAC	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
DAVID A. WINTER	DCPAC	-	-	X	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
DEBORAH ALLEN-HEWITT	IAC	-	X	-	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
MICHAEL R. BEASLEY	IAC	-	X	-	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
THEODORE ECONOMOU (1)	IAC	-	X	-	-	-	-	-	-	-	-	1	-	-	-	-	-
THOMAS S.GAYNER	IAC	-	-	-	-	-	-	-	-	-	-	-	300.00	-	-	-	-
LAWRENCE E KOCHARD	IAC	-	X	-	-	-	X	-	-	-	-	2	300.00	600.00	-	-	600.00
NANCY G. LEAKE	IAC	-	X	-	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
WILBERT BRYAN LEWIS	IAC	-	X	-	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
ROD SMYTH	IAC	-	X	-	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
WILLIAM H. WEST	IAC	-	X	-	-	-	-	-	-	-	-	1	300.00	300.00	-	-	300.00
														$15,000.00	$ -	$ 8,700.00	$23,700.00
Number Attending		8	16	10	5	7	10	7	6	7	9						
Total Days per Diem Paid (Control Total)		8	15	10	5	2	10	7	6	7	9	79	x $300			=	23,700.00

(1) This individual waived the payment of stipend and per diem payments for meetings attended effective 8/2/15.
(2) This individual waived the payment of per diem payments for meetings attended.

X = Present

Virginia
Retirement
System

P.O. Box 2500, Richmond, Virginia 23218-2500
Toll-free: 1-888-VARETIR (827-3847)
Website: www.varetire.org

Date: September 1, 2021

To: Trish Bishop, Director

From: Jennifer Schreck, Internal Audit Director

Subject: Review of 2021 Agency Performance Outcomes and Operational Measures

As part of our annual process, Internal Audit has reviewed the status of the 2021 Agency Performance Outcomes (APOs) and Operational Measures (OMs), as set forth by management for the fiscal year ended June 30, 2021. The purpose of our review was to obtain reasonable, but not absolute assurance that the status of such outcomes and measures was fairly represented in management's status reports.

Based upon our review of available documentation and discussions with various VRS personnel, nothing came to our attention to cause us to question the representations set forth by management with respect to either the APOs or the OMs. Accordingly, we have no reason to believe that the APOs and OMs were not appropriately represented as satisfied for the fiscal year ended June 30, 2021.

I would like to commend the management team and staff for their accomplishments this past year. Please feel free to share this information with the Administration and Personnel Committee as well as the full Board of Trustees, as you deem appropriate.

Virginia
Retirement
System

P.O. Box 2500, Richmond, Virginia 23218-2500
Toll-free: 1-888-VARETIR (827-3847)
Website: www.varetire.org

Date: September 7, 2021

To: Paula Reid, Director of Human Resources

CC: Trish Bishop, Director
Ron Schmitz, Chief Investment Officer

From: Jennifer Schreck, Internal Audit Director
Joshua Fox, Principal Auditor

Subject: **Review of FY2021 Investment Incentive Compensation**

Internal Audit has reviewed the proposed Investment Incentive Compensation for the fiscal year ended June 30, 2021. The Investment Incentive Compensation amount, in aggregate, is **$7,853,280.10,** where a qualitative multiplier of **1.0** is used for the Chief Investment Officer. We found this aggregate amount, as well as the proposed payment amounts, were accurately computed in accordance with the Investment Professionals' Pay Program, effective June 10, 2021.

Please share this information with the Administration and Personnel Committee as well as the Board of Trustees, as you deem appropriate.

2022 Confirmed VRS Board and Committee Meeting Dates

	Board of Trustees	Audit and Compliance Committee	Administration and Personnel Committee	Benefits and Actuarial Committee	Defined Contribution Plans Advisory Committee	Investment Advisory Committee
February	Thursday Feb 10th @ 1 pm		Tuesday Feb 8th @ 1 pm	Wednesday Feb 9th @ 1 pm		
March		**Tuesday Mar 29th @ 2 pm**				
April	Tuesday Apr 19th @ 1 pm					Wednesday Apr 13th @ 10 am
May (Retreat)	Wednesday May 25th @ TBD					
June	Thursday Jun 23rd @ 1 pm	**Thursday Jun 16th @ 2 pm**	Tuesday Jun 14th @ 1 pm	Monday Jun 6th @ 1 pm		
July	Thursday Jul 14th @ 1 pm					
August						Thursday Aug 18th @ 10 am
September	Thursday Sept 22nd @ 1 pm	**Tuesday Sept 13th @ 2 pm**	Wednesday Sept 14th @ 1 pm			
October	Tuesday Oct 18th @ 1 pm			Monday Oct 17th @ 1 pm		
November	Tuesday Nov 15th @ 1 pm			Monday Nov 14th @ 1 pm		Wednesday Nov 30th @ 10 am
December	Thursday Dec 8th @ 1 pm	**Thursday Dec 8th @ 10 am**				

