KPMG

Commonwealth of Massachusetts

Management Letter

June 30, 2012

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

December 19, 2012

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, 2012, and have issued our report thereon dated December 19, 2012. 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 December 19, 2012.

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 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, 2012

MLC 2012-1

Department of Children and Families – Forecasting Methodology and Protocols

Observation

The Department of Children and Families (DCF) is responsible for forecasting its approximate $78 million in cash flow needs for the Foster Care and Adoption Assistance federally funded programs. At the beginning of each quarter, DCF receives its federal advance for these programs based upon an estimate prepared by management six months prior. At the end of each quarter, adjustments are made to true-up estimates to actual. For the fiscal year ended June 30, 2012, the cumulative adjustments to true-up the estimates to actual resulted in approximately $16.7 million and $5.2 million of additional federal funding for the Foster Care and Adoption Assistance programs, respectively.

Management has indicated that its forecasts are based upon the current quarter claim, past quarter claims, and any new initiatives occurring or expected to occur that may affect the claim being prepared. However, there is no formal documented methodology or protocols used to govern the quarterly forecasting meetings.

Recommendation

We recommend that DCF implement a formalized process to project future claims and expenditures to produce more accurate grant requests and minimize the amount of award adjustments.

Management's Corrective Action Plan

DCF agrees with this management recommendation and is in the process of implementing a formalized methodology to forecast Title IV-E grant awards. This forecast will be based on revenue projections, revenue initiatives, audit adjustments, and other items that may affect the Title IV-E claim. This methodology will be formally documented, and the projection resulting from the methodology will be reviewed and approved by EOHHS and DCF prior to submission of the Title IV-E claim to the federal administration for Children and Families.

Responsible Officials

Janice Axelrod, Director of Federal Revenue Claiming, Executive Office of Health and Human Services

Implementation Date

Fiscal year 2013

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-2

Bond Premiums, Discounts and Issuance Costs

Observation

The Treasurer's Office (TRE) is responsible for summarizing bond activity details; however, once completed the transaction details are provided to the Office of the Comptroller (CTR) for financial reporting in accordance with generally accepted accounting principles (GAAP).

During our audit we identified several Non-GAAP items including:

- Bond premiums, discounts are reported net of certain issuance costs rather than gross of all the issuance costs.

- The net bond premium, discounts and issuance costs are amortized based upon the maturity schedule of underlying debt which does not approximate the GAAP required effective interest method.

The Non-GAAP items were considered immaterial to the Commonwealth financial statements.

Recommendation

As with any Non-GAAP item, the Commonwealth should document its accounting and reporting elections as well as the magnitude of the GAAP departure.

Management's Corrective Action Plan

CTR's reporting election related to bond premiums, discounts and issuance costs has been documented as a part of our annual non-GAAP policies.

Our current debt management system (DBC) does not have the capability to calculate annual amortization using the effective interest method on a series of issuances; instead, this calculation can only be performed on one issue at a time. Preparing this calculation for all Commonwealth debt would require a significant amount of time and manual data entry to combine the individual results to arrive at a grand total for the Commonwealth.

We will continue to monitor the status of DBC's upgrades in order to meet our needs. For the fiscal year 2013 CAFR, we plan to calculate the difference between the GAAP vs. non-GAAP method to document the materiality of the variance.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

Responsible Officials

BJ Trivedi, Director, Financial Reporting Bureau, Office of the Comptroller
Michael Rodino, Manager, Financial Reporting Bureau, Office of the Comptroller

Implementation Date

Fiscal year 2013

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-3

Department of Housing and Community Development (DHCD) - Accounting and Reporting of Loans

Observation

The Department of Housing and Community Development (DHCD) administers the following federally funded loan programs: the Tax Credit Assistance Program and the HOME Program. The combined outstanding loan balance for these two programs was approximately $263 million at June 30, 2012. The majority of these loans are interest free with maturity dates that can extend for up to forty years. The majority of these loans do not mature until well after 2025. The net realizable value of these loans has never been captured as part of the Commonwealth's financial reporting process.

