# STATE OF VERMONT

# MANAGEMENT LETTER

# JUNE 30, 2022

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, 2022, 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 December 22, 2022, on the State's internal control. This letter does not affect our report on the financial statements of the State dated December 22, 2022, nor our internal control communication dated December 22, 2022.

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
December 22, 2022

**STATE OF VERMONT**
**MANAGEMENT LETTER**
**TABLE OF CONTENTS**
**JUNE 30, 2022**


**COMMENTS AND RECOMMENDATIONS**

**POLLING REPORT RECONCILIATION – DEPARTMENT OF LIQUOR AND LOTTERY, DIVISION OF LIQUOR CONTROL** **1**

**BANK RECONCILIATIONS – DEPARTMENT OF LABOR** **2**

**CLASSIFICATION OF EMPLOYER RECEIVABLES – DEPARTMENT OF LABOR** **3**

**I-9 FORM EMPLOYMENT ELIGIBILITY VERIFICATIONS – HUMAN RESOURCES** **4**

**INFORMATION TECHNOLOGY** **5**

***Polling Report Reconciliation – 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 from the State's trial balance activity recorded in the VISION system to the activity reported in the Division's point-of-sale system, Dynamics365. An annual polling report is generated from Dynamics365 and is included in the GAAP financial statement submission as support for liquor sales revenues reported in the financial statements.

We obtained the annual polling report included in the GAAP financial statement submission from the Department of Finance and Management; as well as a separate annual polling report generated by the Division which was used for testing of individual liquor sales revenues. We noted the total liquor sales revenues did not agree between these two (2) reports obtained from the different departments.

While the aggregate difference between the reports was not material (approximately $22,000), we noted that the agency store sales data differed between the reports in seventy-eight (78) of seventy-nine (79) instances. Such differences were the result of reporting differences occurring throughout the fiscal year.

An immaterial unreconciled variance of approximately $16,000 also remained between the GAAP financial statement submission polling report and the Liquor Control Fund financial statements.

Recommendation

We recommend the Division examine its current GAAP financial statement process and determine the cost/benefit of resolving the unreconciled differences between the polling reports used in the GAAP financial statement submission to the Dynamics365 reports used for the monthly reconciliations of liquor sales revenues. The annual report reconciliation should be approved by a preparer and reviewer.

***Bank Reconciliations – Department of Labor***

Comment

The Department does not have written policies and procedures established for month-end reconciliations of claims disbursements bank accounts. The Office of the State Treasurer requires that reconciliation procedures for each bank account are provided for review annually. In the absence of a policy, best practices require that the reconciled report should be available for review by the Financial Manager (or designee) within thirty (30) days of month-end.

We identified the following deficiencies in our review of the Department's month-end bank reconciliations during our walkthrough of controls over Employer Revenues, Federal Grants, and Claims:

- Four (4) out of five (5) bank reconciliations had no evidence of preparer and reviewer sign offs.
- One (1) out of five (5) bank reconciliations had no evidence of a preparer sign off.
- Five (5) out of five (5) bank reconciliations were not prepared and reviewed timely.
- One (1) out of five (5) bank reconciliations tested for benefit cash accounts for PUA Unemployment Claims contained reconciling items not resolved withing a reasonable timeframe including pending tax withholding transfers, voids, write-offs, and miscellaneous adjustments, some of which date back to 2020.

Recommendation

We recommend the Department strengthen its internal controls over bank reconciliations for cash by formalizing a bank reconciliation policy and ensuring their documentation supports the timely performance of these reconciliations in accordance with the Department's policy. The Department should further ensure all reconciling items are resolved timely, prior to the reviewer approval of the final reconciliation.

***Classification of Employer Receivables – Department of Labor***

Comment

During our substantive testing of contributory employer receivables reported in the unemployment compensation trust fund, we noted one (1) out of nine (9) receivables tested was due from a reimbursable employer. Receivables due from contributory and reimbursable employers are reported in separate categories in the proprietary funds statement of net position.

The Department of Labor elected not to reclassify the reimbursable receivables since the projected reclassification was immaterial based on the overall substantive testing results.

Recommendation

We recommend the Department of Labor revisit its year-end reporting process and identify how balances due from contributory and reimbursable employers can be separated in the source records so such receivables can be accurately distinguished in the financial statements.

### *I-9 Form 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 on file for all new hires in order to verify such new hires are eligible to work in the United States.

During our testing over new hires, we identified the I-9 forms for five (5) of forty-six (46) employees tested were not prepared on or before the first day of employment, signed, and retained on file. Single instances occurred at the Department of Fish and Wildlife, Department of Public Safety, and the Department of Children and Families; two instances occurred at the Department of Health.

Recommendation

We recommend the Department strengthen its internal controls over new hires to minimize exceptions related to late or incorrect I-9 forms.

***Information Technology***

Comment – Password Management (Agency of Digital Services (ADS), 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.

- For ADS, there was no current year evidence provided for the current configuration of the ERP domain passwords. From prior year evidence the configurations only required a minimum password length of 6 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.

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))

ADS did not provide evidence of a formal periodic user access review for the ERP domain users performed during the FY22 to verify that all accounts are assigned to active employees and that access rights within the domain are appropriate.

Recommendation

We recommend that ADS perform an access review of the ERP domain 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 ensure that all terminated user access has been removed.

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

While and internal weekly vulnerability scans are conducted for ADS systems, there is no documented evidence that an external penetration test has not 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 of a formal comprehensive IT Risk Assessment having been 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, which could negatively impact confidentiality, security, and integrity of data and/or availability of systems.

Recommendation

We recommend documenting 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 provider could be contracted to provide such services.

Comment – Segregation of Duties – Business Roles (Department of Human Resources (VTHR))

VTHR PeopleSoft Delivered Role is assigned to a Business Application Support Specialist that also has access to Compensation Adjustments. The PeopleSoft Delivered Role should belong to individuals that have no responsibility for performing HR business functions within the system to ensure segregation of duties is maintained.

Recommendation

We recommend that administrator level of access in the system should be restricted to individuals that have limited or no responsibility to perform business functions within the system (typically IT individuals).

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

For one of the four application changes sampled for testing during the period, there was no documented evidence of testing or approval prior to being moved to production. This sampled change was related to the SalesForce Application.

Recommendation

We recommend following the statewide change management policy and formally documenting the request, testing, and approval of all changes related to the SalesForce application.

Comment – Policy Documentation (Department of Motor Vehicles (DMV))

Key policy documents, such a Disaster Recovery Policy, Business Continuity Policy, and Incident Response Policy are not formally documented.

Recommendation

We recommend that formal documents be established that reflect the processes for Disaster Recovery, Business Continuity and Incident Response.