

VIRGINIA ALCOHOLIC BEVERAGE CONTROL AUTHORITY

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 basic financial statements of the Virginia Alcoholic Beverage Control Authority (Authority) as of and for the year ended June 30, 2025, and issued our report thereon, dated December 2, 2025. Our report, included in the Authority's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the Authority's website at www.abc.virginia.gov. Our audit found:

- the financial statements are presented fairly, in all material respects;
- one internal control finding requiring management's attention; however, we do not consider it to be a material weakness;
- five additional 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; and
- adequate corrective action with respect to the prior audit finding identified as complete in the Findings Summary included in the Appendix.

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

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Internal Controls Over Employee Separation Process
Type: Internal Control
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

The Alcoholic Beverage Control Authority (Authority) does not have adequate internal controls over the completion of employee separation checklists or removal of systems access for terminated employees. During our review, we found the following deficiencies:

- For four out of 25 (16%) terminated employees, the Authority did not enter the termination date correctly in the Commonwealth's human resources and payroll system, resulting in variances of 30 to 50 days from the employees' personnel files;

- For 11 out of 25 (44%) terminated employees, the Authority did not enter the termination date timely in the Commonwealth's human resources and payroll system;

- For six out of 16 (37.5%) terminated employees, the employee separation checklist did not indicate a timely return of Authority property; and

- For six out of 25 (24%) terminated employees, the Authority did not remove systems access timely, resulting in delays between seven and 26 days past their termination dates.

The Authority's Employee Separation Policy (Separation Policy) states, "Supervisors will initiate a Payroll Action Notice (PAN) and separation checklist process on the same workday the employee is separated from the Authority, after the employee has left the premises. The standard time for Division Directors to complete the Employee Separation Checklist is five business days after the effective date of separation." The Authority's Separation Policy also states, "In cases of voluntary separation, each Division Director, in conjunction with the Director of Human Resource and CEO, may initiate immediate termination or restriction of an employee's computer access to Authority systems upon initial notification of an employee's intended separation date." The Authority's Human Resource Departments (Human Resources) failure to enter terminated employee information, complete Employee Separation Checklists, and remove systems access timely was caused by supervisors not timely initiating and submitting PANs. In addition, Human Resources entered the incorrect information from the PAN regarding the employees last day worked. By not completing these actions timely and accurately, the Authority risks making incorrect payments to terminated employees, employees not returning Authority property, and unauthorized access to critical systems.

Due to the Authority's unique structure, the Authority should define specific procedures for retail store employees, enforcement employees, and headquarter employees as access levels and risks are inherently different. Human Resources should also hold supervisors accountable for the timely

completion of employee checklists and removal of systems access, as well as ensure accurate information is entered into the system.

Conduct Information Security Assessments
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Authority does not define the frequency nor conduct regular assessments and audits of its information technology (IT) systems and environment. While the Authority's Information Security Program Management Policy (Security Policy) requires regular assessments and audits of its Information Security Program, it does not define a minimum frequency for the assessments and audits to be performed. The Authority has not conducted an IT security assessment or audit since calendar year 2023 and currently does not include plans to conduct IT security assessments or audits in its Internal Audit Plan.

The Authority's adopted information security standard, the National Institute of Standards and Technology Standard, 800-53 (NIST Standard) requires the Authority to assess the controls of its IT systems and environment at an organization-defined frequency to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements. In addition, the Authority's Security Policy states that its Internal Audit Division shall ensure regular assessments and audits of the Information Security Program are completed.

Without defining a frequency to perform assessments and audits, the Authority cannot ensure that assessments and audits are properly planned and executed. Not performing IT security assessments and audits increases the risk that the Authority will not detect and remediate potential weaknesses in its sensitive systems and environment in a timely manner. The Authority's lack of a defined frequency for conducting IT security assessments and audits, and significant turnover in its Internal Audit Division in the last year, led to the lapse in ensuring the Authority performs IT security assessments and audits.

