Commonwealth of Massachusetts

Management Letter

June 30, 2018

KPMG LLP
Two Financial Center
60 South Street
Boston, MA 02111

March 29, 2019

The Comptroller's Advisory Board
Commonwealth of Massachusetts
Boston, Massachusetts

Advisory Board Members:

We have audited the basic financial statements of the Commonwealth of Massachusetts (the Commonwealth), for the year ended June 30, 2018, and have issued our report thereon dated January 18, 2019. In planning and performing our audit of the basic financial statements of the Commonwealth, we considered internal control over financial reporting (*internal control*) as a basis for designing our auditing procedures for the purpose of expressing our opinions on the basic financial statements. The objective of our audits is to express opinions on the Commonwealth's basic financial statements, in accordance auditing standards generally accepted in the United States of America (AICPA), but not for the purpose of expressing an opinion on the effectiveness of the Commonwealth's internal control. Accordingly, we do not express an opinion on the effectiveness of the Commonwealth's internal control.

During our audit we noted certain matters summarized on the attached schedule of observations related to internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are not considered to reflect deficiencies, significant deficiencies, or material weaknesses in internal control over financial reporting. All deficiencies, significant deficiencies, and material weaknesses in internal control over financial reporting have been previously communicated to management and the Comptroller's Advisory Board, as applicable.

Our audit procedures are designed primarily to enable us to form opinion on the basic financial statements and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Commonwealth's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The Commonwealth's written responses to our comments and recommendations have not been subjected to the auditing procedures applied in the audit of the basic financial statements and, accordingly, we express no opinion on them.

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

Very truly yours,

KPMG LLP

KPMG LLP is a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2018

MLC 2018-01

Department of Children and Families – Access to HR/CMS Application

Massachusetts Bay Transportation Authority – Access to HR/CMS Application

Repeat observation: No

Observation

The Commonwealth of Massachusetts (the Commonwealth) has various policies and procedures in place to remove users with more than default access from key financial applications when they leave Commonwealth employment. The policies and procedures include the timely removal of a user's access to those financial applications.

During 2018, we found that 28 HR/CMS users with more than default access left Commonwealth employment and two (2) of those users did not have their access rights removed timely. The terminated users had their access removed 18 and 20 days after termination. The 28 users sampled from the termination listing were selected based on the following criteria – 1) User was a member of the HRD or CTR department or 2) User's title was associated with Payroll or Human Resources.

Recommendation

We recommend that management review their internal controls and make adjustments where necessary to ensure that all terminated employees with more than default access to financial applications have such access removed timely.

Management's Corrective Actions

DCF:

DCF has modified its biannual review process going forward to include sharing of security access reports with the Department's Human Resources Liaison. The DSO will provide the Human Resources Liaison with a copy of the biannually reviewed Human Resource / Compensation Management System Department Security (SECHRCMS) Luminist report. When staff voluntarily or involuntarily terminate, the Human Resources Liaison will notify the DSO timely. The DSO will process the termination of access timely after receiving the request.

MBTA:

The employee noted ended employment on one date and fully separated one week later due to the timing of payroll and leave balance reconciliations. This resulted in a delay in notification to all parties of the separation. Access was disconnected on the day of notification. The process has been updated to include the MBTA's DSO on the distribution report of weekly separations. The list is reviewed against active HRCMS users and appropriate action taken working closely with the security team at the CTR office.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2018

Responsible Officials

DCF

Miriam Vazquez, Designated Security Officer, DCF
Jaylila Worrell, Human Resources Liaison, DCF
David O'Callaghan, Chief Financial Officer, DCF

MBTA

Paul Brandley, Chief Financial Officer & Treasurer, MBTA
Gina Spaziani, Director of Finance, Planning & Analysis, MBTA

MLC 2018-02

Department of Children and Families – Inappropriate Access to Approve Timesheets

Repeat Observation: No

Observation

The Commonwealth of Massachusetts has various policies and procedures in place over the approval of employee timesheets. Generally, a supervisor or designee is responsible to approve an employee's time before it is forwarded to the payroll module. Additionally, specific roles exist that provide access to approve the time of employee's that are not in one's hierarchy. These roles are intended for specific personnel at the Comptroller's office and departmental specific payroll and human resource personnel. Departmental personnel are granted the ability to approve timesheets outside their hierarchy by the department's security officer.

During our audit, we noted 10 Department of Children and Family's (DCF) users had access to approve timesheets outside their approval hierarchy. Upon inquiry with the DCF security officer, it was determined that 5 of those users should not have such access. Access to approve timesheets outside their approval hierarchy was removed when discovered. DCF found that those 5 users did not approve any timesheets outside their hierarchy during the audit period.

