

Management Letter and State Reporting Requirements

The Honorable Mayor; Members of the City Commission
and City Manager
City of Miami, Florida

We have audited the financial statements of the governmental activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the City of Miami, Florida (the City) as of and for the year ended September 30, 2011, which collectively comprise the City's basic financial statements and have issued our report thereon dated May 18, 2012. Other auditors audited the financial statements of the discretely presented component units and pension trust funds as described in our report on the City's financial statements. Our report does not include the results of the other auditors testing of internal control over financial reporting or compliance and other matters that are reported on separately by those auditors.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*; Section 215.97, *Florida Statutes*; and Chapter 10.550, *Rules of the Auditor General*. We have issued our Report of Independent Certified Public Accountants and Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards* and our Report of Independent Certified Public Accountants on Compliance and Internal Control over Compliance That Could Have a Direct and Material Effect on each Major Federal Program and State Project in Accordance with OMB Circular A-133, Section 215.97, *Florida Statutes*, and Chapter 10.550, *Rules of the Auditor General* and on the Schedule of Expenditures of Federal Awards and State Financial Assistance. Disclosures in those reports and schedules, which are dated May 18, 2012 and June 19, 2012, respectively, should be considered in conjunction with this management letter.

Additionally, our audit was conducted in accordance with the provisions of Chapter 10.550, *Rules of the Auditor General*, which govern the conduct of local governmental entity audits performed in the State of Florida. The suggestions included in this letter, which resulted from our consideration of internal control, are submitted to assist in improving procedures and controls. In addition, this letter includes other communications required by the *Rules of the Auditor General*.

We have the following suggestions for improvement in accounting procedures and controls.

A. Current Year Recommendations

2011-01 Leases

Observation

The City does not have a process in place to evaluate the classification of leases as operating versus capital for financial reporting purposes. Performing a timely review of lease agreements would reduce the risk that leases are not misclassified and recorded incorrectly (i.e., record capital asset and related depreciation expense and record capital lease obligation for the present value of future minimum lease payments and amortize the interest portion of capital lease obligation to interest expense). Furthermore, management was unable to compile a list of leases by vendor and dollar amount and lease agreements were not readily available or accessible. The impact of not performing a timely review and assessment of leases in the future could have a significant impact on the financial statements and related disclosures.

Recommendation

We recommend that the City centralize the review, tracking and monitoring of lease agreements and perform a monthly review of new lease agreements. This will ensure the timely identification of and classification of leases. We also recommend management develop a checklist to facilitate to determination of the classification of all leases.

Management's Response

We agree and we obtained from the Department of Asset Management two lists of leases, one where the City is the lessor, the other where the City is the lessee. We are establishing procedures whereby:

1. The compendium (synopsis) of each new lease that the City is about to enter into is provided to the Finance Department to ensure proper classification, and recording.
2. A checklist will be developed to facilitate determination of the classification of all leases.
3. Complete updated lists are to be provided to the Finance Department by Asset Management at the end of every quarter.
4. Folders with lease compendium, classification, and receipt records are maintained in the Treasury Division in cases where the City is the lessor (revenues)
5. Folders with lease compendium, classification, and payment records are maintained in the Accounting Division in cases where the City is the lessee (expenditures).
6. Finance Division will be included on the distribution for all new leases

2011-02 Payroll Processing

Observation

The Oracle Human Resource Management System (HRMS) is pre-programmed to automatically approve each employee's hours worked in the event that the employee's supervisor does not approve the hours entered into the HRMS for the pay period in order to avoid delays in processing the payroll. This may result in employees being compensated for time not worked.

Recommendation

We recommend the City cease the practice of processing payroll in all instances where an appropriate supervisor has not approved the employees' time records in advance. If this is deemed not practical, then the City should establish a control procedure which requires the review of HRMS "exception reports" for each pay period in order to identify time and attendance records that were not approved at the department level. An after the fact review of the identified attendance records should be performed to ensure that employees were only compensated for time earned/worked.

Management's Response

We agree that timecards should be authorized by the supervisors prior to processing payroll. We must also pay employees timely for the time worked in accordance with the Fair Labor Standards. The City has implemented control procedures to ensure the Oracle Time & Labor timekeeping records are reviewed and approved by management prior to issuing payroll. The process was implemented July, 2011, hence; there have been less than one percent of electronic time cards approved automatically on the pre-programmed setting.

Prior to finalizing payroll, the CMIA OTL Time Card Status report is run periodically to monitor records that have not been approved by the departments remaining in an error or submitted status. The payroll supervisor or designee will queue the report on Friday afternoon preceding the payroll processing week and send it to the departments for review. This process is continued up to the following Tuesday morning to identify records in submitted and error status and monitor approvals. The payroll staff will continue to work very closely with the payroll liaisons to clear errors and confirm the department supervisor's approval prior to the pre-programmed approval deadline.

