

---

# ***Metropolitan Transportation Commission***

## **Internal Controls Report**

October 26, 2016





October 26, 2016

Brian Mayhew  
Chief Financial Officer  
Metropolitan Transportation Commission  
375 Beale Street  
San Francisco, CA 94105

Dear Brian:

In planning and performing our audit of the financial statements of Metropolitan Transportation Commission ("MTC") as of and for the year ended June 30, 2016, in accordance with auditing standards generally accepted in the United States of America, we considered its internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the Company's internal control over financial reporting. Accordingly, we do not express an opinion on the Company's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified.

AICPA AU-C 265, *Communicating Internal Control Related Matters Identified in an Audit*, of the AICPA Professional Standards includes the following definitions of a deficiency, a significant deficiency and a material weakness:

Deficiency - a deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.

Significant deficiency - a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Material weakness - a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Based on prior years' practice, we are providing you with a full detail report of all deficiencies.



This letter is intended solely for the information and use of the Commissioners, management, others within MTC and governmental granting agencies and is not intended to be and should not be used by anyone other than these specified parties.

If you would like any further information or would like to discuss any of the issues raised, please contact Joan Murphy at (415) 498-7690.

Very truly yours,

cc: Steve Heminger, Executive Director  
Eva Sun, Deputy Finance Officer  
Susan Woo, Deputy Treasurer  
Suzanne Bode, Accounting Manager

## Contents

<i>Current Year Recommendations.....</i>	<i>1</i>
A. Business Process Controls.....	1
1. Ensuring Purchase Requisitions Obtain the Proper Level of Approval .....	1
B. Information Technology General Controls .....	2
1. Formalize Change Management Policy and Processes (IFAS/OneSolution and ATCAS II) .....	2
2. Domain Password Policy (IFAS/OneSolution) .....	3
3. User Provisioning and Access Review (IFAS/OneSolution).....	3
4. Developer Access to Production (ATCAS II) .....	4
<i>Prior Years' Recommendations.....</i>	<i>5</i>
A. Business Process Controls.....	5
1. Ensuring the Physical Existence of Fixed Assets (Open) .....	5
2. Timely Recording of SAFE Callbox Disposals and Depreciation (Closed) .....	6
3. Approval of Travel Expenses (Closed).....	7
4. Reviewing Create and Post Journal Entries (Closed) .....	8
5. Verifying Completeness and Accuracy of Census Data Used by CalPERS for Pension Valuations (Closed).....	9
B. Information Technology General Controls .....	10
1. Definition of the Roles and Responsibilities for ATCAS II System Support (Open) .....	10
2. Application Access Management (Open) .....	12
3. Formalize Change Management Policy and Processes (Open) .....	13

## ***Current Year Recommendations***

### **A. Business Process Controls**

#### **1. Ensuring Purchase Requisitions Obtain the Proper Level of Approval**

##### **Observation**

Per MTC's Purchase Requisition Approval policy, General Requisition in an amount under \$25,000 may be signed and approved by the relevant Section Director. Purchase requisitions between \$25,001 and \$200,000 must be signed by the Deputy Executive Director and Requisitions over \$200,001 must be approved by Committee and signed by the Executive Director. Additional approval may need to be acquired from Office of General Counsel, Manager of Administrative Technology Services, or Administration Committee depending on the type of purchase.

As part of our testing of internal controls, we observed a purchase requisition in the amount of \$32,420 which lacked required approval by a Deputy Executive Director.

##### **Impact**

If the purchase requisition approval process is not adhered to, there is a risk that unauthorized or inappropriate purchase requisitions could be approved which could lead to the inappropriate expenditure of funds.

##### **Recommendation**

We recommend that MTC re-emphasize the importance of adhering to approval requirements in internal communication/training and implement monitoring controls to ensure the policies and procedures are complied with. Some examples of safeguards are manual reviews or system based workflow restrictions.

##### **Management Response**

MTC's Contracts unit will implement electronic routing of requisitions to ensure that all required approvals are obtained. Implementation is expected to be completed prior to June 30, 2017.

## B. Information Technology General Controls

### 1. Improve Change Management Processes (IFAS/OneSolution and ATCAS II)

#### Observation

As part of our audit, testing was performed over a sample of application changes in IFAS/OneSolution and ATCAS II. We discovered that some changes were not reviewed or approved and/or formal documentation was not maintained of the review/approval.

