



Commonwealth of Massachusetts

Management Letter

June 30, 2011



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

January 13, 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, 2011, and have issued our report thereon dated January 3, 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 January 3, 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

KPMG LLP is a Delaware limited liability partnership,
the U.S. member firm of KPMG International Cooperative
("KPMG International"), a Swiss entity.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-01

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

The software used by CTR for debt monitoring, DBC- Debt Manager, had certain limitations prior to FY12. The program calculated the amortization of bond premiums and discounts based on the outstanding principal method only. The software designer has informed us that a new module is now available to amortize net bond premiums, discounts and issuance costs using the GAAP required effective interest method. CTR will attempt to implement this new module in FY12.

Responsible Official

B.J. Trivedi, Director, Financial Reporting Bureau, Office of the Comptroller

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-02

Accounting for Derivatives

Observation

The preparation of financial statements in accordance with U.S. generally accepted accounting principles (GAAP) requires that the Commonwealth comply with a wide array of regulations. In certain instances the Commonwealth has chosen to not apply GAAP, but rather take a more practical approach to the accounting. While permissible for immaterial items, the Commonwealth is none-the-less required to monitor these so-called non-GAAP policies and assess their materiality each time financial statements are prepared. If the impact of any individual non-GAAP policy is material to the financial statements, then the Commonwealth would be required to address the matter. During our audit we noted that the Commonwealth does not document its accounting and reporting elections as well as the magnitude of the GAAP departures.

Specifically during our audit, we identified several Non-GAAP items related to the implementation of the new standard related to accounting for derivatives. The Government Accounting Standards Board (GASB) guidance for the accounting and reporting of derivative activity is complex and evolving to meet the current economic climate. As such, proper implementation of the standard requires a thorough understanding of the literature as well as underlying transactions (including subsequent refunding of hedged debt). The non-GAAP items included:

- Recognition of termination accounting due to:
 - Replacement of a counterparty
 - Refunding of underlying debt
- Recognition of investment accounting due to an over-hedging situation

These 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. For such a highly complex topic, the two primary groups responsible for derivative activity (Treasury and Comptroller) should meet regularly to discuss recent developments in both derivative activity and the reporting requirements thereon.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

Management's Corrective Action

Treasury is in the process of documenting the accounting and reporting elections as well as overall summary of the derivative accounting rules. This documentation will include a template that can be updated annually to quantify the magnitude of the GAAP departure.

Responsible Officials

B.J. Trivedi, Director, Financial Reporting Bureau, Office of the Comptroller
Colin MacNaught, Office of the State Treasurer
Sue Perez, Office of the State Treasurer

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-03

Accounting for Refunding of Grant Anticipation Notes

Observation

The Commonwealth initially overstated its fund balance by approximately \$184 million by incorrectly accounting for payments to escrow agent as cash held by fiscal agent. For GAAP reporting, payments to escrow agents as part of refunding of existing debt should be reported as other financing uses. This item was corrected prior to the issuance of the fiscal 2011 Comprehensive Annual Financial Report (CAFR).

Recommendation

We recommend that all refunding be accounted for in accordance with GAAP.

Management's Corrective Action Plan

The Comptroller's Office agrees with this comment and will document and implement procedures to correctly record refundings of this type in the FY12 Statutory Basis Financial Report (SBFR) and Comprehensive Annual Financial Report (CAFR).

Responsible Official

B.J. Trivedi, Director, Financial Reporting Bureau, Office of the Comptroller
Neil Gouse, Financial Reporting Bureau, Office of the Comptroller

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-04

Timing of Departmental Charge-backs for Fringe Benefit and Indirect Cost Allocations

Observation

During fiscal 2011 it was noted that several accruals related to fringe and indirect charge-backs were not captured in the correct fiscal year. The two primary examples of these timing issues were charge-backs which should have been made by the Office of the Comptroller to the Department of Education and the Massachusetts Department of Transportation (via the Commonwealth Transportation Trust Fund).

Recommendation

We recommend that management review its policies and procedures regarding oversight of year-end close out, particularly as it relates to the charge-back process and determine if additional controls are needed to ensure that administrative charge-backs are processed in the correct fiscal year.