Recommendation

We recommend that DHCD review the accounting and reporting of its loan portfolio and make modifications to the current control environment to ensure that ALL of its loans are properly administered. Our recommendations include, but are not limited to, the following:

- An up-to-date database of loans should be maintained to ensure all scheduled principal and interest payments are collected when due and or appropriate action is taken on delinquent borrowers.

- The financial reporting process should capture all loans outstanding and appropriately identify and support the net realizable value of the portfolio which should be reported to the Comptroller's Office for proper disclosure.

Management's Corrective Action Plan

DHCD is currently developing a database application to enable accurate accounting and reporting of our loan portfolio. It is anticipated that this new application will be completed in June, 2014.

While the new application is being developed, DHCD will continue to maintain and enhance its current database to account for and report on the loan portfolio. This database captures key project information, including all Promissory Note information, to assist with the ongoing management of program projects. Using this database, DHCD will provide reports to the State Comptroller's Office regarding TCAP and HOME assets, as directed.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

Responsible Officials

Jo Ann McGuirk, Deputy Associate Director for the Division of Housing Development
Wayde Porrovecchio, Director of Finance for the Division of Housing Development

Implementation Date

DHCD will enhance the current database to account for and report on the loan portfolio by July 1, 2013.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-4

Department of Workforce Development - Accounts Receivable – Review of the Allowance for Uncollectible Items

Observation

In fiscal 2011, the Department of Workforce Development (DWD) changed its methodology for estimating the allowance for uncollectible accounts from a statutory basis to a GAAP basis. In fiscal 2012, although the allowance analysis was improved it was not complete as DWD does not have an entire accounts receivable history upon which to apply its GAAP basis methodology.

Recommendation

We recommend that DWD continue to build the historical accounts receivable data in order to more accurately estimate its allowance for uncollectible accounts.

Management's Corrective Action Plan

The allowance for doubtful accounts calculations are based on data showed in the aged account receivable report, in conjunction with an analysis of the collections against last year's debt. DUA/EOLWD will continue to build historical accounts receivable data.

Responsible Officials

Michelle Amante, Director Department of Unemployment Assistance
Walter Goldstein, Revenue Operations Director DUA

Implementation Date

Effective Immediately.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-5

Construction in progress not appropriately transferred to capital assets

Observation

The Commonwealth routinely enters into contracts for the construction of capital assets which may not be completed or put into use for several months. Prior to completion, the capital asset is classified as construction in progress (CIP). Upon completion, a CIP item is reclassified as a completed project and is then depreciated over its useful life.

We noted that the Department of Conservation and Recreation (DCR) did not properly reclassify three CIP items to depreciable assets once they were placed in service, resulting in an understatement of depreciation expense.

Recommendation

DCR should establish controls to ensure that assets are properly classified as in progress (CIP) or as completed projects. If necessary, DCR should seek out training to properly identify when such assets are considered complete for financial reporting purposes.

Management's Corrective Action Plan

After discussing the finding DCR determined the following steps needed to be implemented:

- Closer review of back up information provided by Planning and Engineering to Finance relative to fixed assets. This includes reviewing encumbrances and payments.

- Communicate with Planning and Engineering if any questions arise about a project's completion date or continued construction.

- Run a CIP report twice a year and confirm if the project remains CIP or completed. The report will be run January and end of June.

All CIPs that required updating are completed

Responsible Officials

Doug Leab, Business Manager Specialist, DCR
George Trubiano, Budget Director, DCR

Implementation Date

Immediate

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-6

Accounting and Financial Reporting of Retainage Related to Capital Projects

Observation

The Commonwealth routinely enters into contracts for the construction of capital assets. When these contracts require payments over a period of time, the contract will often include a "retainage" clause. This allows the Commonwealth to hold back a portion of the payment to ensure a good faith effort is made by the contractor to complete the project.

The accounting and financial reporting policies and procedures, which have been established to record capital assets, were also intended to capture retainage costs. However, it was noted during testwork that for several departments retainage was not capitalized until it was ultimately paid as opposed to when the costs were incurred as required by U.S. generally accepted accounting principles.