As a result, we were required to perform additional manual substantive testing to support the fiscal 2016 financial statement audit.

As of the time of our testing and through to the conclusion of our year-end fieldwork, no documentation of MTC's formal change management policy had been provided; however, a system wide change management policy was provided after testing had concluded. Accordingly, we were unable to perform testing of adherence to MTC's policy.

#### Impact

We believe a formal change policy is vital to a mature IT control environment. Clearly communicated policies can provide guidance on the nature and extent of testing and review performed in a test or production environment depending on the assessed risk. In addition, such policies, when adhered to, can ensure that all changes are reviewed and approved as desired. A lack of effectively operating change management controls increases the risk that inappropriate or erroneous changes could be made without detection.

#### Recommendation

We recommend that the Organization ensure that application changes are reviewed and approved and that such review and approval is formally documented. Building specificity around the level of review needed for different types of changes would aid the Organization in appropriately executing change management controls.

#### Management Response

Management will review its current system-wide change management policy as it applies to IFAS/OS and make any necessary changes and/or clarifications with regards to this application.

BATA follows change management processes for changes to the ATCAS production environment. BATA will apply these processes consistently for all changes. These processes are audited yearly, and management believes they are right-sized for the ATCAS financial system.

## 2. Domain Password Policy (IFAS/OneSolution)

### Observation

Per MTC policy, procedures exist and are followed to maintain the effectiveness of authentication and access mechanism for application - authentication mechanism requires each user to log on using a username and password. Minimum password quality requirements are enforced by the application.

PwC noted that the MTC Network policy did not include a clear requirement for password changes and additionally noted that the MTC Active Directory password configurations do not require users to change their passwords. Because the IFAS/OneSolution application relies on the MTC Active Directory for authentication, IFAS/OneSolution users are not required to change passwords at certain intervals.

### Impact

An absence of regular password changes can lead to a greater risk of inappropriate access to key systems.

### Recommendation

It is recommended that MTC implement a program whereby routine password changes are required within the MTC Active Directory.

### Management Response

Management agrees with this comment and will work with the Executive office to create a policy for regularly changing passwords meeting strength criteria.

## 3. User Provisioning and Access Review (IFAS/OneSolution)

### Observation

PwC noted that two users added to the IFAS/OneSolution application during the FY 2016 were provisioned roles that were not formally requested or approved on the Access Request forms. For one user, PwC noted that the user was requested to have accounts payable report access but instead was provisioned accounts receivable report access. For another selected individual, the user was requested to have access to create purchase orders for Dept. 18, but was instead provisioned access to create purchase orders for Dept. 1.

Further PwC noted that the annual review of user access to IFAS/OneSolution is performed by the ERP Analyst by examining access levels of each user within the system for what they currently have to what their access was set at the end of the prior fiscal year. The review is a lookback procedure to note if a user's access has changed during the fiscal year and to note that there is a valid form to track the change in access; however the two instances noted above were not identified by this review. As such PwC noted both a design deficiency with the control as well as a deficiency in the operating effectiveness of the control.

**Impact**

As the ERP Analyst is a member of the IT organization and not the business/finance organization, he is not presumed to have the ability to determine if a user's current access is appropriate per his/her current functional business role. For example, for an accounts payable clerk, the ERP Analyst would not necessarily be aware of the access required for the individual's current role such as whether the employee needs access to run reports, view certain GL accounts, etc. Inappropriate access to key systems has the potential to lead to a breakdown of segregation of duties.

**Recommendation**

It is recommended that the review be performed by a knowledgeable individual and that the individual also ensures that data was input accurately into the system as part of his/her review of the change request form. For example, there should be a check that all changes made in the system are in accordance with the approved request forms/provisions.

**Management Response**

Management acknowledges the issue stated in this comment. In order to address this issue, the accounting manager will also perform an annual review in conjunction with IT to ensure that data entry is correct and levels of authorization are still appropriate.

**4. Developer Access to Production (ATCAS II)****Observation**

PwC identified multiple contracting developers with access to the production operating system and database. PwC additionally noted one user from a third party provider who has access to the production environment.

**Impact**

Developer access to the production environment creates a risk of inappropriate system changes with a limited possibility of being able to log those changes. This creates the opportunity for fraud and increases the risk of undiscovered errors.