Management's Corrective Action

The timing issue with respect to the Massachusetts Department of Transportation was related to payments from the Massachusetts Turnpike Authority (MTA). MTA was not on the MMARS accounting system at the time FY10 chargebacks were processed. This resulted in chargebacks being paid by check and spilling over from FY10 to FY11. With the MTA now part of the Massachusetts Department of Transportation on MMARS, and thus part of the automated electronic chargeback process, payment of MTA chargebacks by check is no longer an issue. To prevent other timing-related issues, the Comptroller's Office will document and implement a closing process in FY12 that will result in end of year chargebacks being processed in a timely and accurate manner.

Responsible Official

Taneka Simmons, Director, Federal Grants and Cost Allocation Bureau, Office of the Comptroller

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-05

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 test work that for several departments retainage was not capitalized until it was ultimately paid as opposed to when the costs were incurred as required by 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

We will emphasize proper accounting of retainage in the Capital Asset Reporting Policy Guide for FY 2012. We will also work with the Internal Audit group of the Comptroller’s Office to determine if the departments are following the policy properly.

Responsible Official

B.J. Trivedi, Director, Financial Reporting Bureau, Office of the Comptroller
Trish McKenna, Financial Reporting Bureau, Office of the Comptroller

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-06

Compliance with Comptroller Policies and Procedures

Observation

The Office of the Comptroller (CTR) is responsible for the implementation and enforcement of policies and procedures designed to enhance the Commonwealth's internal control over financial reporting. CTR has developed an Internal Control Questionnaire (ICQ) in order to monitor compliance with these policies and procedures and to gain comfort over the departmental control environments.

As part of our audit risk assessment procedures, we analyzed certain responses received in 2011 to the ICQ. We noted a few departments failed to appropriately update their internal control plans (ICPs). The current Comptroller policy requires that internal control plans be reviewed and updated on an annual basis.

Recommendation

We recommend that the CTR reinforce the requirement to have accurate and updated internal control plans in place.

Management's Corrective Action Plan

We will continue to review the ICP as part of each site visit we conduct and comment on them in our Quality Assurance reports. The State Auditor (SAO) also reviews ICPs at each of their site visits, including during their single audit fieldwork. The SAO assessments of department ICPs are published in a separate report. We have used the ARRA related department reviews as another opportunity to review ICPs in total (not just for ARRA updates). This has revealed cases where some departments have not implemented previous recommendations. Thus, we are conducting a desk review that follows up on all of our ICP recommendations in 2011 reports to ensure that they have been, or are being, implemented. Per standard practice, QAB will document and contact each department responding on the annual Internal Control Questionnaire that their plans were not updated and determine next steps. The Department Assistance Bureau offers standard classroom training on Internal Control Plans, as well as department-specific training upon request or recommendation. Finally, the Office of the Comptroller will continue to remind departments of the ICP requirements in its internal control guidance, the Close\Open Handbook, in meetings such as the CFO conference and the annual fiscal year Close\Open meetings, and at each New CFO training session.

Responsible Official

Peter Scavotto, Director of Quality Assurance, Office of the Comptroller

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-07

Department of Workforce Development (DWD) – Reconciliation of Cash Accounts

Observation

DWD maintains an independent IT system for the facilitation of program operations and administration. Activity from the non-integrated DWD system is aggregated and input into MMARS on a summary basis. In the current and prior year audits it was noted by KPMG that several DWD cash accounts and corresponding accounting transactions were not properly captured on and reconciled to MMARS.

Recommendation

We recommend that the Comptroller and DWD evaluate the recording of transactions in MMARS regarding unemployment compensation benefits. Every effort should be made to perform complete and accurate reconciliations between the Department's activities and MMARS. All cash belonging to the Commonwealth should be reflected in the general ledger and ultimately in the financial statements. Proper cut-off should be followed by the Department.

Management's Corrective Action Plan

DWD management will continue to work with internal process owners and the Office of the Comptroller to evaluate and accurately perform daily and monthly reconciliations between the Department's activities and the MMARS accounting system in timely manner.

