


DEPARTMENT OF PLANNING AND BUDGET

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2025

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the statewide budget and appropriation processing controls at the Department of Planning and Budget (Planning and Budget) for the year ended June 30, 2025. Our audit found:

- proper recording and reporting of financial and budget transactions, in all material respects and in accordance with the budget approved by the General Assembly, in the Commonwealth's accounting and reporting system and in the Commonwealth's budgeting system;

- two matters involving internal control and its operation requiring management's attention, that also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards.

This report includes two risk alerts that require the action and cooperation of management at Planning and Budget and the Virginia Information Technologies Agency (VITA) regarding risks related to access to centralized audit log information and timely security audits.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendation.

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve IT Risk Management and Contingency Planning Documentation
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Department of Planning and Budget (Planning and Budget) does not conduct some aspects of its information technology (IT) risk management and contingency planning documentation in accordance with the Commonwealth's Information Security Standard, SEC530 (Security Standard). IT risk management and contingency planning documentation identifies and analyzes the sensitivity and risks of Planning and Budget's data, as well as plans to support its business functions and recover IT systems when they become unavailable. Risk management documents include Planning and Budget's Business Impact Analysis (BIA), IT System and Data Sensitivity Classifications (Sensitivity Classifications), IT System Risk Assessments (RA), and System Security Plans (SSP). Contingency planning documents include Planning and Budget's Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP).

Specifically, Planning and Budget does not perform the following:

- Planning and Budget does not perform an annual review of user access to the COOP's storage location to protect IT contingency planning documentation from unauthorized disclosure or modification. The Security Standard requires Planning and Budget to protect the contingency plan from unauthorized disclosure and modification. The Security Standard also requires Planning and Budget to employ least privilege to allow only authorized access for users necessary to accomplish assigned organizational tasks and to review account access on an annual basis and following an environmental change. Without protecting contingency planning documentation from unauthorized disclosure or modification, Planning and Budget increases the risk for unauthorized changes and inaccurate incident response procedures in its COOP and DRP.

- Planning and Budget does not include current system boundary diagrams within its SSPs. The SSP Policy and Security Standard require Planning and Budget to develop an SSP for the information system that describes the operational context of the system. Without current information documented in the SSP, Planning and Budget increases the risk that it will not effectively identify all potential risks and implement security controls needed to protect its sensitive system environment.

Planning and Budget's lack of access review contributed to the oversight in identifying and removing access from those who no longer need access to the COOP's storage location. Additionally, management oversight led to Planning and Budget not including current system boundary diagrams to the SSPs.

Planning and Budget should protect its IT contingency planning documentation by reviewing accounts with access to the COOP storage location and enforcing the principle of least privilege.

Additionally, Planning and Budget should improve its SSP documentation to include current information about each system's operational environment. Taking these corrective actions will help maintain the confidentiality, integrity, and availability of Planning and Budget's sensitive and mission-critical data.

Improve Security Awareness Training Program

Type: Internal Control and Compliance
Severity: Significant Deficiency

Planning and Budget does not administer its security awareness training program in accordance with its IT Security Awareness and Training Policy (Security Awareness Policy), the Security Standard, and the Commonwealth's Security Awareness Training Standard, SEC527 (Security Awareness Training Standard). An established security awareness training program is essential to protecting agency IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the agency. Specifically, the following weaknesses exist with Planning and Budget's security awareness training program:

- Planning and Budget does not provide security awareness training to all contractors with access to its IT systems. Planning and Budget's Security Awareness Policy requires that the agency provide security awareness training to all business partners within the first 30 days of commencing work and repeat the training at least annually afterward. Without ensuring contractors complete security awareness training, Planning and Budget increases the risk that the contractors are not aware of the specific requirements for its IT environment. Additionally, the contractors may be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

- Planning and Budget does not provide role-based training to one contractor designated as a data custodian. Planning and Budget's Security Awareness Policy states the Information Security Officer (ISO) shall identify opportunities to create the appropriate role-based information security training materials and communicate the training opportunities to those with security roles and responsibilities. Additionally, it states managers will ensure that employees and business partners who manage, administer, operate, or design IT systems receive additional role-based information security training. The lack of adequate role-based training increases the risk that users will be unaware or unequipped to perform their assigned security-related functions, resulting in an increased data security risk.