The Authority should update its Security Policy to define a frequency requirement for performing IT security assessments and audits. The Authority should then develop a plan for conducting IT security assessments and audits in accordance with the defined requirement, and ensure completion of planned assessments and audits, either through its Internal Audit division or through the acquisition of external third-party services. Performing IT security assessments and audits will ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve IT Risk Management and Contingency Planning
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

The Authority has not remediated two of the five weaknesses identified in the prior year's audit relating to its IT Risk Management and Contingency Planning program. While the Authority completed corrective actions relating to its IT system and data sensitivity classification, tested its Continuity of Operations Plan, and conducted a full disaster recovery test, the following two weaknesses remain:

- The Authority does not have a complete System Security Plan (SSP) for any of its 16 sensitive systems as required by its Information Technology Risk Management Policy (Risk Management Policy) and the NIST Standard. The Security Policy requires the Authority to complete a SSP for all sensitive IT systems and perform an annual review for updates. Not having a SSP for each sensitive system could result in the Authority not properly identifying and mitigating risks, which could result in weaknesses exploited by bad actors and potentially compromise the Authority's sensitive information.

- The Authority does not have a completed risk assessment on record for four of its 16 (25%) sensitive systems. The Authority's Risk Management Policy requires the Authority to conduct a risk assessment for critical information systems and critical production applications at least once every three years. The Security Policy requires formal risk assessments of sensitive systems every three years, with informal risk assessments in other years. Without completing risk assessments for each sensitive system at least once every three years, the Authority may not identify potential risks in its sensitive systems, which increases the risk of not having mitigating controls in place to prevent a compromise of its sensitive data.

The Authority has experienced staffing shortages and resource limitations, causing delays in completing its corrective actions. The Authority should dedicate the necessary resources to complete corrective actions related to risk assessments and develop SSPs for systems it deems sensitive. Additionally, the Authority should perform annual reviews of the risk assessments and the SSPs to ensure that they are relevant and up to date. Completing SSPs and risk assessments will help ensure the Authority protects the confidentiality, integrity, and availability of its sensitive and mission critical systems and data.

Improve Virtual Private Network Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Authority does not require or implement certain security controls to its Virtual Private Network (VPN) in accordance with its internal policies and the NIST Standard. We identified seven control weaknesses and communicated them to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The NIST Standard requires the Authority to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the Authority's IT mission critical systems and data. A lack of oversight and monitoring led to the Authority not defining certain requirements in a policy and procedure and ensuring the VPN security controls and processes are implemented in accordance with its policies and the NIST Standard.

The Authority should obtain and dedicate the necessary resources to ensure that its VPN policies and procedures align with the NIST Standard requirements. The Authority should also implement the controls required to address the weaknesses identified in the FOIAE communication, which will help ensure the Authority protects the confidentiality, integrity, and availability of its sensitive and mission critical systems and data.

Continue Improving Oversight of Third-Party Service Providers
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2020

The Authority has made progress to develop and implement a formal and consistent process to oversee and manage its IT third-party service providers (providers) in accordance with the NIST Standard. Providers are entities that perform tasks and business functions on behalf of the Authority.

Since the prior year's audit, the Authority completed corrective action for one of the three prior weaknesses by updating its IT System and Organization Control (SOC) Review Procedure, as well as its Security and Risk Management Policies, to accurately reflect the Authority's current requirements and process to maintain oversight of its providers. However, the following two weaknesses remain:

- The Authority has not completed a formal risk assessment for 32 of its 37 (86%) providers. The Security and Risk Management Policies require the Information Security Department to perform a risk assessment for all new, replacement, and production systems, and to conduct risk assessments for critical information systems and production applications at least once every three years. Without completing risk assessments, the Information Security Department is unable to determine the risks that impact its sensitive data or providers and dedicate the resources to ensure appropriate security controls are implemented to reduce or mitigate those risks.

- The Authority has not received and reviewed independent audit assurance that provides an opinion over the operating effectiveness of the controls in place for two of its 13 (15%) applicable providers as defined in its Risk Management Policy and SOC Review Procedure. If the provider qualifies for the Authority's review, the Authority is required to obtain a SOC report to review for the provider. The NIST Standard requires the Authority to employ organizationally defined processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis. By not receiving and reviewing independent audit assurance, such as a SOC report, for each provider on an ongoing basis,

the Authority cannot validate that the providers have effective IT controls to protect the Authority's sensitive and confidential data, increasing the chance of a breach or possible data disclosure.

Due to turnover in the Information Security Department, the Authority did not have adequate resources to complete formal risk assessments or receive and review independent audit assurance for all providers that qualify.

The Authority should conduct a formal risk assessment for each provider to determine the potential risks that may impact the provider, the security controls necessary to mitigate the risks, and determine the sensitivity of the data handled by the providers. The Authority should then obtain and review independent audit assurance for each provider to validate that IT controls are implemented as required and effective to mitigate potential risks. These actions will help to safeguard the confidentiality, integrity, and availability of the Authority's sensitive and mission critical data.

