Metro

Financial Statement Audit Management Recommendations

June 2002

A Report by the Office of the Auditor

METRO

PEOPLE PLACES
OPEN SPACES

Alexis Dow, CPA
Metro Auditor

REGIONAL SERVICES

600 NORTHEAST GRAND AVENUE | PORTLAND, OREGON 97232 2736
TEL 503 797 1891 | FAX 503 797 1831

METRO

Office of the Auditor

June 24, 2002

To the Metro Council and Executive Officer:

As part of their audit of Metro's financial statements, KPMG LLP studied Metro's internal control in order to determine appropriate auditing procedures and to provide assurance on Metro's internal controls. They noted no matters involving Metro's internal control and its operation that they consider to be a material weakness. They did note other matters related to Metro's internal control and certain other accounting, administrative or operating matters. The accompanying report describes their observations and recommendations.

KPMG LLP recommends changes in the following areas of internal control:

Information Systems

- Establish stronger password controls for PeopleSoft when Metro upgrades to version 8.
- Conduct a network security assessment and vulnerability analysis of network and remote access connections.
- Segregate system users in development, test and production environments for changes made to application and interface programs.
- Store system backup tapes at a secure offsite location on a more frequent basis, i.e. daily.
- Store on-site backup tapes in a fireproof vault or cabinet.
- Test backup tapes periodically to ensure data is recoverable and the media has not deteriorated.
- Launch a more robust IT Disaster Recovery and Business Continuity initiative to mitigate risks.
- Review and monitor user access rights on PeopleSoft regularly.

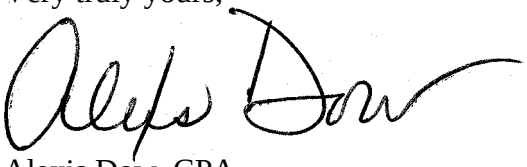
Accounting and Administrative

- Clarify responsibilities of Metro and the Zoo Foundation in regards to federal grants.
- Perform an inventory of fixed assets bi-annually and tag assets with identification numbers.
- Establish procedures to reconcile fixed asset detail to the accounting system at least quarterly.

This report presents management's response following each recommendation.

We appreciate the cooperation and assistance provided to KPMG LLP by staff in the Administrative Services Division.

Very truly yours,



Alexis Dow, CPA

KPMG

Suite 2000
1211 South West Fifth Avenue
Portland, OR 97204

Telephone 503 221 6500
Fax 503 796 7650

January 18, 2002

To the Council, Executive Officer and Auditor
Metro
Portland, Oregon

Ladies and Gentlemen:

We have audited the financial statements of Metro for the year ended June 30, 2001, and have issued our report thereon dated November 7, 2001. In planning and performing our audit of the general purpose financial statements, we considered Metro's internal control solely to determine our auditing procedures for the purpose of expressing our opinion on the general purpose financial statements. We also have examined management's assertion regarding the effectiveness of Metro's internal control over financial reporting as of June 30, 2001, and have issued our report thereon dated November 7, 2001. We have not considered internal control since November 7, 2001.

Our procedures were designed primarily to enable us to form an opinion on the general purpose financial statements and on management's assertion regarding the effectiveness of internal control over financial reporting, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We have attempted, however, to use our knowledge of the company's organization gained during our work to make comments and suggestions that we hope will be useful to you.

During our audits, 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 as follows:

METRO SHOULD CLARIFY THE RESPONSIBILITIES OF METRO, THE ZOO AND THE ZOO FOUNDATION IN REGARDS TO OBTAINING AND MANAGING FEDERAL GRANT

Observation

During our audit, an internal control issue came to our attention with respect to the receipt and management of Federal grants obtained by the Oregon Zoo. When Metro's accounting staff was completing the Schedule of Expenditures of Federal Awards, they had difficulty in determining final Federal revenue and expenditure information for the Oregon Zoo. The expenditure information was difficult to track because some federal grant funds awarded to Metro on behalf of the Zoo for education and special events were deposited in Zoo Foundation accounts.

