Commonwealth of Massachusetts

Management Letter

June 30, 2017

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

March 29, 2018

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) as of and for the year ended June 30, 2017, and have issued our report thereon dated January 10, 2018. In planning and performing our audit of the basic financial statements of the Commonwealth, in accordance with auditing standards generally accepted in the United States of America, we considered the Commonwealth'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 basic financial statements, 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 involving 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 summarized on the attached schedule of observations.

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.

In addition, we identified certain deficiencies in internal control that we consider to be significant deficiencies, and in accordance with *Government Auditing Standards* communicated them in writing to the Commonwealth in a separate report dated January 10, 2018.

Our audit procedures are designed primarily to enable us to form opinions 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.

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

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2017

MLC 2017-01

Executive Office of Technology Services and Security – Data Center Access Review

Repeat observation: No

Observation

During fiscal year 2017, the person responsible for performing a quarterly review of users with access to the data center transitioned into another role. Therefore, he was no longer the appropriate person to perform the review. However, an appropriate replacement was not identified and the review was not performed.

Based on an independent review, no inappropriate access was identified.

A review of access is performed to detect potential unauthorized access and can serve as a mitigating control in case access is not appropriately granted or not revoked timely. Access to the data center is a critical security component and without a review, the risk increases that inappropriate physical access to the in-scope systems is used to affect the confidentiality, integrity and availability of the system and its data.

Recommendation

Management should assign the responsibility of a data center access review to an appropriate individual or group of individuals within the organization and ensure that the review is performed. In addition, management is recommend to verify the review considers:

- The review is performed, and documented, at an appropriate level of detail and the reviewer is able to verify access to the data center is commensurate with the person's job responsibilities.
- If the review is performed by multiple individuals, relevant correspondence with those individuals should be retained to document the review.
- The review leverages a complete and accurate population of individuals with access directly from the system of record.
- If and when individuals are identified that have inappropriate access to the data center, the reviewer should consider the impact this may have had. This should include considering whether the inappropriate access was ever used. These activities should be documented as part of the review.

Management's Corrective Actions

The Compliance and Assurance team of the Executive Office of Technology Services and Security (EOTSS) has developed, implemented, and performed access reviews of the three secured areas at the Massachusetts Information Technology Center in Chelsea. We started the new process in October 2017 and are continuing for the quarter beginning January 2018.

Responsible Official

James Cusson, Compliance & Assurance Program Director, EOTSS

MLC 2017-02

Executive Office of Health and Human Services (EOHHS) – Unpaid Claims

Repeat Observation: Yes, 2016-04

Observation

For fiscal year-end financial reporting purposes, the Commonwealth records a liability for Medicaid and several capitated benefits incurred by not yet paid, referred to as the Unpaid Claim Liability (UCL). Management's estimate model is reviewed by a KPMG actuarial specialist. This independent review indicated an initial UCL lower than our acceptable range, resulting in a proposed audit adjustment.

Recommendation

We recommend that additional management review controls should be put in place over the accuracy of both the inputs and methodology of the UCL estimate.

Management's Corrective Action Plan

MassHealth will work with KPMG's actuarial specialist to ensure that the Medicaid incurred but not reported estimate is within the initial range of Unpaid Claim Liability calculated by KPMG.

Responsible Official

Mohamed Sesay

MLC 2017-03

Group Insurance Commission (GIC) – Service Organization Controls Report

Repeat Observation: Yes, 2016-05 and 2015-09

Observation

The Group Insurance Commission (GIC) utilizes five insurance companies that provide health plan administrative services. GIC relies on insurance companies for claim receipt and entry, claim adjudication, and claim payment and customer funding. The insurance companies' controls are reviewed annually by a third-party which provides a service organization control (SOC) report detailing the status of controls and whether they are operating effectively. One insurance company provided its first ever SOC report covering only the last month of fiscal year 2017. GIC expects this insurance company will provide future SOC report(s) covering fiscal year 2018 in sufficient time to be evaluated as part of future annual audits.