Improve Physical and Environmental Security Policy and Processes

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2024

The Authority does not require and has not implemented certain physical and environmental security requirements in accordance with its Physical Protection Policy and the NIST Standard. Since the prior year audit, the Authority completed corrective action for three of the five weaknesses identified. We communicated the remaining two control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The NIST Standard requires the Authority to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the Authority's IT mission critical systems and data. The Authority has experienced significant staff turnover in the past year, leading to delays in resolving the remaining two weaknesses.

The Authority should obtain and dedicate the necessary resources to implement the controls required to address the weaknesses identified in the FOIAE communication, which will help ensure the Authority protects the confidentiality, integrity, and availability of its sensitive and mission critical systems and data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 2, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Alcoholic Beverage Control Board
Virginia Alcoholic Beverage Control Authority

Dale Farino, CEO
Virginia Alcoholic Beverage Control Authority

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

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the **Virginia Alcoholic Beverage Control Authority** (Authority) as of and for the year ended June 30, 2025, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated December 2, 2025.

Report on Internal Control Over Financial Reporting

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

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

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve Internal Controls Over Employee Separation Process," "Conduct Information Security Assessments," "Improve IT Risk Management and Contingency Planning," "Improve Virtual Private Network Security," "Continue Improving Oversight of Third-Party Service Providers," and "Improve Physical and Environmental Security Policy and Processes," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Authority's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and**,** accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled "Conduct Information Security Assessments," "Improve IT Risk Management and Contingency Planning," "Improve Virtual Private Network Security," "Continue Improving Oversight of Third-Party Service Providers," and "Improve Physical and Environmental Security Policy and Processes."

The Authority's Response to Findings

We discussed this report with management at an exit conference held on December 3, 2025. Government Auditing Standards require the auditor to perform limited procedures on the Authority's response to the findings identified in our audit, which is included in the accompanying section titled "Authority Response." The Authority's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The Authority has not taken adequate corrective action with respect to the prior reported findings identified as ongoing in the Findings Summary included in the Appendix. The Authority has taken adequate corrective action with respect to prior audit findings identified as complete in the Findings Summary included in the Appendix.

Purpose of this Report

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

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

AVC/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Ensure Follow-Up Inventories are Performed	Complete	2024
Improve Internal Controls Over Employee Separation Process	Ongoing	2022
Conduct Information Security Assessments	Ongoing	2025
Improve IT Risk Management and Contingency Planning	Ongoing	2023
Improve Virtual Private Network Security	Ongoing	2025
Continue Improving Oversight of Third-Party Service Providers	Ongoing	2020
Improve Physical and Environmental Security Policy and Processes	Ongoing	2024

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

December 9, 2025

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

Attached are the Virginia Alcohol Beverage Control Authority ("VA ABC," the "Authority") responses to the audit findings for fiscal year ended June 30, 2025. The Authority appreciates the opportunity to respond to the findings noted, and to strengthen our controls based on the recommendations. Our responses to the findings in the Report on Internal Controls are as follows:

Improve Internal Controls Over Employee Separation Process

VA ABC concurs with the recommendation. The Authority will review current policies regarding employee separations to ensure they reflect the current operational environment and ABC's risk posture moving forward. ABC will also ensure that all employees are properly trained on current and future policies.

Conduct Information Security Assessments

VA ABC concurs with the recommendation. Throughout the fiscal year, VA ABC conducted limited procedures to mitigate the risk arising from the absence of security assessments and IT audits. Resources will be allocated to ensure IT security assessments and audits are conducted regularly in line with defined timelines.

Improve IT Risk Management and Contingency Planning

VA ABC concurs with the recommendation and will allocate the appropriate resources to complete the remaining SSPs and risk assessments.

www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

Improve Virtual Private Network Security

VA ABC concurs with the recommendation. VA ABC will ensure that VPN procedures align with NIST as well as implement the controls addressed in the FOIAE communication.

Continue Improving Oversight of Third-Party Service Providers

VA ABC concurs with the recommendation and will complete the backlog of risk assessments according to policy. VA ABC will continue to obtain, and review required vendor SOC reports.

Improve Physical and Environmental Security Policy and Processes

VA ABC concurs with the recommendation and has taken appropriate corrective action.

Sincerely,

Dale F. Farino
Chief Executive Officer

www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400