Recommendation

We recommend that DCF strengthen internal controls to ensure that only appropriate personnel have access to approve timesheets outside their approval hierarchy.

Management's Corrective Action Plan

In general, although DCF reviews the appropriateness of access to HR/CMS every 6 months, we have not historically reviewed the specific roles granted to individuals. As a result of this finding, DCF has modified its biannual review process to take into account both the appropriateness for the employee to have access to HR/CMS but also to ascertain the appropriateness of the specific role(s) granted to the employee relative to their duties and responsibilities. Any new requests for HR/CMS access will be similarly assessed and roles assigned accordingly. DCF has updated its internal controls to reflect this modification to our biannual review process.

Responsible Officials

David O'Callaghan, Chief Financial Officer, DCF
Miriam Vazquez, Designated Security Officer, DCF

MLC 2018-03

Office of the Comptroller – Capitalization of Expenses

Repeat Observation: No

Observation

During our audit of capital assets, we found a capital asset addition that should not have been capitalized. The item totaled $1.9 million and, due to statistical sampling, the expected misstatement totaled $81.5 million. The capital asset addition represented consultant expenses, technical support, subscription and connection licenses and administrative expenses that are not capitalizable.

Recommendation

We recommend management strengthen their internal controls to ensure that only capitalizable expenses are added to capital assets.

Management's Corrective Action Plan

The Comptroller's Office will reiterate in its instructions to departments that certain expenses should not be capitalized. In addition, it will strengthen its review of capitalized expenses to ensure that only appropriate expenses are capitalized.

Responsible Officials

Michael Rodino, Director of Financial Reporting, CTR
Pauline Lieu, Deputy Director of Financial Reporting, CTR

MLC 2018-04

Office of the Comptroller – Hosting Applications on the Cloud

Executive Office of Technology Services and Security – Hosting Applications on the Cloud

Repeat Observation: No

Observation

The Office of the Comptroller (CTR) is planning to migrate the HR/CMS application from an internally hosted environment supported by the Executive Office of Technology Service and Security (EOTSS) to an externally hosted environment in the cloud. A migration from internally to externally hosted software presents challenges to entities, including the considerations of information technology general controls over the new environment and internal controls over the transition between environments. During this transition, the Commonwealth should consider the following:

Program Development

Ensure internal controls are present, performed and documented so management can demonstrate that:

- Access to the new environment is appropriately restricted prior to go-live.
- All data has migrated completely and accurately from the old to the new environment.
- The functionality in the new environment has been appropriately tested by end-users to confirm it is working as designed and intended.
- Appropriate approvals by appropriate relevant personnel from business and IT have been obtained before the move went live.

General IT Controls

- Internal controls for access, change management and computer operations in the “old” hosting environment will need to be operating effectively until the transition to the new environment.
- Any areas and controls impacted by the transition (understood to be physical access controls and potentially certain infrastructure controls) should be reviewed as part of go-live to ensure that controls are implemented effectively in the new environment.

Service Organization Control (SOC) Report

With the introduction of a cloud provider, the Comptroller’s office should obtain and review the SOC report in detail to verify that:

- The SOC report provides the expected amount of assurance (e.g., SOC 1 Type II vs. SOC 1 Type I).
- The opinion is not adverse or qualified.
- SOC reports and bridge letters are available to adequately cover the Commonwealth’s fiscal year (e.g., SOC report for year ended 12/31 and a bridge letter to cover 1/1 to 6/30).
- The independent service auditor associated with the SOC report is reputable.
- The internal controls tested in the SOC report are those that the Commonwealth requires/expects to be performed by the service provider and cover the areas outsourced to the cloud provider (e.g. if the Commonwealth has outsourced the Operating System support, the SOC report should include controls over Operating System access).

- The internal controls relied upon by the Commonwealth do not have exceptions. If there are exceptions, determine whether these impact the Commonwealth or whether adequate procedures have been performed and documented by the cloud provider to verify there is no impact.
- The SOC report includes Complimentary User Entity Controls (CUEC's). The Comptroller's office should determine whether these are relevant to the Commonwealth and if so whether these controls exist and are operating effectively.

Recommendation

Should HR/CMS switch hosting environments during fiscal year 2019, KPMG expects to perform audit procedures in these areas. Therefore, we recommend that the Comptroller's office consider the above points and enhance their existing internal controls where necessary.

Management's Corrective Action Plan

The expectation is that the migration to the Amazon Web Services (AWS) cloud will occur before the end of FY19. CTR will work with EOTSS to review and incorporate these suggestions, or will document any additional or alternative measures.

Responsible Officials

Kevin McHugh, Acting Deputy Comptroller, CTR
Madhavi Donepudi, Director of Enterprise Applications Services, EOTSS

MLC 2018-05

Office of the Comptroller – Fiduciary Activities Standard

Repeat Observation: No

Observation

In January 2017, the GASB issued Statement No. 84, *Fiduciary Activities*. This Statement establishes criteria for identifying fiduciary activities of all state and local governments. The focus of the criteria generally is on (1) whether a government is controlling the assets of the fiduciary activity and (2) the beneficiaries with whom a fiduciary relationship exists. Additionally, criteria are included to identify fiduciary component units and postemployment benefit arrangements that are fiduciary activities.

An activity meeting the criteria should be reported as one of four fiduciary funds described in the Statement: (1) pension (and other employee benefit) trust funds, (2) investment trust funds, (3) private-purpose trust funds, and (4) custodial funds. Custodial funds should report fiduciary activities that are not held in a trust or equivalent arrangement that meets specific criteria.

Identification of potential fiduciary activities, determining whether such activities are fiduciary activities, and documenting the conclusions for each potential fiduciary activity is anticipated to be a time consuming process for large general governments. For that reason, such governments are advised to begin implementation of this Statement far in advance of December 31, 2019, the first year-end this Statement is applicable.

Recommendation

We recommend that management begin to implement this Statement by establishing a project team and project plan with major milestones timed to ensure that this Statement is implemented for the Commonwealth's June 30, 2020 year-end. The project plan should incorporate the following high level activities:

- Identification of potential fiduciary activities
- Determination of whether potential fiduciary activities are fiduciary activities
- Categorization of fiduciary activities into one of the four fiduciary fund types
- Documentation of all determinations and decisions made
- Analyze anticipated changes to existing financial reporting
- Communication of anticipated changes to existing financial reporting to relevant stakeholders
- Implementation of any necessary changes to the CAFR compilation process

Management's Corrective Action Plan

The Comptroller's Office has begun planning for implementation of GASB 84, and intends to continue analyzing fiduciary activities to be ready for implementation of the standard in the FY2020 CAFR.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2018

Responsible Officials

Howard Merkowitz, Deputy Comptroller, CTR
Michael Rodino, Director of Financial Reporting, CTR
Pauline Lieu, Deputy Director of Financial Reporting, CTR

MLC 2018-06

Office of the Comptroller – Lease Standard

Repeat Observation: No

Observation

In June 2017, the GASB issued Statement No. 87, *Leases*. In addition to defining a lease arrangement, this Statement requires recognition of certain lease assets and liabilities for leases that previously were classified as operating leases and recognized as inflows or outflows of resources based on the payment provisions of the contract. It establishes a single model for lease accounting based on the foundational principle that leases are financings of the right to use an underlying asset. Under this Statement, a lessee is required to recognize a lease liability and an intangible right-to-use lease asset, and a lessor is required to recognize a lease receivable and a deferred inflow of resources. The requirements of this Statement are effective for the fiscal year ending June 30, 2021.

Historically, financial statement preparers focused on potential capital leases when evaluating leasing arrangements. Now that all lease arrangements will have to be identified and analyzed, identification of such leasing arrangements is anticipated to be a challenge for all entities. Given the decentralized nature of large general governments, it will be even more challenging. Additionally, financial statement preparers will need to institute new financial reporting processes to obtain all leasing arrangements from outlying departments/agencies in order to analyze leasing arrangements and determine the appropriate financial reporting for such arrangements.

Recommendation

We recommend that management begin to implement this Statement by establishing a project team and project plan with major milestones timed to ensure that this Statement is implemented for the Commonwealth's June 30, 2021 year-end. The project plan should incorporate the following high level activities:

- Identification of all leasing arrangements
- Analyze all leasing arrangements to determine if they meet the definition of a lease
- Documentation of procedures performed to identify and analyze all leases
- Establish a process to obtain all future leases, including documentation of such processes
- Analyze anticipated changes to existing financial reporting
- Communication of anticipated changes to existing financial reporting to relevant stakeholders
- Implementation of any necessary changes to the CAFR compilation process

Management's Corrective Action Plan

The Comptroller's Office has begun planning for implementation of GASB 87, and intends to continue analyzing leasing arrangements to be ready for implementation of the standard in the FY2021 CAFR.

Responsible Officials

Howard Merkowitz, Deputy Comptroller, CTR
Michael Rodino, Director of Financial Reporting, CTR
Pauline Lieu, Deputy Director of Financial Reporting, CTR