Responsible Official

Barbara McDonough, Director of Financial Services

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-08

Department of Workforce Development (DWD) – 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. The allowance analysis while improved 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 shown in the aged account receivable report, in conjunction with an analysis of the collections against last year's debt. DWD will continue to build historical accounts receivable data.

Responsible Official

Barbara McDonough, Director of Financial Services

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-09

Massachusetts Teachers' Retirement System (MTRS) - Census Data

Observation

The Massachusetts Teachers' 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 funding 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

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

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

to review any data anomalies that trigger an error or exception flag. These tight controls will 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 scheduled for December of 2012.

Responsible Official

Joan Schloss, MTRS Executive Director

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-10

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 accounting 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 funding 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 MSRB is currently more than eighteen months into the process of developing and implementing a new system that is expected to go live in 2013. As part of this process the MSRB has undertaken various reviews to ensure that data on the existing system is accurate before being transferred to the new system. MSRB's current practice and policy include, comprehensive reviews of member data that are performed prior to the initiation of benefits at the time of retirement, or when a member leaves employment, transfers service to another public employer, or otherwise separates from Commonwealth service.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

As part of the new line of business implementation all the data contained in the MSRB's current legacy system is being reviewed in conjunction with an overall data cleansing effort being undertaken by an outside vendor. Corrupt, missing or incomplete data is being identified and a comprehensive data reconciliation strategy is underway. 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.

As part of this implementation, external agencies will be required to provide correct and accurate work 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 "Board'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 Official

Nicola Favorito, Deputy Treasurer, State Retirement Board

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2012-11

Department of Housing and Community Development (DHCD) - Accounting, Reporting and Safeguarding 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 \$250 million at June 30, 2011. The majority of these loans are interest free with maturity dates that can extend for up to forty years. The first of these loans are scheduled to mature on June 23, 2012 (\$270,000). The majority do not mature until well after 2025. During our audit, we noted the following:

- The net realizable value of these loans has never been captured as part of the financial reporting process.
- The loan instruments are stored on the premise in locked file cabinets, which may not be the most secure environment.
- DHCD has not documented its position on the “continuing compliance” component of these loans.

Recommendation

We recommend that DHCD review the accounting, reporting and safeguarding 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.
- Safeguarding controls should be continually monitored and updated to ensure these valuable and moveable assets are properly secured from unauthorized access and or misappropriation.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

- DHCD should document its position on the “continuing compliance” component of all its federally funded loans and review that policy with its federal representatives to ensure proper adherence to federal compliance regulations.

Management’s Corrective Action Plan

We have implemented measures to more adequately safeguard the TCAP and HOME Promissory Notes and will provide reports to the Comptroller’s Office regarding the TCAP and HOME assets, as directed. We will continue to take all steps necessary to comply with the regulatory requirements, as well as the U. S. Department of HUD’s Continuing Compliance requirements, of these two programs and to address all KPMG observations and recommendations.

Responsible Official

Wendy Cohen, TCAP Program Manager
JoAnn McGuirk, HOME Program Manager
Kate Racer, Associate Director Housing Development

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-12

New Guidance on Service Organization Controls (replaces previous SAS 70 guidance)

Observation

Recent internal control breakdowns (e.g. security and privacy breaches, and frauds) and increasing regulatory focus on internal controls (e.g. Health Information Technology for Economic and Clinical Health Act (HITECH) and Health Insurance Portability and Accountability Act (HIPAA)), have resulted in the American Institute of Certified Public Accountants (AICPA) amending and expanding the services and reports that independent CPA firms provide to users of third-party service organizations.