Recommendation

Departments should follow the existing retainage policy and enter balances into Massachusetts Management Accounting and Reports System (MMARS) throughout the construction period to properly record the value of assets and payables. Controls should be reviewed to ensure that departments are properly entering retainage into MMARS.

Management's Corrective Action Plan

CTR's capital asset reporting policy will be updated to include a retainage policy for departments. All construction in progress (CIP) activity during the year will be reviewed by CTR staff to assure retainage is being accounted for in accordance with generally accepted accounting principles (GAAP). We will also work with our general accounting bureau to determine if all retainage has been properly accounted for, capitalized and reported in the CAFR.

Responsible Officials

BJ Trivedi, Director, Financial Reporting Bureau, Office of the Comptroller
Michael Rodino, Manager, Financial Reporting Bureau, Office of the Comptroller

Implementation Date

Fiscal year 2013

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-7

Group Insurance Commission (GIC) - Service Organization Controls Report

Observation

The Group Insurance Commission (GIC) utilizes United Behavioral Health (UBH) as one of five insurance companies providing health plan administration services. GIC relies on UBH for claim receipt and entry, claim adjudication, and claim payment and customer funding. UBH's controls are reviewed annually by a third-party which provides a service organization control (SOC) report detailing the status of UBH's controls and whether they are operating effectively. However, UBH's SOC report only covers the ten-month period from January through October.

Recommendation

We recommend that GIC require all its health plan administrators provide appropriate confirmation, in the form of a bridge letter, regarding the status of its control environment for the period not covered by its SOC report.

Management's Corrective Action Plan

This contract is currently out to bid. The contract requires the vendor to submit a 12 month service organization control (SOC) report.

Responsible Officials

Ennio Manto, Director of Finance, GIC

Implementation Date

July 1, 2013

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-8

MassHealth - Service Organization Controls Report

Observation

The MassHealth agency utilizes several service organizations that provide assistance with claims processing. The service organizations controls are reviewed annually by third-parties who provide a service organization control (SOC) report detailing the status of the service organizations controls and whether they are operating effectively. However, the SOC reports received by MassHealth only cover a portion of the full fiscal year.

Recommendation

We recommend that MassHealth require all of their claims processing administrators to provide appropriate confirmation, in the form of a bridge letter, regarding the status of its control environment for the period not covered by its SOC report.

Management's Corrective Action Plan

MassHealth will coordinate efforts with its service organizations to assure that bridge letters are provided confirming the status of control environments from the period ending the date of the SOC report through the end of the SFY of the single audit in progress.

Responsible Officials

David Kerrigan, Internal Control Manager, EOHHS

Implementation Date

June 30, 2013

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-9

New Hire Documentation

Observation

Both management and non-management positions must have proper approval and sufficient documentation including, but not limited to, position title, start date, and salary amount to document a new hire.

It is the department itself that enters new hire documentation into the Human Resource and Compensation Management System (HR/CMS).

We sampled 40 departmental authorization forms and noted 3 forms did not contain a field to indicate its approval nor the effective start date. These exceptions all related to the Massachusetts College of Art and Design (MCA). This lack of information could lead to employees being inaccurately set up on HR/CMS.

Recommendation

We recommend that MCA update its departmental authorization form so that critical data, including approvals and effective start dates, is properly captured.

Management's Corrective Action Plan

The college's Trust Fund Temporary Employee Authorization and Student – Trust Fund Employee Authorization forms did not have a place for the authorized department signatory to date the form. The college added this. The authorized department signatory's signature is the approval.

Responsible Officials

Elaine O'Sullivan, Director of Human Resources
Kathryn Oram, Associate Director of Human Resources

Implementation Date

Summer 2012

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-10

Payroll Approval

Observation

The Commonwealth has established a system by which departmental time sheets are entered into the Human Resource and Compensation Management System (HR/CMS). For many departments, employee's time sheets are signed by the employee and reviewed and approved by a supervisor or someone at a higher level than the employee. The time sheets are then entered into the HR/CMS system at each department by the respective department's "timekeeper." Each department's time must be entered in HR/CMS and submitted before Tuesday of each pay period at which time they can no longer make changes to the pay period on HR/CMS. Some departments use "self-service" functionality that automates the electronic signature of both the employee and supervisor.