The Oregon Zoo Foundation (the Foundation) is a separate legal entity and functions as the primary fundraiser for the Zoo. The Foundation has also managed the receipt of certain Federal funds related to the Zoo. In addition, the Foundation is actively involved in obtaining federal grants under the Metro (Oregon Zoo) / BLM grant agreement. Metro has a contract with Bureau of Land Management (BLM), which focuses on education and special events, such as the Annual Wildflower Exhibit at the Zoo. The grant agreement between Metro and BLM is an open contract and new work orders open under the overall grant agreement on a yearly basis.

During the year, the Foundation worked with BLM directly and had funds (on a reimbursement basis) wired directly to the Foundation bank accounts, rather than being reimbursed through Metro. Based on review of the grant agreement, the primary grantee is Metro, and Metro should be acting as the recipient of the grant, while the Zoo Foundation should be treated as the sub-recipient. As the grant recipient, Metro has an oversight responsibility to manage and report on the expenditure of the Federal award.

Recommendation

We recommend that any contracts to obtain Federal grants be entered into by the entity in charge of expending the grant and performing the majority of the work under the grant. Secondly, all reimbursement requested by the Zoo or the Zoo Foundation under Federal grants arrangements should be received directly by Metro in order to facilitate grant management and reporting activities. Lastly, we believe that approval for grant reimbursement should reside with Metro personnel familiar with Federal grant requirements.

Metro Response

Metro agrees. Metro should have received the grant and distributed it under contract to the Zoo Foundation as a sub-grantee. This matter was fully briefed, discussed, and resolved at the February 7, 2002 public meeting of the Oregon Zoo Foundation Board of Trustees attended by Metro Executive Officer, two Metro Councilors, and the Zoo's Deputy Director. The parties noted that the BLM grant was obtained through the initiative and hard work of the Foundation and that all expenditures were made properly in accordance with grant requirements. At the same time, the parties agreed that the funds should have been received, deposited, and distributed by Metro as the actual grantee. This procedure will be followed in the future.

PERFORMANCE OF BI-ANNUAL INVENTORY OF ALL FIXED ASSETS

Observation

Metro currently does not conduct a periodic inventory of its fixed assets, nor does it perform a reconciliation of its fixed asset detail records to the PeopleSoft system.

Recommendation

We recommend that Metro perform a complete physical inventory of all fixed assets bi-annually and tag all assets with identification numbers. We also recommend the establishment of formal policies and procedures to ensure that a reconciliation of fixed asset detail to the PeopleSoft financial reporting system is prepared at least quarterly, and appropriate supervisory review takes place on a timely basis. We suggest that Metro establish fixed asset procedures to be performed each month and at year-end, and assign individual responsibility for each task. The performance of bi-annual fixed asset inventory and monthly reconciliation of fixed asset detail to the PeopleSoft system will assure that general ledger balances are reasonable on a periodic basis.

Metro Response

Management agrees with this recommendation. In FY 2002-03 Metro will develop fixed asset procedures and assign responsibility for each task. Depending on the magnitude of the required effort, the actual inventory may not be completed until the following fiscal year. The goal will be to update the inventory on a regular schedule.

CHANGES IN THE GOVERNMENT REPORTING MODEL

Observation

After years of study and consideration of the needs of users of government financial statements, the Governmental Accounting Standards Board (GASB) issued its revolutionary new reporting model in June 1999. The new model dramatically changes the presentation of governments' external financial statements. In the GASB's view, the objective of the new model is to enhance the clarity and usefulness of government financial statements to the citizenry, oversight bodies, investors and creditors. It will substantially affect Metro's financial data accumulation and financial statement presentation processes. Some of the key aspects of the change follow:

- *Government-Wide Reporting* – Traditionally, governments have reported their activities by fund type. The new reporting model also requires the preparation of government-wide financial statements that reflect all governmental activities. These financial statements are to be reported on the full accrual, economic resources measurement focus, which differs from the fund-perspective financial statements. Certain funds will therefore be presented in the financial statements using two different bases of accounting. Additionally, general government fixed assets, *including infrastructure*, and long-term liabilities of the government will need to be reported with all other governmental assets and liabilities.

