STATE OF VERMONT

MANAGEMENT LETTER

JUNE 30, 2023

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

Management
State of Vermont

In planning and performing our audit of the financial statements of the State of Vermont (the State) as of and for the year ended June 30, 2023, 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, we considered the State's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

However, during our audit we became aware of deficiencies in internal control (other than significant deficiencies and material weaknesses) and other matters that are opportunities to strengthen your internal control and improve the efficiency of your operations. The memorandum that accompanies this letter summarizes our comments and recommendations regarding those matters. We previously provided a written communication dated January 26, 2024, on the State's internal control. This letter does not affect our report on the financial statements of the State dated January 26, 2024, nor our internal control communication dated January 26, 2024.

We will review the status of these comments during our next audit engagement. We have already discussed these comments and recommendations with State personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

This communication is intended solely for the information and use of management and others within the State, and is not intended to be, and should not be, used by anyone other than these specified parties.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Boston, Massachusetts
January 26, 2024

STATE OF VERMONT
MANAGEMENT LETTER
TABLE OF CONTENTS
JUNE 30, 2023

COMMENTS AND RECOMMENDATIONS

Bank Reconciliations – Department of Liquor and Lottery, Division of Liquor Control

Comment

The Department of Liquor and Lottery, Division of Liquor Control (Division) performs monthly reconciliations of liquor sales revenues amongst the following sources:

- Bank Statements
- Statewide Accounting System (VISION)
- Point-of-Sale System (Dynamics 365)

The Division's written procedures established for these reconciliations do not specify procedures regarding timely review and approval. The Office of the State Treasurer requires that, in the absence of a policy, best practices require that the reconciliations should be reviewed within thirty (30) days of month-end.

We identified the following deficiencies in our review of the Division's month-end reconciliations during our testing of effectiveness of controls over liquor sales revenues:

- Two (2) of twenty-four (24) monthly reconciliations were not signed off by a reviewer.
- Eight (8) of 24 reconciliations indicated the review was not performed within 30 days of month end.
- None of the 24 reconciliations tested included evidence to substantiate that monthly sales revenues were reconciled to Dynamics 365.

Recommendation

We recommend the Division strengthen its internal controls over monthly reconciliations by formalizing their own documented reconciliation policy. The Division should also ensure documentation supports the timely performance and review of the monthly reconciliations; as well as reconciliations of activities to Dynamics 365.

Capital Assets – Division of Buildings and General Services (BGS) and the Agency of Transportation (AOT)

Comment

During our testing of governmental activities capital assets additions, we noted three (3) out of twenty-five (25) additions tested in our sample were not traceable to any supporting documentation. Two (2) of the additions tested were recorded by BGS and one (1) addition was recorded by AOT.

The Department of Finance and Management's internal control best practice process for capital assets indicates that adequate project cost records should be maintained and transferred timely to detailed subsidiary records. While the testing results of our audit sample were sufficient to reduce risk of material misstatement to an acceptably low level, the lack of documentation in these instances presents an unnecessary increased control risk of misstatement over the State's capital assets activities and disclosures.

Recommendation

We recommend that BGS and AOT strengthen internal controls over capital asset additions in accordance with the Department of Finance and Management's best practice policy.

General Disbursements – Division of Buildings and General Services (BGS); Department of Motor Vehicles (DMV)

Comment

The Agency of Administration's Bulletin No. 3.5, *Procurement and Contracting Procedures* (Bulletin 3.5) establishes polices and procedures which apply to the procurement and purchase of all goods and services, regardless of dollar amount, by the agencies of the executive branch.

During our control testing of Statewide general disbursements, we noted one (1) out of forty -six (46) disbursements tested lacked a supporting contract for services meeting the requirements of Bulletin 3.5. The disbursement was processed by the DMV.

Additionally, we noted four (4) out of forty-six (46) disbursements related to statewide contracts for which the documents required by Bulletin 3.5 and in custody of BGS were lost during the flooding in July 2023. Electronic versions of the documents were made available for review during our testing.

Such documentation required by Bulletin 3.5 is essential for demonstrating sound internal controls over general disbursements.

Recommendation

We recommend that DMV and BGS strengthen internal controls over compliance with the contract requirements of Bulletin 3.5.

I-9 and Background Check Employment Eligibility Verifications – Human Resources

Comment

The State's Personnel Policy and Procedure Manual requires all agencies and departments to have a completed I-9 form and background check on file for all new hires in order to verify such new hires are eligible to work in the United States and eligible to work for the State.

During our testing over new hires, we identified the I-9 forms for four (4) of forty-six (46) employees tested were not prepared on or before the first day of employment, and signed and retained on file. These instances occurred at the Department of Environmental Conservation (1), the Department of Vermont Health Access (1), and Judiciary (2). Additionally, one of the two Judiciary employees also did not have a background check retained on file.

Recommendation

We recommend the Department ensure the required documentation is maintained related to I-9 forms and background checks.

Information Technology

Comment – Password Management (Agency of Digital Services (ADS), Department of Finance and Management (DOF), Agency of Human Services (AHS), Department of Labor (DOL), and Department of Motor Vehicles (DMV))

The Statewide Security Standards (section 2.1.1). states that password settings should have a minimum length of 12 characters and complexity enabled.