**Recommendation**

It is recommended that developers not be given access to production. If developer access is deemed vital for efficient operating procedures, the goal of segregation of duties can be achieved by allowing developer changes to be made to the production environment only after the change has been appropriately reviewed and approved by IT Operations.

**Management Response**

Management is currently working with the ATCAS II developer and its subcontractor to limit production access. Restriction considerations may include read only access, read/write access for specific maintenance windows as approved by BATA IT, and implementation of an access tracking system.



## ***Prior Years' Recommendations***

### **A. Business Process Controls**

#### **1. Ensuring the Physical Existence of Fixed Assets (Open)**

##### **Observation**

We observed that management currently does not have a formal procedure to monitor the existence and usage of non-IT assets individually below \$5,000 and used for more than one year as these assets are not capitalized in MTC's fixed asset ledger and therefore tracked. Furthermore the process to track the existence of IT assets (laptops, phones, tablets etc.) is performed by the IT department but this process is not formalized or reconciled to the fixed asset ledger records maintained by Finance.

##### **Impact**

Management has limited capability to ensure that purchased items valued individually less than \$5,000 are still in the possession of the entity as these assets are not identified in formal records and therefore their existence is not monitored. There is a risk/possibility of asset misappropriation/theft and the entity incurring additional expenses to then replace the asset.

##### **Recommendation**

We recommend that management a) re-consider the capitalization threshold of \$5,000 as this amount is relatively high compared to the price of certain items typically included in MTC's fixed assets and b) consider whether this is an optimal threshold of fixed assets to track for existence. The process of ensuring the physical existence of assets will become more crucial as MTC moves to its new headquarters and purchases a significant amount of fixed assets.

##### **Management Response from 2015**

Management will work on implementing a new inventory tracking system in conjunction with the move to the new office at Beale Street. Management has already purchased the software and this system will be maintained by the Administrative Services section.

##### **PwC Update for 2016**

MTC is in possession of AssetTrak ARS by BMI Systems, a fixed asset scanning system that would integrate with One Solution, MTC's existing financial accounting application. However, the AssetTrak system was not installed due to issues with the One Solution application which were resolved with the One Solution upgrade that took place in May 2016. Due to resource constraints management decided to delay installation until December 2016. Management's goal is that this new system will be utilized within the fixed assets and inventory processes in the second half of FY 2017.

## 2. Timely Recording of SAFE Callbox Disposals and Depreciation (Closed)

### Observation

Per MTC SAFE's fixed asset policy, disposals of capital assets are to be recorded in the general ledger ("GL") during the period in which the transactions occur. Furthermore, depreciation should begin when an asset is placed into service. We observed that in FY2015, there were callbox disposals recorded in the GL that were actually disposed of in FY2011, FY2012, FY2013 and FY2014. We also noted that there were other callboxes that began depreciating in FY2015 although those callboxes had been placed into service in FY2011, FY2012, FY2013 and FY2014.

These transactions were not recorded timely in the GL because the service operator performing the annual count of the callboxes miscounted the number of callboxes and reported the incorrect number of callboxes to MTC SAFE's accounting department.

### Impact

Recording the callbox disposals in the wrong period resulted in an overstatement of both the cost and related accumulated depreciation of capital assets in FY2011-FY2014.

### Recommendation

We recommend that management re-evaluate the physical count and reconciliation procedures related to callbox annual counts, so that accurate additions or disposals will be timely communicated to MTC SAFE accounting department to update its records.

### Management Response from 2015

Effective July 2, 2015, management hired a new contractor, Case Systems Inc. This contractor has a better maintenance and inventory tracking system. In addition, MTC staff will also participate along with the contractor when they perform the annual inventory counts.

### PwC Update for 2016

In December 2015, MTC staff performed a site visit with the contractor and conducted an inventory count. It was confirmed that the inventory reconciled with the record. As such, this item is considered closed.

### 3. Approval of Travel Expenses (Closed)

**Observation**

MTC's preferred travel service vendor is Great Escapes. Employees who are required to travel can book their airfares through Great Escapes, who will then issue an invoice to MTC requesting payment. Since the expenditure gets paid via the accounts payable invoice payment process instead of getting charged on a corporate credit card, such items could be omitted from the travel expenditure authorization form, which typically lists all travel related expenses including corporate credit card expenses; travel expenses that are not paid via credit card are manually added onto the list, and the authorization form gets submitted for approval.