Additionally, the Chief Financial Officer (CFO) of each department (or other person with Department Head Signature Authorization {DHSA}) will review the pay period's payroll and sign a Payroll Expenditure Approval Form, independent of the department timekeeper submission and self-service submissions. This form is kept by the department and "… *will remain available for three years for review by the Office of the Comptroller or other auditing entity*."

We sampled 40 payroll expenditure approval forms and noted that for 11 items (from 11 different departments), departmental DHSA approval occurred after the payroll was paid.

Recommendation

We recommend departments adhere to established policy and sign payroll expenditure approval forms in a timely manner.

Management's Corrective Action Plan

CTR will add specific language about reviewing and signing timely in its policy and instructions. In addition, it will reinforce the importance of compliance in the Payroll User Group meeting and other department educational events. The expenditure approval form is now updated with language to clarify the date by which that form needs to be signed.

Responsible Officials

Kevin McHugh, Director, Payroll Bureau

Implementation Date

Complete by March 3rd Payroll User Group meeting

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-11

Massachusetts Teachers' Retirement System (MTRS) – Census Data

Observation

The Massachusetts Retirement Board (MTRB) is responsible for maintaining member information for all active, inactive, and retired employees who contribute to and participate in the Massachusetts Teachers' Retirement System (MTRS). The database of information is gathered from many different sources and in some cases in various different formats. The MTRS is currently in the process of implementing a new Benefits Processing and Member Self-Services IT system. The legacy system was significantly aged and in some cases did not provide management with appropriate levels of information and in other cases contained corrupted or incomplete data. In addition to servicing the needs of the MTRS, the information contained in the MTRS member system is also utilized by the Public Employees Retirement Administration Commission (PERAC) to calculate a projected pension liability, a significant accounting estimate that is part of the financial reporting process. To compensate for the anomalies in the data, PERAC makes adjustments to its actuarial model before finalizing its results, results that ultimately impact future requirements for the Commonwealth. The MTRS has made efforts to update the accuracy of the data prior to moving onto the new system however, in the current year testing it was noted that some of the data integrity issues noted in prior years continued to appear.

Recommendation

We recommend that the MTRS conduct a review to identify inconsistent, inaccurate, or corrupted data within the data that has been moved to the new system. Once the review is complete, we recommend that the data be scrubbed and updated to the extent possible. We would also recommend that the MTRB enforce strict guidelines on external entities that provide information to the system to reduce the level of inaccurate or inconsistent member data.

Management's Corrective Action Plan

As noted previously, starting in 2007, MTRS established a dedicated Data Cleansing and Conversion Team (TEAM) in preparation of replacing our legacy system with a new line of business application. We continue to clean the data of our membership as we prepare for the final data conversion effort associated with Rollout three (R3) Benefits Processing and Member Self-Service. Effective May of 2010, all employer deduction reports are processed through the new line of business application (MyTRS: Employer Self-service application) which has data validations that require employers to review any data anomalies that trigger an error or exception flag. These tight controls have and will continue to reduce the level of inaccurate and inconsistent member data. MTRS's data cleansing effort continues as we prepare for the final data conversion for R3 implementation, which is now scheduled for August of 2013.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

Responsible Officials

Joan Schloss, MTRS Executive Director

Implementation Date

The 2013 MTRS active and retiree PERAC actuarial data file will be reported from our new management information system.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-12

Massachusetts State Employees' Retirement System (MSERS) – Census Data

Observation

The Massachusetts State Retirement Board (MSRB) is responsible for maintaining member information for all active, inactive, and retired employees who contribute to and participate in the Massachusetts State Employees' Retirement System (MSERS). The database of information is gathered from several different sources and in some cases in various different formats including both state and non-state entities. The system that is currently used is significantly aged and in some cases does not provide management with appropriate levels of information and in other cases contains incomplete data. In addition to servicing the needs of the MSERS, the information is also utilized by two actuarial groups (PERAC and Aon) to calculate a projected pension liability and other post employment benefits liability both of which are significant account estimates that are calculated as part of the financial reporting process. To compensate for the anomalies in the data, PERAC makes adjustments to its actuarial model before finalizing its results, results that ultimately impact future finding requirements for the Commonwealth.