- Planning and Budget does not monitor and enforce employee compliance to ensure each user completes security awareness training as required. As a result, two out of 58 (3%) employees assigned to security awareness training did not complete training by the required deadline. Planning and Budget's Security Awareness Policy designates the ISO to coordinate, monitor, and track the completion of the security awareness training for all Planning and Budget employees and business partners and report incomplete training to the Planning and Budget Director. Additionally, the Security Awareness Policy states the ISO or designee may revoke account rights until mandatory security awareness training is completed. Without a process to consistently monitor and enforce users to complete security awareness training by the

required deadline, Planning and Budget increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data.

- Planning and Budget does not submit its security awareness training plans and compliance information to the Virginia Information Technologies Agency (VITA) by the end of February annually as required by the Security Awareness Training Standard. By not ensuring the required information is submitted annually, Planning and Budget may not receive approval for its upcoming training plan nor confirm its security awareness training program's compliance with the Commonwealth's security standards.

Planning and Budget's staffing constraints prevented it from monitoring and enforcing its users to complete training as required. Furthermore, management oversight resulted in Planning and Budget not submitting its security awareness training plan and compliance certification to VITA.

Planning and Budget should procure training platform accounts for its contractors to receive security awareness and role-based training as required by its Security Awareness Policy and the Security Standard. If procuring accounts for its contractors is not feasible, Planning and Budget should develop and document other compensating controls to ensure its contractors receive the necessary security awareness and role-based training. Additionally, Planning and Budget should monitor and enforce its training program to ensure all users complete the required training by the deadline in accordance with its Security Awareness Policy, the Security Standard, and Security Awareness Training Standard. Further, Planning and Budget should ensure it submits its security awareness training plans and compliance information to VITA by the annual deadline. Improving the security awareness training program will help protect the agency from malicious attempts to compromise confidentiality, integrity, and availability of sensitive information.

RISK ALERTS

During the course of our audit, we encountered two issues that are beyond the corrective action of Planning and Budget's management alone and require the action and cooperation of management and VITA. The following issues represent such a risk to Planning and Budget and the Commonwealth.

Access to Central Audit Log Information

First Reported: Fiscal Year 2023

Planning and Budget relies on the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As the ITISP contract administrator, VITA is responsible for providing agencies with access to its security information and event management (SIEM) tool that stores information about historical security events throughout these components that may affect Planning and Budget's IT environment.

VITA and the ITISP contractors implemented the current SIEM tool in October 2023 after several unsuccessful iterations since 2018. While the current SIEM tool stores audit logs for the ITISP infrastructure components, the SIEM tool does not present the information in a usable format that will allow agencies to adequately monitor their IT environments. Additionally, VITA does not configure the SIEM tool to give alerts about specific events captured in the audit logs. These alerts are necessary to provide Planning and Budget with timely notification of potentially anomalous or malicious activity.

The Security Standard requires agencies to review and analyze audit records at least every 30 days for indications of inappropriate or unusual activity and assess any potential impact of the inappropriate or unusual activity. Using a SIEM tool without all necessary audit log information displayed to agencies reduces organizational security posture by not being able to react to and investigate suspicious system activity in a timely manner.

Planning and Budget should continue to work with VITA to create relevant and usable information on the SIEM tool, including setting the appropriate alerts, to ensure Planning and Budget can review the activities occurring in its IT environment in accordance with the Security Standard. Our separate audit of VITA's contract management will also report this issue.

Timely Security Audits

Planning and Budget contracts with VITA to perform IT security audits over Planning and Budget's sensitive systems. Under the contract, VITA is to conduct IT security audits in compliance with the Commonwealth's IT Security Audit Standard, SEC502 (Security Audit Standard), which includes auditing systems to ensure compliance with applicable Commonwealth security standards within three years from the last audit completion date. Based on a review of Planning and Budget's IT audit plan and VITA's status or completion of Planning and Budget's security audits, VITA did not perform the audits within the Security Audit Standard's three-year requirement.

Not auditing sensitive IT systems every three years increases the risk for vulnerabilities, threats, and system misconfigurations to go undetected and delays Planning and Budget's ability to take remediating actions. In addition, having unaudited systems puts Planning and Budget at risk of malicious users exploiting vulnerabilities to possibly compromise sensitive information and potentially causing systems to become unavailable.

VITA performed the last security audits in calendar year 2022 and Planning and Budget renewed its contract for VITA's auditing service in 2023. However, due to VITA experiencing staffing shortages due to turnover during calendar year 2025, VITA did not conduct Planning and Budget's audits within three years from the completion date of its last IT security audits.