In January 2015, MTC updated its policy and procedures with regards to travel expenses, to improve the submission and approval of travel expenses.

**Impact**

If the travel authorization process is not robust enough, then there is risk that inappropriate or unauthorized travel could occur and get paid for by MTC.

**Recommendation**

We recommend that management ensure appropriate policies and procedures are in place for approving travel expenses, and implement monitoring controls to ensure the policies and procedures are complied with.

Management should also review and identify whether there are other travel service vendors that are paid through the invoice payment process, such that they could unintentionally be excluded from the travel authorization process.

**Management Response from 2015**

Management will have all employees submit a complete travel expenditure authorization form for approval. This form incorporates the total budget request for the travel which includes the airfare, hotel, conference fees, local travel, and per diem.

**PwC Update for 2016**

Employees prepare a travel authorization form. The form can include expenses incurred by the employee as well as items included on a corporate charge card as well as air fare booked through the travel service vendor, Great Escapes. Approval for airfare booked through Great Escapes is provided on the invoice or via the travel authorization form. As such, this finding is considered closed.

#### 4. Reviewing Create and Post Journal Entries (Closed)

**Observation**

On a monthly basis, a system administrator identifies all people with journal entry create and post rights and then independently reviews the transaction listings for all these employees and identifies all entries where system create and post identifiers match i.e. the same person is the creator and poster (approver) of the journal entry. These entries are reported to the General Accounting Manager who ensures all these entries have been reviewed and approved by an independent reviewer evidenced by a wet signature on the journal document. However, in most cases the entries created and posted are by the General Accounting Manager and therefore the review performed is not an effective control procedure as the General Accounting Manager is reviewing his/her own work.

**Impact**

Without an effective process for reviewing journal entries that have been created and posted by the same person there is a risk of inappropriate journal entries being recorded and an entity's assets mismanaged. Segregation of duties is critical to such a process.

**Recommendation**

We recommend that the review of journal entries that have been created and posted by the same person be performed by someone who does not have the ability to create and post their own journal entries. We also recommended that the report used for this control be generated from the system by the reviewer and not from IT.

**Management Response from 2015**

Finance management will generate the report that identifies users that have created and posted the same journal entry rather than IT as IT has all system access. The report will be run monthly and reviewed by Finance management that does not have the ability to create and post journals. This task will be incorporated into the monthly close schedule.

**PwC Update for 2016**

A report generated from IFAS used to identify users that have created and posted the same journal entry is now run and reviewed by a member of finance management that does not have the ability to create and post journals. As such, this finding is considered closed.

## 5. Verifying Completeness and Accuracy of Census Data Used by CalPERS for Pension Valuations (Closed)

### Observation

Management performed procedures to check the completeness and accuracy of the census data file used by CalPERS' actuary to determine MTC's net liability and pension expense for its pension plan under GASB Statement No. 68, Accounting and Financial Reporting for Pensions ("GASB 68"). Management identified matters for further investigation with CalPERS, related to certain inactive members, which were resolved. Following completion of management's verification procedures, we tested a sample of active members in the census data file and noted the following differences between management's data and CalPERS' data which required management to perform additional investigation relating to:

- Date of hire – differences between management's records and CalPERS' for five members of the plan
- Pensionable compensation - differences between management's records and CalPERS' for one member of the plan

Management investigated these items (finding that the CalPERS amounts were accurate) and reperformed their validation of date of hire and pensionable compensation amounts for other members of the plan. After management completed this re-validation of the data, we selected an additional sample of active members in the census data file and noted no exceptions from our testing.

### Impact

Census data underpins the calculation of MTC's net pension liability and pension expense under GASB 68 and therefore inaccurate or incomplete census data may result in a misstatement of those amounts.

### Recommendation

We recommended that management formalize procedures related to census data checks by documenting the process and controls to be followed by staff performing the census data checks, so that such checks are more easily performed. In subsequent years management may also consider obtaining from CalPERS a roll forward of the census data from one year to the next and review a reconciliation for any significant differences for which support is required.