Data errors are not unusual in large systems and do not appear to be of a magnitude that would significantly impact actuarial calculations which are performed by the Commonwealth.

Recommendation

We recommend that the MSRB continue to review and identify inconsistent, inaccurate, or corrupted data within the current member system to ensure that when data is transferred to the new system any inaccurate or corrupt data is not included. We would also recommend that the MSRB enforce strict guidelines on external entities that provide information to the system to reduce the level of inaccurate or inconsistent member data. Finally, as the MSRB continues through the process of system design we recommend that they consider future information needs and appropriate levels of control when designing the new system.

Management's Corrective Action Plan

The initial implementation of the MSRB's new computer operating system ("MARIS") is expected to go live during the first part of 2014. As part of this process, the MSRB is continuing its data cleansing efforts with the assistance of an outside vendor to update and ensure that data on the existing legacy system is accurate before being migrated to the new system. Corrupt, missing or incomplete data is being identified and a comprehensive data reconciliation strategy is underway. These measures have identified data anomalies and inconsistencies which are addressed by staff. The end result will be more consistent and accurate data for migration to the new line of business. This will have a positive short term impact on the quality of data submitted to actuarial groups.

The MSRB's current practice and policy include comprehensive reviews of member data: at the time of enrollment, prior to the initiation of benefits at the time of retirement, and when a member leaves employment, transfers service to another public employer, or otherwise separates from Commonwealth service.

Additionally, recently enacted pension reform legislation contained a significant number of changes to retirement benefits for current and new participants of the retirement system, including a new tier of benefits and different eligibility rules for new Commonwealth employees. This has also affected the design, timing and implementation of the system.

Going forward, the Commonwealth and external agencies will be required to provide more detailed, correct and accurate payroll, employment and demographic data. Inaccurate or inconsistent data submissions will be returned to external agencies and will not be accepted or posted until reviewed and corrected. This control will ensure improved data quality and management and ultimately support improved accuracy of the MSRB's business processes.

Built into the design of the new system is the commitment that data is not only being maintained for the MSRB's requirements but those of outside actuarial groups and management agencies. This commitment will allow for a flexible approach in the diversity and form in which information can be retrieved.

Responsible Officials

Nicola Favorito, Deputy Treasurer, State Retirement Board

Implementation Date

See corrective action plan narrative for implementation timeline.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-13

Group Insurance Commission (GIC) - Post-Employment Benefits Accrual

Observation

The Group Insurance Commission (GIC) provides health insurance and other benefits to state and certain authority employees, retirees, and their survivors and dependents. The GIC also provides health-only benefits to participating municipalities. Non-Commonwealth entities benefit from being part of a larger risk pool, yet remain individually responsible for the premiums associated with their own members.

GIC contracts with several third-party administrators (TPAs) to process claims. The GIC's eligibility system (MAGIC) and the amounts it pays in claims (which the GIC allocates to insured retirees and survivors) serve as the source data used by the Commonwealth's outside actuary to estimate the Commonwealth's Other Post-Employment Benefit (OPEB) obligations.

For financial reporting purposes, the Commonwealth needs to collect additional information in order to apportion the liability between the Commonwealth and non-Commonwealth participating employers on an individual claim basis. Some, but not all, of the GIC's TPAs currently provide such information. Consequently, certain assumptions are developed to provide a reasonable break down of the OPEB obligation for financial reporting purposes.

Recommendation

We recommend that the GIC develop the systems to support this financial reporting requirement.