- *Statement of Activities* – Governments will now be required to use a "net program cost" format for the government-wide statements instead of a traditional operating statement. This new format groups revenues and expenses by functional categories (such as public safety, public works, etc.). The purpose of the new statement is to inform readers about the cost of specific functions and the extent to which they are financed with program revenues or general revenues of the government. Governments will have the option of reporting both direct and indirect program costs. Depreciation expense will now generally be reflected as a cost in the statement of activities.

- *Infrastructure Reporting* – Historically, Metro has not been required to report infrastructure assets in its financial statements. Infrastructure assets are long-lived capital assets that are generally stationary in nature, such as roads, bridges, drainage systems and dams. Under the new standard, Metro must report infrastructure assets, if any, acquired within the last twenty-five years at historical cost. Due to the nature of Metro's operations, this requirement will have limited impact to Metro. Many governments, however, do not have financial records to substantiate the historical cost of infrastructure.

- *Fund Level Reporting* – Fund level financial statements will still be required and will provide information about Metro's fund types, including fiduciary funds. General capital assets and general long-term liabilities will only be reported at the government-wide level. Fund level reporting will continue to focus on fiscal accountability and reflect the flows and balances of current financial resources. A reconciliation between the fund and the government-wide statements will be required on the face of the fund statements. Finally, proprietary fund cash flows statements must be presented using the direct method, which is Metro's current methodology.

- *Presentation of Budgetary Information* – The standard requires budgetary statements for the general fund and certain other governmental funds as required supplementary information. The original adopted budget of Metro as well as the final revised budget must be presented. Actual results on a budgetary basis will need to be reconciled to the GAAP (generally accepted accounting principles) basis on the face of the statements.

- *Management's Discussion and Analysis (MD&A)* – A comprehensive MD&A will now be included as required supplementary information. MD&A will introduce the financial statements by presenting an analysis of the government's financial performance for the year and its financial position at year-end. MD&A will be *in addition* to the transmittal letter currently required for Government Finance Officers Association (GFOA) award candidates, such as Metro, but we expect that the GFOA will make changes in their requirements so as to avoid any duplication between the two documents.

The effective date of the new pronouncement will require implementation by Metro for its year ending June 30, 2002. This date is also effective for Metro's component unit. The magnitude of these changes and the time required preparing for implementation should not be underestimated.

Recommendation

We recommend that Metro continue to look at its systems and processes to ensure that the required information will be available to ensure timely implementation. Further, we recommend that Metro consider the cost of required changes to its systems and processes to ensure availability of necessary funds in its upcoming budget.

Metro Response

In accordance with its GASB 34 plan, Management will implement the critical GASB 34 reporting requirements for the FY 2001-02 Comprehensive Annual Financial Report that will be issued at the end of November 2002.

PEOPLESOFT PASSWORD CONTROLS SHOULD BE STRENGTHENED

Observation

The current version of the PeopleSoft application (Finance and HR) that is implemented at Metro does not support strong password controls such as password length, password expiration and password history. Strong passwords and password parameters are one method of restricting access to information that needs to be secured. In the absence of strong password controls, there is an increased risk of unauthorized access to Metro's resources, misuse of Metro's resources and fraudulent activities.

Recommendation

PeopleSoft's version 8 supports stronger password controls. We recommend that when Metro upgrades to version 8 of the PeopleSoft application, that it take advantage of this new functionality, which will strengthen internal controls, such as:

1. Password length (set to 6-8 characters)
2. Setting a Password expiration period (e.g. 90 days)
3. History of passwords (e.g. set to 3)
4. Setting up of audit logs to record user activity such as user login and logout time.