Planning and Budget should work with VITA to complete its system security audits within the required interval, which will assist Planning and Budget in identifying and remediating system vulnerabilities in a timely manner and reduce risks to Planning and Budget's IT environment. Additionally, our separate audit of VITA will report this issue.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Stephen E. Cummings
Secretary of Finance

Michael Maul
Director, Department of Planning and Budget

We have audited the financial records and operations of the **Department of Planning and Budget** (Planning and Budget) for the year ended June 30, 2025. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Comprehensive Financial Report audit. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of financial and budget transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia for the year ended June 30, 2025. In support of this objective, we evaluated the accuracy of recorded financial and budget transactions in the Commonwealth's accounting and financial reporting system and the Commonwealth's budgeting system; reviewed the adequacy of Planning and Budget's internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements. We also evaluated whether the budget approved by the General Assembly was appropriately recorded in the Commonwealth's accounting and financial reporting system and whether controls in this system are adequate to ensure program expenses do not exceed appropriations.

Audit Scope and Methodology

Planning and Budget's management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following processes and systems.

Budget execution
Commonwealth's budgeting system
Information security and general system controls (including access controls)

We performed audit tests to determine whether Planning and Budget's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of Planning and Budget's operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and, when appropriate, we projected our results to the population.

Our consideration of internal control over financial reporting (internal control) was for the limited purpose described in the section "Audit Objectives" and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve IT Risk Management and Contingency Planning Documentation" and "Improve Security Awareness Training Program," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a

timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Conclusions

We found that Planning and Budget properly stated, in all material respects, the financial and budget amounts recorded and reported in the Commonwealth's accounting and financial reporting system and the Commonwealth's budgeting system; and that the budget approved by the General Assembly is appropriately recorded in the Commonwealth's accounting and financial reporting system.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Internal Control and Compliance Findings and Recommendations."

Since the findings noted above include those that have been identified as significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards," which is included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2025. The Single Audit Report will be available at www.apa.virginia.gov in February 2026.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on December 17, 2025. Government Auditing Standards require the auditor to perform limited procedures on Planning and Budget's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." Planning and Budget's response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

This report is intended for the information and use of the Governor and General Assembly, Planning and Budget's management, and the citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

MBR/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Improve IT Risk Management and Contingency Planning Documentation	Ongoing	2025
Improve Security Awareness Training Program	Ongoing	2025

* A status of Ongoing indicates new and/or existing findings that require management's corrective action as of fiscal year end.

COMMONWEALTH *of* VIRGINIA
Department of Planning and Budget

MICHAEL D. MAUL
Director

1111 E. Broad
Street Room 5040
Richmond, VA 23219-1922

February 6, 2026

Ms. Staci A. Henshaw
Auditor of Public Accounts
James Monroe Building
101 N. 14th Street
Richmond, Virginia 23219

Dear Ms. Henshaw:

The Department of Planning and Budget (DPB) appreciates the opportunity to respond to the findings and recommendations contained in the 2025 audit report. DPB has reviewed the findings and recommendations provided by the Auditor of Public Accounts (APA) as part of its audit of financial records and operations for the fiscal year that ended on June 30, 2025. I offer the following response to the internal control and compliance findings and recommendations for DPB.

Internal Control and Compliance Findings and Recommendations

Improve IT Risk Management and Contingency Planning Documentation

DPB acknowledges the importance of risk management and contingency planning documentation. In response to this finding, DPB will annually review access to the storage locations of its Continuity of Operations Plan (COOP), applying the principle of least privilege. DPB will also update its System Security Plans (SSP) to include current system boundary diagrams.

Improve Security Awareness Training Program

DPB acknowledges the need to improve its Security Awareness Training Program. After this finding was shared with DPB, the department made internal policy changes, provided security awareness training to its contractors, and submitted security awareness training plans and compliance information to the Virginia Information Technology Agency (VITA). DPB also designated a backup Information Security Officer (ISO) to assist with administering its Security Awareness Training Program.

FAX (804) 225-3291 (804) 786-7455 TDD (804) 786-7578

Risk Alerts

DPB appreciates the Risk Alerts noted by the Auditor of Public Accounts. While beyond the corrective action of DPB, the department will continue to address with VITA its access to central audit log information. DPB is particularly concerned about timeliness of its audit, which it expected VITA to complete in the spring of 2025. VITA's Centralized IT Security Audit Services held the entrance conference with DPB on February 24, 2025; issued a draft report on November 24, 2025; and held the exit conference on December 2, 2025. The final report was not received until February 5, 2026.

DPB will use the findings and recommendations from the APA to continually improve its existing practices and policies. Thank you again for the opportunity to respond to your report.

Sincerely,

Michael D. Maul
Director

cc: The Honorable Mark D. Sickles
Secretary of Finance