### Management Response from 2015

This was the first year management has received a file with information from CalPERS regarding eligible employees and retirees. With this first year experience with the census data completed, management will formalize procedures to verify and confirm census data for the next year.

### PwC Update for 2016

MTC's Human Resources department has developed a set of procedures to validate the information in the census data sent by CalPERS and applied the procedures to the census data file used for the FY 2016 audit. As part of the FY 2016 financial statement audit PwC did not note any census data issues. This finding is considered closed.

## B. Information Technology General Controls

### 1. Definition of the Roles and Responsibilities for ATCAS II System Support (Open)

#### Observation

There is an established contractual relationship with the ATCAS II system vendor (the “Contractor”) that provides a high-level overview into the responsibilities and roles played by the Contractor with respect to the administration and operation of ATCAS II.

Additionally, there are detailed manuals developed for the ATCAS II support personnel detailing the procedural guidance for maintenance and operation of the ATCAS II system by BATA and Caltrans Toll Operations.

However, there is currently no formal documentation outlining the responsibility for every-day activities such as those related to managing ATCAS II access, change management and infrastructure support, to delineate between the Contractor and BATA (IT, Finance, Operations) and establish a formal Service Level Agreement (“SLA”) for the system operations support. Specifically, we noted the following:

- a) The Contractor’s developers have access to ATCAS II production databases and we noted that a number of changes were migrated to production by development personnel. Even though a change management process is followed, currently there is no detective review performed by BATA Management to ensure that the version approved during testing is consistent (unchanged) from the version promoted into production.
- b) The Contractor provides BATA management with the ATCAS II application backup status reports on a monthly basis. We noted instances of incomplete and/or missed backups earlier in the year noted on the status reports. Even though there is a monetary penalty enforced for the unsuccessful backup completion cases, and the backups were noted to complete successfully later in the year, there is currently no process in place to track and resolve the root cause of the incomplete backups to ensure full remediation.

#### Impact

Without a complete and accurate set of ATCAS II roles and responsibilities, including a detailed SLA with the third party service provider, there is an increased opportunity for misunderstanding of the roles and responsibilities, as well as expectations of Management.

As it relates to developer access to production, without segregating the developer and promote-to-production functions, there is an increased risk that changes will be made to the ATCAS II system without sufficient testing or approval, leading to a potential for incomplete/inaccurate transactions processing, inaccurate data, or fraud.

Without reliable backups, there is an increased risk of data loss, interruptions to user service, inability to restore in the event of an emergency leading to an inability to process transactions systematically, and increased costs associated with manually taking tolls.

**Recommendation**

BATA Management (Finance, IT, Operations) and the Contractor should evaluate responsibilities and document expectations for each group, including a formal SLA with the service provider. Potential areas for consideration include:

- Change Management roles and responsibilities, including segregating or monitoring of developer access to production; and
- Computer operations roles and responsibilities, including performing backups, monitoring backup success/failure, researching/resolving backup failures, monitoring interfaces between systems, researching/resolving failed interfaces, performing recovery tests, approving recovery tests, retaining documentation, prox card administration, user configurable settings, etc.

**Management Response from 2015**

Following the completion of ATCAS II system acceptance and before the next fiscal year end, BATA will complete an ATCAS II operations and maintenance responsibilities matrix. The matrix will draw from ATCAS II contract documents as well as best practices for system management. Functional areas covered will include software development and release, operating system and firmware upgrades, user configurable settings management, prox card administration, business continuity, system interfaces, and access management.

**PwC Update for 2016**

MTC had a drafted responsibility matrix which had yet to be finalized as of the date of this report. PwC will review the roles, responsibilities and service levels defined in the matrix which is expected to be finalized in FY 2017 as part of the FY 2017 audit. Note that part a) of this finding which relates to developer access to production is recurring in FY 2016 and is discussed as part of current year recommendation B.4.

## 2. Application Access Management (Open)

### Observation

MTC has established controls for user access management activities for its financially significant applications and systems. However, during our audit procedures we noted that the following access-related controls were not operating effectively:

- a) Access to the ATCAS II application was not deprovisioned timely for one employee separated from BATA. Even though the access was not removed timely, the termination was identified and access disabled by IT based on the execution of the quarterly access review.
- b) Even though there is a process in place to periodically review the user access matrix (“UAM”) for the ATCAS II application, the frequency of the review is not clearly defined, and the last review was performed in FY14. While a comparison of the current, point in time UAM to the one reviewed in FY2014, indicated that the changes identified were appropriately approved, the periodic review was not performed consistently.