Management's Corrective Action Plan

The GIC now receives sufficiently granular (on an individual claim basis) data (through supporting documentation) with its bills from three of its third-party administrators (TPAs). We continue to work toward collecting these data from all of our self-insured vendors (our mental health and pharmacy carve-out vendors have not yet changed their reporting). We will implement a new contract with a mental health/substance abuse effective July 1, 2013, and the chosen vendor will be required to meet our reporting needs in FY2014 pursuant to this procurement.

Responsible Officials

Catherine Moore, Budget Director, Group Insurance Commission

Implementation Date

Fiscal year 2014

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-14

Information Technology Division (ITD) – Password – CIW

Observation

Due to system limitations, password restrictions are not systematically enforced for end-users accounts gaining access to CIW.

Without a system-configured password policy, passwords may be compromised, enabling unauthorized and unmonitored access to financial information.

Recommendation

ITD should consider systematically enforcing CIW application password parameters for length, complexity, lockout, expiration, etc.

Management's Corrective Action Plan

As stated previously, CIW is not an application; rather it is a data repository and requires Security Office and Management approval before any access is allowed. It should also be noted that once that access is granted, the data type that the user is permitted to view (only Read access is permitted) is governed by their Role as assigned by the Security Office and systemically enforced by the warehouse. As noted previously, users can only access the warehouse via a valid LANID which systemically enforces a strong password policy.

Because the CIW is not an application, there is no way to systemically support or enforce password restrictions without a front-end security module. Due to significant budgetary constraints, the required funding hasn't been available. The CIW is looking to partner with ITD Security and the current IDM initiative to see ascertain if IDM can be leveraged to remediate this finding. It is to be noted that several applications within ITD have successfully been integrated utilizing IDM. ITD expects that this initiative would be completed by September 2013, as the contractor was assigned to integrate CIW with IDM in February 2013.

Responsible Officials

Kevin J. Burns, Chief Information Security Officer, ITD

Implementation Date

Possible IDM integration date of February 2014

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-15

Information Technology Division (ITD) – Password parameters

Observation

For the following systems the Commonwealth had some password configurations in place. However, system enforced password restrictions including minimum length, history, complexity, expiration and account lockout were not fully configured on these systems.

- HR/CMS database and servers
- Netezza servers
- NewMMARS servers

Weak password parameters increase the risk that applications may be compromised, enabling unauthorized and unmonitored access to financial information.

Recommendation

ITD should consider systematically enforcing password parameters including minimum length, complexity, expiration, account lockout etc. for these systems.

Management's Corrective Action Plan

1. HR/CMS Servers (AIX operating system) and databases are configured with complex, system enforced passwords at this time. Account lockout can be configured and the manner in which to message account lockout is being designed. Further, ITD enabled auditing relative to the databases and ITD intends to monitor the logs on monthly basis to ascertain the frequency to which accesses and changes occurred.

2. Netezza is not a server but rather is a Linux based appliance upgraded this year with another IBM product, Twinfin and the servers were configured with complex passwords in October 2012.

3. New MMARS servers (AIX operating system) are being configured with complex passwords at this time, and expects the process to be completed by June 2013.

Responsible Officials

Kevin J. Burns, Chief Information Security Officer, ITD

Implementation Date

June 2013

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-16

Office of the Comptroller (CTR) – User Access Control and Internal Control

Observation

Super-user level access via membership in the "Department Fiscal – All Functions" (DFISC) security role in the MMARS application is provided by the Office of the State Comptroller (CTR) to individuals after obtaining documented approval by the authorized department security officer. DFISC access provides the user with access rights that result in segregation of duties conflicts as the users can initiate, process, and record transactions without intervention by another user.

Manual approval and monitoring controls designed to prevent and/or detect inappropriate activity via these accounts are the responsibility of department management. The number of users with DFISC level access to MMARS has been decreased over the past two fiscal years. Currently there are approximately 500 DFISC user accounts across all departments.

In the complex organizational environment at the Commonwealth the existence of DFISC level access has been deemed appropriate by management. Given the inherent risk for unauthorized and/or inappropriate transactions to be processed in this type of environment, it is necessary to design stronger monitoring controls to manage and mitigate that risk. These controls should be designed and implemented on a robust scale that is appropriate to the number of DFISC users.