We identified the following exceptions:

- For ADS, the configurations for the ERP domain is set for a minimum password length of 6 characters, complexity disabled, and max password age of 180 days.
- For DOL, the configuration for the VISION application requires a minimum password length of 8 characters with complexity disabled.
- For AHS, the network password configuration only requires 8 characters. The BFIS application password configuration only requires 8 characters. The AlloCAP web application password configuration only requires 6 characters. In addition, the AlloCAP web application does not require multifactor authentication for access outside of the State's network.
- For DOL, the VABS/CATS application configuration specifies 3-6 and the SalesForce configuration specifies 10 characters. It was noted that prior to accessing these applications, an employee must log into the network through the state system logon requirements.
- For DMV, the Active Directory configurations and the FAST application configurations do not meet the standard of 12 characters in password length. In addition, account lockout threshold is set to 10 invalid attempts.

Recommendation

We recommend that password settings for the identified Agency’s networks and applications be configured to align with Statewide Security Standards, which states that best practice is to have a minimum length of 12 characters and complexity enabled.

Comment – Periodic Access Review (Agency of Digital Services (ADS) and Agency of Human Services (AHS))

ADS did not provide evidence of a formal periodic user access review for the ERP domain users performed during fiscal year 2023 to verify that all accounts are assigned to active employees and that access rights within the domain are appropriate.

While AHS periodically performed account inactivity and password lockout reviews over Access Applications, a review of active users and permission for ACCESS was not performed. In addition, there is no review over inactive or active user accounts for the SSMIS application. AHS policy indicates that an access review should be completed by the System Administrator annually.

Recommendation

We recommend that ADS and AHS perform an access review of the domain users and application users in accordance with ADS Information Security Policy section 2.3.2 to ensure that only active employees have active accounts, that permissions are appropriate for each employee's role, and that all terminated user access has been removed.

Comment – Risk Management (Agency of Digital Services (ADS))

While internal weekly vulnerability scans are conducted for ADS systems, there is no documented evidence that an external penetration test has been performed to determine exploitable vulnerabilities and attack vectors from outside of the agency's network during the audit period.

In addition, there is no documented evidence that a formal comprehensive IT Risk Assessment was performed over the ADS environment during the audit period. Risks should be assessed on a periodic basis to identify reasonably foreseeable internal and external threats to data and information technology assets. Such threats could negatively impact confidentiality, security, and integrity of data and/or availability of systems.

Recommendation

We recommend ADS document regular external penetration assessments to identify vulnerabilities and attack vectors. The tests should include a full scope of blended attacks, such as wireless, client-based, and web application attacks, addressing critical systems in a non-production environment. These attacks can also include some social engineering elements such as email Phishing tests for all staff.

We recommend that an IT risk assessment be performed that is modeled after an established framework in order to adequately assess the Agency's risk environment, identify gaps in controls and identify the level of compliance with required regulations. Alternatively, a third-party could be contracted to provide such services.

Comment – Terminated User Access (Department of Tax (VTAX) and Department of Motor Vehicles (DMV)

For VTAX, one (1) terminated employee that was sampled for testing was not disabled from the VTax application within a timely manner. Human resources records indicated the employee was terminated on November 30, 2022 but not disabled until October 5, 2023.

For DMV, three (3) terminated employees were not disabled from the FAST application after their termination date. It was noted that the terminated employees did have their network access removed at the time of our testing.

Recommendation

We recommend that terminated employee access be removed immediately, and that procedures around termination be enhanced to remove terminated user access at time of termination and to review whether terminated users’ access has been removed from the significant applications.

Comment – Change Management – Segregation of Duties (Agency of Human Services (AHS))

Personnel who have development responsibilities for the ACCESS and SSMIS applications also have access to migrate changes to the production environment, which does not allow for appropriate segregation of duties.

Recommendation

We recommend that AHS address the lack of segregation of duties for the application change management functions by either separating the specific individuals access and responsibility, or by having a separate individual with no access periodically review logs of the change management activity.

Comment – Change Management – Documentation (Department of Labor (DOL))

For the application changes tracked in the change management ticketing system, evidence of testing and approval actions are documented within email conversations that the ticketing system captures. However, there is no standard way of tracking the testing and approval of changes to clearly define who completed each action and when the actions were completed.

Recommendation

We recommend that DOL following the statewide change management policy and formally document the request, testing, and approval of all changes related to the applications.

Comment – Vulnerability Management (Department of Motor Vehicles (DMV))

The last external penetration test performed over the FAST application to determine exploitable vulnerabilities and attack vectors from outside of the department's network occurred in February of 2020. In addition, there was no documented evidence of a formal vulnerability assessment over the FAST application being performed during the audit period. It was noted that these assessments are planned to be performed in the upcoming fiscal year.

Recommendation

We recommend performing and documenting regular external penetration assessment and internal vulnerability assessment at least on an annual basis to identify vulnerabilities and attack vectors. The tests should include a full scope of blended attacks, such as wireless, client-based, and web application attacks, addressing critical systems in a non-production environment. These attacks can also include a social engineering element; such as email phishing tests for all staff.