Recommendation

We recommend that the GIC require all its health plan administrators provide timely SOC report(s) and/or bridge letter(s) regarding the status of the insurance company's control environment for the full fiscal year. Management should obtain and evaluate each SOC report/bridge letter as well as assess and document each SOC reports' user control considerations. Management needs to be mindful that it is the combination of SOC report(s) and user control considerations that form the basis of the internal control environment.

Management's Corrective Action Plan

The GIC requires all of its self-insured health care vendors to provide annual service organization control (SOC) reports (with bridge letters as necessary) detailing the status of their internal controls and whether they operated effectively during the prior fiscal year. As noted in KPMG's observation, one of the five GIC health care vendors failed, again, to provide its annual SOC report in FY2017.

In FY2017 this health care vendor submitted a corrective action plan, and a schedule for complying with the SOC reporting requirement, to GIC management. The GIC team met with this vendor many times over the course of FY2017, and the progress toward and delivery of the SOC report was a key agenda item in these discussions. As KPMG noted in its observation above, this vendor ultimately was only able to meet the control standards and receive a SOC-1 Type II report that covered the last month of fiscal year 2017. The vendor is therefore responsible for paying the GIC a performance guarantee penalty for its failure to comply with the FY2017 SOC reporting requirement.

The vendor is contractually required to provide the GIC with its 2018 SOC-1 Type II report for all twelve months of FY2018; in the event of any sort of failure, the performance guarantee penalty will be assessed. Since the vendor has now demonstrated its ability to satisfy its third party auditor with how it performs the control activities that are tested in this reporting, the GIC expects the vendor to be able to comply with the GIC's SOC reporting requirement in the fall of 2018.

GIC staff plans to append a memo reviewing the agency's performance relative to the complementary user end controls identified in its vendors' SOC reports to the GIC's Internal Controls documentation. Similar to the Internal Controls documentation generally, this would then be reviewed annually going forward.

Responsible Official

Catherine Moore, Acting Director of Financial Management

MLC 2017-04

Executive Office of Administration & Finance (A&F) – Actuarial Assumptions

Public Employee Retirement Administration Commission (PERAC) – Actuarial Assumptions

Repeat Observation: No

Observation

While Massachusetts General Law (MGL) outlines the roles and responsibilities of the Public Employee Retirement Administration Commission (PERAC), the Secretary of Administration & Finance (Secretary), and the House and Senate Committees on Ways and Means (Ways and Means) as they relate to the pension funding schedule and related underlying actuarial assumptions, there is no similar framework as it relates to the roles and responsibilities of "management" in preparing key actuarial estimates for financial reporting purposes. Consequently, for the Commonwealth's Comprehensive Annual Financial Report (CAFR), it remains unclear which levels of "management" involved in the Commonwealth's pension administration have ultimate responsibility for supporting such key actuarial estimates.

As reported in the June 30, 2017 CAFR, the net pension liability for the Massachusetts Teachers' Retirement System (MTRS) and the Massachusetts State Employees Retirement System (MSERS) was approximately $22.9 billion and $12.8 billion, respectively. To highlight the importance of certain key actuarial estimates, a 1-percentage-point decrease in the discount rate would result in revised net pension liabilities for MTRS and MSERS as of June 30, 2017 of approximately $28.4 billion and $17.5 billion, respectively. Similar magnitude impacts would result if the discount rate were increased, thereby decreasing the net pension liabilities.

Recommendation

Given the impact of key actuarial estimates for financial reporting purposes, we recommend that the Commonwealth clarify which statutory stakeholder (PERAC, Secretary and/or Ways and Means) also has responsibility for supporting such key actuarial estimates for financial reporting purposes.

Management's Corrective Action

The Secretary and PERAC look forward to working with the other Commonwealth stakeholders to consider any appropriate and necessary clarifications.

Responsible Officials

Robert Ross, A&F
Joseph Connarton, PERAC