Recommendation

The Commonwealth should consider implementing a monitoring control to monitor 100% of transactions or for defined risk thresholds and/or frequency of transactions that are processed by users with super-user access.

Management's Corrective Action Plan

CTR strengthened the activities and processes around powerful access to MMARS in several ways:

- The number of DFISC users was reduced to 446.
- The Security Unit reviews each requests for powerful access in light of the department's total population of MMARS users.
- At each statewide meeting, the Comptroller raises the risk of fraud and the importance of being vigilant in reviewing what fiscal staff is processing.
- The annual Department Security Officer briefings communicates the risks associated with powerful access and the importance of mitigating controls.
- Security reports that identify when user activities indicate the potential for fraud are published monthly.
- Queries that identify risky situations are available in the CIW for department use.
- The Quality Assurance Bureau reviews risky situations and requests supporting documentation from departments: the frequency of desk reviews has increased to at least twice/year/department.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

In FY13, the following actions are occurring:

- The annual certification by the Department Head of enterprise systems access will include a statement indicating that a member of management is reviewing security reports detailing what staff are processing in MMARS.
- The Internal Control Questionnaire will be expanded to require confirmation that review of MMARS user activity happens at least monthly.
- The importance of reviewing available security reports will be highlighted in detail at the annual DSO briefing, as well as the annual CFO and Fiscal Year Close\Open meetings.
- The Department Assistance Bureau will send quarterly reminders to departments of the availability of the monthly user activity reports via eUpdate notification.

Responsible Officials

Joan Shea, Deputy Comptroller, Office of the State Comptroller

Implementation Date

By November 2013 for the last three bullets. All other items are implemented.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2012

MLC 2012-17

Office of the Comptroller (CTR) – End User Developed Application (EUDA)

Observation

The Office of the Comptroller (CTR) uses MS Excel to create year-end financials. We noted that that passwords to some fund source excel files were available to analysts who do not work on the funds. Further, CTR has not documented a description of the excel file layout and inter-connections as it relates to the financial report.

Preparing complex financials using EUDAs introduces a risk that individuals with access to the files may change data or formulas without appropriate change approvals. Lack of formal documentation describing the EUDA may result in loss of understanding of the EUDA environment when the person with this knowledge leaves the organization.

Recommendation

- Document current EUDA system as it relates to the financial report.
- Implement a formal change process, which should require documented approvals when changes are made to formulas and links.
- Grant access to excel spreadsheets only to individuals who work on the spreadsheets.
- Consider using a reporting package to create year-end financials. This reporting package should be governed by formal it General Controls.

Management's Corrective Action Plan

Password access to the Excel spreadsheet is restricted at different levels.

1. Accountants in the Financial Reporting and Analysis Bureau (FRAB) who are responsible for specific funds are the only staff who can use the fund worksheets in order to review and post adjustments to their respective funds. Access to the Excel worksheets/workbooks is limited to FRAB staff. Individuals from other bureaus cannot access these files.

2. Where the information is summarized for the financial statements, the worksheets are linked to a specific macro program. If the macro program is not installed on a user's computer, the financial worksheets fail to open properly. The macro program is installed only on the computers used by FRAB accountants.

FRAB has documented the reporting process along with the security procedures in place to prevent unauthorized modification of the Excel spreadsheets used to generate the reports.

Several years ago FRAB attempted to use a financial reporting package available in the market; however the complexity of the Commonwealth's reporting stressed the features available in the program, which failed to generate acceptable reports. To date the Comptroller's Office has not been able to find software that meets our reporting requirements, but will continue to review "off the shelf" software packages to assess whether they meet the Commonwealth's reporting needs.

Responsible Officials

BJ Trivedi, Director, Financial Reporting Bureau, Office of the Comptroller
Michael Rodino, Manager, Financial Reporting Bureau, Office of the Comptroller

Implementation Date

Documentation of the EUDA system has been completed. The process of assessing the viability of "off the shelf" software packages is an on-going process.