Once timekeeping has been approved, the interface process is completed and the payroll registers are reviewed by the payroll liaisons. Several exception reports are used by the payroll staff to validate the accuracy of the time and attendance records. The payroll staff will work closely with the payroll liaisons, researching all exceptions and record adjustments where necessary.

2011-03 Grant Reimbursements

Observation

We noted that the City does not request reimbursements for grant expenditures in a timely manner, soon after the incurrence and payment of qualified related expenditures. The delay may have an adverse effect on cash flows and may affect the collectability of the amounts due from the grantor agencies.

Recommendation

We recommend that the City establish a process to ensure that amounts expended related to grants under reimbursement-type agreements are timely submitted for reimbursement, all required forms are compiled and prepared in the format prescribed by the grantor, and reimbursement packages are reviewed and approved by supervisory personnel.

Management's Response

The City agrees with the findings and recommendations of the auditor. The grant monitoring is decentralized and relies on the departments to assign program managers to the grants under their supervision that are responsible for managing the program and filing the reimbursement requests. The City has been actively working with the program managers to submit grant reimbursements on a timely basis. The Finance Department contacts the departments' program managers each month to alert the departments to submit reimbursement requests. It should be noted that as a result of these ongoing efforts the amount of qualifying reimbursable grant expenditures that were not submitted has decreased from 35M in FY09, 22M in FY10 to 14M in FY11.

The City is continuing to implement policies and procedures to enhance the turnaround time of reimbursement requests. The City will create a grant reimbursement schedule that will include all grants throughout the city with the related timing for submitting reimbursement requests. Electronic notifications will be sent out to the program managers to remind them of the submission requirements and personnel will be assigned to programs to monitor the timing of the submission and reimbursement for grants.

2011-04 Information Systems General Controls

Policies and Procedures

We obtained the following IT policies and procedures; however, it was noted that these policies were still in draft form and not yet approved at the time of the audit:

- Oracle Development Standards
- Oracle System Administration

Procedures

- Oracle RMAN Backup and Recovery Procedures

Information technology policies and procedures serve as the groundwork to enforce the City's security objectives. Formal, controlled procedures over system administration and formal security policies can help heighten employee awareness and strengthen the control environment over IT processing.

Recommendation

The City should formalize policies and procedures to provide written documentation of management's expectations, consistency among personnel, and training documentation for new employees. These should include:

- Change Management
- User Administration and Network Security
- Data Ownership and Information Security

These procedures should also be updated regularly as necessary. Once the policies and procedures are finalized, they should be approved and distributed by senior management.

Management's Response

At the time of the audit, the approved policies and procedures were being revised as a result of a major Oracle application and platform upgrade. We have moved from Oracle Release 11i running in a Windows environment to Oracle Release 12 running on a Linux platform. The following policies and procedures were finalized and signed off as part of the Oracle R12 application upgrade:

- Oracle Development Standards
- Oracle System Administration
- Procedures
- Oracle RMAN Backup and Recovery Procedures

Policies and procedures addressing more general topics will be developed and distributed to and approved by senior management as time and resources become available. Such as:

- Change Management
- User Administration and Network Security
- Data Ownership and Information Security

Authorization of Configuration and Parameter Changes

Configuration and parameter changes for Oracle were noted as not being consistently approved using the City's change management process. This could result in unauthorized or unapproved changes applied to the production environment and changes applied to the production environment may not function properly or inadvertently break existing functionality.

Recommendation

Configuration and parameter changes should accordingly adhere to the policy ensuring changes are authorized, tested and documented prior to being applied in the production environment.

Management's Response

Configuration and parameter changes to Oracle modules are done through Super User responsibilities that are assigned to business process owners within the Finance Department. These individuals have been trained on setting up the specific Oracle modules they use to support the business. This is a best business practice that is supported by the architecture of the Oracle ERP.

Work Orders will be created every time there is a need for a change in configuration. To facilitate auditing of configuration changes, Oracle provides standard reports that show current setups. These reports would be generated every quarter to validate setup modifications and ensure all changes are properly documented.

Monitoring of Changes

The change process, e.g., steering committee, management review of changes to production) is not monitored on a regular basis.

This could result in unauthorized or unapproved changes promoted to the production environment. Also, changes applied to the production environment may not function properly or inadvertently break existing functionality.

Recommendation

Management should consider implementing a formal change monitoring process to reconcile changes made to the production environment. Changes should be reviewed on a routine basis by a member (or members) of IT Management who does not have development responsibilities or access to implement changes into production. Evidence of Management's review should be retained.

Management's Response

All software enhancements, fixes and patches are tracked via work orders. A report of work orders migrated to production will be generated periodically and reviewed with IT Management personnel outside of development.

Password Policy

Password aging, history, complexity or failed attempts have not been configured for Oracle Financials. Password aging was noted as enabled at the individual account level for a user inspected. It was noted that draft Oracle System Administration Procedures had been developed, but had not yet been approved at the time of the audit. Insufficient security controls around passwords may lead to security breach that can pose a potential threat to the availability and integrity of systems, applications and data.

Recommendation

A consistent, City-wide password policy should be adopted to mitigate risks associated with a breach. Based on standard practices, some of the recommended settings are as follows:

- Passwords set to expire every 45 – 90 days;
- Passwords be a minimum of 6 characters;
- Password history enabled to prevent employees from recycling passwords; and
- Password complexity should be enabled where/when possible.

Management's Response

A password policy recommendation will be presented to the IT Steering Committee for approval. Oracle provides ample functionality to facilitate the implementation of more stringent password policies.

Periodic User Access Reviews

There is not currently a process in place to periodically review user access to Active Directory and the Oracle application. The lack of a periodic review that responds to changes in employment status can result in excess access or a breakdown in segregation of duties.

Recommendation

A formal periodic access review process should be established to ensure access to Oracle is given to only those users who require it based on their job responsibilities, as well as, verify the continued employment status of employees. Users with access that is inappropriate, unnecessary, or identified as belonging to terminated employees should be communicated to the security administrators.

Management's Response

A process will be put in place for Department Directors to validate user access periodically. Additionally, an Oracle Alert will be implemented to inform the Network Administrator and other stakeholders when employee terminations are completed in the Oracle HR Module.

Logical Access Monitoring

AuditTrail has not been enabled; AuditTrail tracks which rows in a database table(s) were updated, at what time, and which user was logged in using the form(s). However, it was noted that Sign-on Audit Level was set to FORM. Hence the system is configured to log the form users choose and how much time users spend using each form. The lack of a formal user access monitoring process increases the risk of unauthorized user activity and tampering of data within the financially significant applications.

Recommendation

Although not critical to the City at this time, Oracle does provide the AuditTrail feature. The logging of critical events represents a detective control that can assist in the identification of unauthorized or incorrect changes made to data. Events that may be considered critical to log on an exception basis may include (but not limited to):

- User additions, deletions and modifications;
- Responsibility additions, deletions and modifications.

If/when AuditTrail is used, management should periodically review the AuditTrail data (e.g., quarterly) to detect unauthorized or erroneous changes made.

Management's Response

The generation of Audit logs is costly in terms of performance and space. As a result, the implementation of Audit logs for specific transactions will be reviewed by the ITD Steering Committee. A set of transactions to be audited will be identified with input from the ERP Information Technology Team and the Super Users. A process to monitor the identified transactions will be presented to the IT Steering Committee.

Termination Timeliness

The System Administrator runs a report of users active in Oracle to compare to an employee listing from Human Resources on a weekly basis; however, a formal process has not been defined to notify the helpdesk or system administrators of employee termination in a timely manner. An individual could gain access to financially significant applications and/or other applicable logical access layers using the terminated employee's user credentials. This could also result in unauthorized access to the production servers and lack of accountability for actions taken under the use of the user accounts.

Recommendation

An individual could gain access to financially significant applications and/or other applicable logical access layers using the terminated employee's user credentials.

Management's Response

The City is in the process of creating an Oracle Alert that will be distributed to the Help Desk and other stakeholders when an employee is terminated in the Oracle System. This is the same alert mentioned in item "Periodic User Access Reviews" above. The alert is in the testing stage with a target production date of June 30th.

Data Center Access Reviews

Access to the data center is not regularly reviewed for appropriateness. Individuals with access to the data center, who do not require that access, increases the risk of damage to equipment and potentially unauthorized system access.

Recommendation

Given the large number of individuals that have access to the 4th floor of the building where Data Center is located; management should determine an appropriate frequency to periodically review data center access. Data center access should be limited to key IT personnel responsible for operations and support; generic user access avoided whenever possible.

Management's Response

The physical security of the data center will be monitored to ensure the access off the floor into the data center is secure. Additionally, security access will be limited to data center personnel via security access cards.

Timeliness of Incident Resolution

IT operations problems or incidents such as system errors, access issues etc. are not resolved in a timely manner. Untimely remediation of incidents makes the production environment vulnerable to repeated operationally faults and issues.

Recommendation

A process should be in place to resolve the incidents in a timely manner.

Management’s Response

Outstanding work orders are reviewed on an ongoing basis and prioritized with the user who reports the incident and the Super User. Issue resolution takes into consideration the business constrains and priorities at that particular time.

B. Status of Prior Year Recommendations

The *Rules of the Auditor General* (Section 10.554(1)(i)1) require that we address in the management letter, if not already addressed in the auditor’s reports on compliance and internal controls or schedule of findings and questioned costs, whether or not recommendations made in the preceding annual financial audit report have been followed.

Finding #	Finding Title	Status
2010-01	Bank reconciliations	Corrected
2010-02	Recording of accruals and accounts payable	Not corrected – see current year material weakness disclosed as finding 2011-01 in the Schedule of Findings and Questioned Costs
2010-03	Payroll processing	Not corrected – comment repeated above.
2010-04	Filing for grant reimbursements	Not corrected – comment repeated above.
2010-05	Capital Asset Management	Not corrected – see current year material weakness disclosed as finding 2011-02 in the in Schedule of Findings and Questioned Costs

C. Other required communications

Section 10.554(1)(i)1., *Rules of the Auditor General*, requires that we determine whether or not corrective actions have been taken to address findings and recommendations made in the preceding annual financial audit report. Please refer to Status of prior year recommendations section above.

Section 10.554(1)(i)2., *Rules of the Auditor General*, requires that our audit include a review of the provisions of Section 218.415, Florida Statutes, regarding the investment of public funds. During the course of our audit, nothing came to our attention that would cause us to believe that the City had not complied with Section 218.415, *Florida Statutes*, regarding the investment of public funds.

Section 10.554(1)(i)4., *Rules of the Auditor General*, requires that we address violations of provisions of contracts and grant agreements or abuse that have an effect on the financial statements that is less than material but more than inconsequential. In connection with our audit, we were not made aware of instances of noncompliance with the provisions of contracts or grant agreements or abuse meeting such criteria other than as disclosed in this letter.

Section 10.554(1)(i)5., *Rules of the Auditor General*, provides that the auditor may, based on professional judgment, report the following matters that are inconsequential to the determination of financial statement amounts, considering both quantitative and qualitative factors: (1) violations of laws, regulations, contracts or grant agreements, or abuse that have occurred, or are likely to have occurred, and (2) control deficiencies that are not significant deficiencies, including, but not limited to: (a) improper or inadequate accounting procedures (e.g., the omission of required disclosures from the annual financial statements); (b) failures to properly record financial transactions; and (c) inaccuracies, shortages, defalcations, and instances of fraud discovered by, or that come to the attention of, the auditor. In connection with our audit, we were not made aware of such instances of noncompliance, other than as disclosed in this letter.

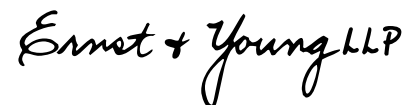
Section 10.554(1)(i)6., *Rules of the Auditor General*, requires that the name or official title and legal authority for the primary government and each component unit of the reporting entity be disclosed in this management letter, unless disclosed in the notes to the financial statements. The official title and legal authority for the primary government and each component unit is disclosed in Note 1 of the financial statements for the year ending September 30, 2011.

Section 10.554(1)(i)7.a., *Rules of the Auditor General*, requires a statement be included as to whether or not the local governmental entity has met one or more of the conditions described in Section 218.503(1), *Florida Statutes*, and identification of the specific condition(s) met. During the course of our audit, nothing came to our attention that would cause us to believe that the City was in a state of financial emergency as a consequence of conditions described in Section 218.503(1), *Florida Statutes*.

In connection with our audit, we applied financial condition assessment procedures pursuant to Sections 10.554(1)(i)7.c. and 10.556(7), *Rules of the Auditor General*. It is management's responsibility to monitor the City's financial condition, and our financial condition assessment was based in part on representations made by management and the review of financial information provided by same. We noted several indicators of deteriorating financial condition such as low general fund and total governmental fund assigned and unassigned fund balances, expenditures in excess of appropriations which were appropriately disclosed in the City's Comprehensive Annual Financial Report, deficit fund balances in certain governmental funds, a deficit unrestricted net asset balance for governmental activities of over \$300 million. The City is also not in compliance with its own financial integrity ordinance which requires the City to maintain specified levels of reserves.

Section 10.554(1)(i)7.b., *Rules of the Auditor General*, requires that we determine whether the annual financial report for the City for the fiscal year ended September 30, 2011, filed with the Florida Department of Financial Services pursuant to Section 218.32(1)(a), *Florida Statutes*, is in agreement with the annual financial audit report for the fiscal year ended September 30, 2011. In connection with our audit, we determined that these two reports were in material agreement.

This report is intended solely for the information and use of the City of Miami, state and federal agencies, the Florida Auditor General, management, and others within the City and is not intended to be, and should not be, used by anyone other than these specified parties.

A handwritten signature in black ink that reads 'Ernst & Young LLP'.

May 18, 2012