Closed Session

REVIEW OF AUDIT DIRECTOR'S PERFORMANCE

In accordance with the Freedom of Information Act, the Committee will need to go into closed session to discuss the performance of the Audit Director. The necessary wording to convene and certify a closed session is provided below.

Any recommendations agreed to by the Committee during the closed session must be voted upon and approved in open session to be communicated to the Board.

To Convene Closed Meeting

"I move that the Audit and Compliance Committee of the Virginia Retirement System Board of Trustees convene a closed meeting under the Virginia Freedom of Information Act to evaluate the performance of the current Internal Audit Director pursuant to the personnel exemption at *Code of Virginia* § 2.2-3711(A)(1)."

[**Second needed]**
[**Roll call vote needed**]

Certification after Closed Meeting

"I move the following resolution:

WHEREAS, the Audit and Compliance Committee of the Virginia Retirement System Board of Trustees convened a closed meeting on this date pursuant to an affirmative recorded vote and in accordance with the provisions of the Virginia Freedom of Information Act; and

WHEREAS, *Code of Virginia* § 2.2-3712 requires a certification by this Committee that such closed meeting was conducted in conformity with Virginia law;

NOW, THEREFORE, BE IT RESOLVED, that the Committee certifies that, to the best of each member's knowledge, (i) only public business matters lawfully exempted from open meeting requirements under this chapter were discussed in the closed meeting to which this certification resolution applies, and (ii) only such public business matters as were identified in the motion by which the closed meeting was convened were heard, discussed or considered by the Committee."

[**Second needed]**
[**Roll call vote needed**]

Authority

Per its Charter, the Committee is charged with reviewing and making recommendations to the Board regarding the performance of the Audit Director. The Committee typically conducts such a review at its September meeting, supported by the Human Resources Director.

Results

The various Internal Audit Annual Progress Reports presented in today's meeting book highlight the Department's and Audit Director's activities for the year under review.

Executive Pay Plan

The Audit Director falls under the Board approved Executive Pay Plan which provides guidelines regarding the annual salary and bonus amounts provided to the three positions reporting directly to the Board.

The Audit Director's compensation components include a base salary, which falls within the established pay range of the Administrative Pay plan and may be adjusted based on market study findings; supplemental pay, as determined by the Board; performance bonus, and gainsharing.

Virginia Retirement System

Request for Board Action
RBA 2021-09-____

Approve a __% performance bonus for the Audit Director.

Requested Action

The VRS Board of Trustees approves a ___% performance bonus for the Audit Director.

Description/Background

The Audit and Compliance Committee reviewed and evaluated the performance of the Audit Director. Based on this review and evaluation, the Committee recommends that the Board approve a ___% performance bonus for the Audit Director payable ___________ ___, 2021.

Rationale for Requested Action

The Audit and Compliance Committee recommends that the Board approve a ___% performance bonus for the Audit Director, payable ___________ ___, 2021, based on the Committee's review and evaluation of the Audit Director's performance during FY 2021. The Audit and Compliance Committee Charter, in paragraph 8 of the duties and responsibilities section states, "Review and evaluate the performance of the Audit Director in all areas for which he or she is responsible and report the results and conclusions to the Board." Section IV. H.(8) of the Board Governance Policy provides that the Board may review, monitor, and oversee the performance of the Audit Director. Also, the Executive Pay Plan contemplates granting a performance bonus to the Audit Director.

Authority for Requested Action

Code of Virginia § 51.1-124.22(11) authorizes the Board to establish and administer a compensation plan for officers and employees of the Retirement System.

The above action is approved.

____ __________________________________

O'Kelly E. McWilliams, III, Chair
VRS Board of Trustees

Date