Metro Response

Management agrees. PeopleSoft password controls will be upgraded to the recommended security level when version 8 is installed.

METRO SHOULD PERFORM A NETWORK SECURITY ASSESSMENT AND VULNERABILITY ANALYSIS

Observation

There are several external parties that connect to the PeopleSoft system through Metro's network. These external parties are the Zoo, MERC and the Solid Waste Management sites. There are other users such as the Department of Transportation and Clackamas county, as well the network security administrator, UNIX and database administrator, that have remote access to the Metro's internal network using the remote connections. It is our understanding that remote users do not go through Metro's firewall.

Although some network monitoring and security procedures are in place, it is our understanding that a formal security network assessment or vulnerability analysis has not been performed.

If a formal network security assessment or vulnerability analysis has not been performed of Metro's network in recent time, including remote connectivity, there may be an increased risk of security vulnerabilities that may increase the risk of unauthorized access to Metro's resources, misuse of Metro's resources and fraudulent activities.

Recommendation

Metro should consider conducting a comprehensive network assessment and vulnerability analysis of its entire network and remote access connections.

Metro Response

Management agrees. The IT Department will propose funding for a security audit in FY 2003-04.

Management treats the T-1 connections to the Zoo, MERC, and Solid Waste as integral parts of the Metro system. Access is limited to Metro employees with log in and password security. Any user on the network must also be able to provide a user id and password to gain access to PeopleSoft.

Other remote access (through dialup connections) is done on a very limited basis and only with prior approval. Metro is examining the use of a virtual private network to replace those dialup connections.

METRO SHOULD STRENGTHEN ITS MANAGEMENT REVIEW CONTROLS OVER CHANGES MADE TO APPLICATIONS AND INTERFACES

Observation

Changes made to the PeopleSoft application and PeopleSoft interface programs are not currently subject to formal management or supervisory review. In some cases, the individual making the changes to the application or program has access to development, test and production environments. This is a segregation of duties conflict.

If the same person has access to all 3 environments, and there is no review by management or a supervisor of the change to the application or program, there is a risk that an unauthorized change could be initiated in the development environment and propagated through test to production. A change could be designed to disrupt the production system or used to perpetrate fraud.

Recommendation

It is best practice to segregate users in development, test and production environments. This is a strong internal control, which can prevent a user from propagating an unauthorized change into production. If it is not feasible to segregate users due to resource constraints, then we recommend as a compensating control, an appropriately qualified manager or supervisor review that changes to applications or programs.

Metro Response

The small size of the IT support staff in the Enterprise Applications group prevents segregating the systems analysts by development, test and production environments. To compensate, Metro uses a peer review process that requires a second analyst checks the work of the first. In addition, functional leads in Administrative Services and Human Resources review the changes to ensure accurate and correct operations. Physical logs are kept documenting the review.

METRO SHOULD STRENGTHEN ITS BACKUP AND RECOVERY PROCEDURES

Observation

We noted the following areas for improvement in controls during our review of IT disaster recovery procedures:

- Currently, only one backup to tape is created of the PeopleSoft application. The tapes are sent offsite once a week.
- The backup tapes that are stored on-site are not currently stored in a fireproof cabinet or vault.
- Backups tapes are not tested on a regular basis to check if the data on these tapes is recoverable in the event of an IT disaster,
- Metro does not currently have a formal documented IT disaster recovery plan or Business Continuity Plan.

Information availability is essential in the Information Age. Natural disasters, malicious intent, and catastrophic accidents can disrupt information availability and negatively impact key business processes and operations. Competitive pressures and market demands, together with an increased dependence on technology for core business processes, are redefining the need for effective risk-based business continuity planning.