### Impact

Without consistent adherence to user access management activities, such as timely revoking separated user access and effectively performing periodic user access appropriateness reviews, there is an increased risk of unauthorized or inappropriate access to financially significant applications. Specifically for the UAM review, changes to the role access potentially affect all users assigned the role being modified and as a result pose an elevated risk of unauthorized access should changes not be appropriately approved. This, in turn, can lead to inappropriate transaction processing, erroneous transaction processing, inaccurate financial data, loss of financial data, or fraudulent activity.

### Recommendation

We recommend that Management implement a means to ensure access management controls are operating effectively and consistently on a continuous basis for safeguarding appropriate restriction of access to financially significant data and applications. In particular, we recommend the following:

- a) Access for separated employees should be removed in a timely manner for all application layers; definition of timeliness should be incorporated into formal policies to provide formal guidelines and requirements in this area, including timely notification of terminations to IT; and
- b) A periodic monitoring review over the UAM changes should be established to identify the changes to the access roles and ensure that all the role changes followed an established change management and approval process.

### Management Response from 2015

Management agrees with observation “a”.

For observation “b”, ATCAS II User Access Matrix (UAM) review will be conducted annually by a committee comprised of BATA IT Manager, BATA ATCAS II Project Manager, and BATA Finance Manager.



**MTC Update for 2016**

The UAM committee completed an annual review of ATCAS II roles and permission levels in June 2016. Current ATCAS II permission settings and changes to permission settings since the last UAM review in 2014 were reviewed. The UAM committee will convene again in early 2017 to complete another annual review.

**PwC Update for 2016**

We noted during our audit procedures that the ATCAS II annual roles and responsibilities review by the UAM Committee took place in June 2016 and there were no exceptions noted. Also, we noted that MTC's definition of timeliness was incorporated into formal policies to provide formal guidelines and requirements in relation to removing access. However, as noted in recommendation B.3 of the Current Year Recommendations, there was inappropriate access granted which was not identified by a review performed. Therefore, we conclude that in FY2016, this control was not operating effectively and accordingly this comment is included as part of current year recommendation B.3.

**3. Formalize Change Management Policy and Processes (Open)****Observation**

There has been a number of changes and upgrades to the systems at MTC and BATA in the recent few years. The organization also plans to move its offices to the new building in the next fiscal year. The move will lead to additional IT changes that need to be managed in tandem with other system changes.

Formalizing the change management policy and processes can lead to improving the maturity of controls within MTC and BATA.

Currently, MTC and BATA do not have an overarching change and configuration management policy covering all their financial reporting systems. Consequently, some practices are informal and not documented, such as assessing the risk and determining the extent of testing to be performed on a change.

In addition, program changes for each system are managed separately. A Change Advisory Board (CAB) or equivalent that oversees all changes is currently not present.

To illustrate:

- a. BATA conducts regular "Punch list" change management meetings only covering ATCAS changes. Similar meetings are not conducted for other BATA changes.
- b. Each change to MTC's financial reporting applications is separately managed. There is no readily available consolidated view of changes that are planned, requested or in-progress.

**Impact**

Formal policies provide a foundation or baseline for the control activities surrounding a process. For example, policies can provide guidance on the nature and extent of testing performed in a test or production environment depending on the assessed risk. Without

these policies, the guidelines for deciding on the operation of the control can be more fluid and may not represent management's intention.

In addition, having a centralized view of all changes made to financial reporting systems allows an organization to better schedule releases or changes. This also provides for a centralized committee to approve the changes and to have visibility of the dependencies and impact of the multiple changes that are occurring.

**Recommendation**

We recommend that the organization consider establishing a formal change management policy. This policy can include control requirements for initiating, testing, implementing and reviewing changes to the organization's financial reporting systems.

In addition, we recommend the organization consider setting up a CAB or equivalent to have a forum to discuss and approve all changes that are occurring.

**Management Response from 2015**

MTC is currently assessing its Technology Strategy from an enterprise perspective. As a part of this analysis, the agency will determine the appropriate level of formal change management to implement.

**PwC Update for 2016**

This finding is included as current year recommendation B.1.