The expanded services and reports referred to as Reports on Controls (ROC) address the following:

- ROC1 Report addresses controls likely to be relevant to user entities financial statements
- ROC 2 Report addresses one or more of the following five key system attributes:
 - o Security
 - o Availability
 - o Process Integrity
 - o Confidentiality
 - o Privacy
- ROC 3 Report addresses the same key controls as ROC 2 in a general-use report with no description of test/results or opinion

The Commonwealth, and specifically departments such as the Group Insurance Commission (GIC), the Office of the Treasury (TRE), and the Executive Office of Health and Human Services (EOHHS), rely extensively and sometimes exclusively on third-party service providers for transaction processing services.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

Recommendation

We recommend that the Commonwealth determine which departments are currently utilizing third-party service providers for key financial or operational services and update or amend existing contracts to properly reflect the new guidance and more importantly the proper level of service auditor report (ROC 1, 2 or 3).

Management's Corrective Action Plan

The Office of the Comptroller will identify the departments which use third-party service providers of financial and/or operational services and arrange for a vendor to deliver training on the new Reports on Controls so that departments are aware of their responsibility and update existing contracts accordingly.

Responsible Official

Peter Scavotto, Director of Quality Assurance, Office of the Comptroller

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-13

Information Technology Division (ITD) - Password – CIW

Observation

Password restrictions are not systematically enforced for end-users accounts used to access CIW.

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

Recommendation

Information Technology Division (ITD) should consider systematically enforcing CIW application password parameters for length, complexity, lockout, expiration, etc.

Management's Corrective Action Plan

CIW is not an application but a data repository which, with Security Officer approval, is accessed via a desktop application such as Microsoft Access. Desktop access requires the user have a valid LAN ID which does systemically enforce a strong password policy. Within the CIW itself, however, there is no way to systemically support or enforce password restrictions without developing a front-end security module. The required funding was not available in FY10 and security development remains as pending.

We are currently assessing the future direction of the CIW and the provision for systemically enforced password parameters for length, complexity, lockout and expiration is recognized as a critical element.

Responsible Official

Maureen Chew, Chief Application Officer, ITD
Lou Angeloni, Chief Financial Officer, ITD

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-14

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 application, database and servers
- Netezza servers
- New MMARS 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 the above listed systems.

Management's Corrective Action Plan

We are currently assessing the future direction of these systems and the provisioning for systemically enforced password parameters for length, complexity, lockout and expiration is recognized as a critical element.

Responsible Official

Maureen Chew, Chief Application Officer, ITD

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-15

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 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 those transactions that meet defined risk thresholds and/or frequency of transactions that are processed by users with super-user access.

Management’s Corrective Action Plan

CTR continues to evaluate all requests for DFISC profiles in MMARS, monitoring the number of users, the percentage of users with broad access and the justification for department requests. The Department Assistance Bureau meets with individual Department Security Officers (DSO) when it appears that tighter internal segregation of duties is possible (20% of security requests). This has resulted in a decrease each year. Detailed security data is now available via query in the Commonwealth Information Warehouse (CIW) and via standard reports in DocDirect. This data allows each department to monitor the system activity of all of its users – tracking transaction volume by user, as well as detail on which user IDs create and submit each encumbrance and payment transaction. CTR worked with the Information Technology Division (ITD) and a subset of operating departments to develop these starter queries and reports, based on the Quality Assurance Bureau’s (QAB) desk review process (see below) that is now being rolled out statewide.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

QAB continues its System User Activity desk review of 100% of departments annually requesting supporting documentation for evidence of segregation of duties and signatory approval on selected transactions. To audit every transaction processed by all users is not feasible given 60 million transactions per year, but the availability of a self-monitoring tool for departments will help address this recommendation. The annual briefing of DSO's will continue to highlight the importance of mitigating risk and, this year, will highlight the availability of security data in CIW.

Responsible Official

Joan Shea, Deputy Comptroller

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

MLC 2011-16

CTR - End User Developed Application (EUDA)

Observation

The Office of the Comptroller (CTR) uses MS Excel to create year-end financials. We noted 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 ones 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 relationship between the linked spreadsheets but will review that documentation to ensure that the documentation is complete, and a formal change process for changing formulas and links will be implemented for the FY12 financial reports.

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2011

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 an acceptable form of financial statements. To date the Comptroller's Office has not been able to find software that meets our reporting requirements.

Responsible Official

B.J. Trivedi, Director, Financial Reporting and Analysis Bureau, Office of the Comptroller