Recommendation

- Due to the fact that only one copy of the backup tape for PeopleSoft is created, and that these tapes are currently kept on site for a period of one week before being stored offsite, if these tapes were damaged, there is a potential that Metro could lose up to a weeks worth of data and transactions. Therefore we recommend that Metro store the backup tapes at a secure offsite location on a more frequent basis i.e. daily.
- On-site backup tapes should be stored in a secure location, preferably in a fireproof vault or cabinet
- Backup tapes should be tested periodically to ensure that the data is recoverable whenever needed and that the media has not deteriorated. This should be part of a formal test of an IT Disaster Recovery plan.
- Metro should launch a more robust IT Disaster Recovery and Business Continuity initiative to mitigate its risks. These plans should be formally documented and tested on a yearly basis.

Metro Response

Because of the high cost for daily, secure courier services for tape movement, Management has elected to use a weekly courier schedule to move backup tapes to offsite storage. Daily backup tapes are stored in a fireproof safe awaiting the weekly courier run.

Metro will prepare a business continuity plan in FY 2002-03.

METRO SHOULD REVIEW AND MONITOR THE USER ACCESS RIGHTS ON PEOPLESOFT REGULARLY

Observation

We noted the following areas for improvement in controls during our review of the user access rights in PeopleSoft:

1. Users are being assigned access on a temporary basis. This can occur for example if someone leaves and another person is temporarily assigned this access to fill in for this position. However, when this position becomes permanently filled, the user who was temporarily assigned this access may still retain this access if the security administrator is not informed of this event.

2. Users are being granted access rights for functions not performed by them. This can occur when for example a user transfers to a different function or role. This user will get additional access to perform his/her new role, but may also retain his/her old access rights if the user's supervisor does not inform the security administrator of this change.

3. An employee who left Metro still had user ID enabled in the PeopleSoft system. It is our understanding that this user's network logon ID had been disabled which would prevent someone from accessing PeopleSoft through this network ID.

The absence of periodic review can lead to weaknesses in internal controls. Metro could be at risk of having users with access rights which might not be commensurate with their job role and duties. This could lead to instances of segregation of duties conflicts, i.e. same rights being granted to different personnel who are performing different duties. There is also a risk that user IDs may remain on the system for users who have left the Organization.

Recommendation

In order to ensure that the IT has controls over the user access rights granted on the system. The following procedures should be followed:

1. If users are assigned access on a temporary basis, the user' supervisor should request this access formally and a form should be filled out, with the period requested (start date – end date). In this way, the security administrator would be able to remove this temporary access when the period has expired.

2. If a user's role is changed, this change should be formally requested by the user's supervisor and recorded. The reason for this change should also be recorded so that the security administrator can determine if the user needs his/her old access to be removed.

3. We recommend that a list of terminated employees/contractors be forwarded to the security administrator on a weekly basis for review. This information should come directly from the HR department and the user's supervisor. This process should be formalized and documented.

Additionally we recommend that users and their access rights on the PeopleSoft system should be reviewed on a quarterly basis. A user list should be forwarded by IT to the appropriate department managers for their review. User's who are no longer at Metro should be removed from the PeopleSoft system and user's with too much access should be further restricted.

Metro Response

The Security Administrator will document all changes through either paper forms or emails giving supervisor authorization.

KPMG's observation #3 is correct. When the account was disabled (which, as KPMG notes, effectively prevents anyone from using that account), ASD and HR management indicated to the Security Administrator they did not know if the employee would return to work. The account was held in suspension pending an outcome.

IT will require a yearly renewal of security access of all user access rights to PeopleSoft. Each supervisor and functional lead must give approval each year for each person's security. If that process indicates security changes made in-between annual reviews are not occurring appropriately, we will increase the review to a semi-annual and perhaps quarterly basis.

* * * * * * * * * * * *

We would be pleased to discuss these comments and recommendations with you at any time.

This report is intended solely for the information and use of the audit committee, management, and others within the organization and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP