Metro

Financial Statement Audit Management Recommendations

March 2001

A Report by the Office of the Auditor

METRO

2001-10716-AUD

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

March 23, 2001

To the Metro Council and Executive Officer:

As part of their audit of Metro's financial statements, Deloitte & Touche LLP studied Metro's internal control in order to determine appropriate auditing procedures and not 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.

Deloitte and Touche LLP recommends changes in the following areas of internal control:

<u>Information Systems</u>

- Complete a thorough software security assessment and implement a risk-management solution.
- Develop a strategic plan linking information systems to Metro's operating plan.
- Develop a business-wide continuity plan for computing operations including disaster recovery.
- Use the existing Information Systems Steering Committee for routine communications between IMS and DRC to further ensure use of common standards.
- Review administrative access to information systems and restrict unnecessary access to strengthen system security.

<u>Accounting and Administrative</u>

- Increase Metro oversight of MERC during periods with high turnover of higher-level management and accounting staff. MERC should attempt to increase retention among this group of employees.
- Reconcile general ledger account balances to Zoo Foundation contributions at least quarterly.
- Obtain an understanding of the recently issued GASB Statement No. 34 and create an action plan for implementation.
- Perform a complete physical inventory of all fixed assets biannually.
- Establish an allowance for potentially uncollectible accounts based on an aging analysis.
- Adjust for cash account reconciling items in a timely manner, including all MERC accounts.
- Identify one Metro employee to approve all grants and be the contact person on grant applications.

This report presents management's response following each recommendation.

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

Very truly yours,

Alexis Dow

Alexis Dow, CPA
Metro Auditor

Deloitte & Touche LLP
Suite 3900
111 S.W. Fifth Avenue
Portland, Oregon 97204-3642

Tel: (503) 222-1341
Fax: (503) 224-2172
www.us.deloitte.com

Deloitte
& Touche

November 22, 2000

The Metro Council, Executive Officer,
and Metro Auditor
Metro
Portland, Oregon

Dear Sirs or Madams:

In planning and performing our audit of the general purpose financial statements of Metro for the year ended June 30, 2000 (on which we have issued our report dated November 22, 2000), we considered its internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on Metro's internal control. Such consideration would not necessarily disclose all matters in Metro's internal control that might be material weaknesses under standards established by the American Institute of Certified Public Accountants. A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We noted no matters involving Metro's internal control and its operations that we consider to be material weaknesses as defined above.

We did note other matters related to Metro's internal control and certain other accounting, administrative or operating matters. Our comments are presented in Exhibit I.

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

We will be pleased to discuss these comments with you and, if desired, to assist you in implementing any of the suggestions.

Yours truly,

Deloitte + Touche LLP

Deloitte
Touche
Tohmatsu

EXHIBIT I

INFORMATION SYSTEMS

NEW COMMENTS

Novell Security and Performance Monitoring

Observation: Security monitoring tools are not implemented on the Novell servers. Metro's Information Technology (IT) staff utilized a demonstration version of BindView, a security and network performance review tool, which expired in June 2000. In addition, third party network performance monitoring tools are not implemented on the Novell servers.

Novell NetWare does not include security monitoring or network reporting tools. As a result, system administrators may lack the necessary tools for comprehensive network security monitoring as well as detailed security recording and exception reporting.

The lack of performance monitoring tools impairs user availability, reliability and network efficiency. Additionally, without preventive network monitoring, the system may not perform as required, a situation may only be discovered at later stages or peak periods when performance is critical.

Recommendation: Metro should complete an end-to-end software security assessment and implement a risk-management solution on the Novell servers. Such a process should examine security and performance.

> ***Management's Response:*** Limited IT funding prevents a broad approach to security and performance monitoring; however, in addition to already improved current practices, we are re-engineering our network-operating environment.
>
> A long term issue for the agency is the duplicate network operating systems: Novell and Unix (GIS). The Information Technology Steering Committee is forwarding a recommendation to the Chief Operating Officer to migrate the Novell users into a Unix-based environment. Once begun, we expect to complete that project in 12 to 18 months.
>
> IT staff will do an end-to-end review of administrative rights in preparation for that migration. Use of Unix-based group membership, concurrent or virtual, will be used to provide sound administrative controls over user access to specific files. Both Security and Network staff will be involved in the design and implementation. The outcome will be a systematic and documented method of determining appropriate security access for any individual based on their organizational needs.

Network performance management tools do improve availability, reliability and network efficiency. Though limited funding prevents IT from investing in broad solutions, we do employ a variety of methods to track network performance. Two examples are:

- Intermapper is a network-monitoring tool used for tracking uptime, utilization and response time. We will be upgrading that tool soon. Additionally, we use Web-based quota tracking tools.

- File service and drive loads are monitored using script-based command sets for checking drive space on Novell servers.

Both minimizing the use of staff time and avoidance of network traffic issues are accomplished in these off-the-shelf and in-house solutions.

We run a CheckPoint firewall which will continue to provide security to our reconfigured network.

RECURRING COMMENTS

Information Systems Strategies, Policies and Procedures

Observation: Metro has a formal information systems strategic plan that is not linked to the business strategic planning process due to the fact that Metro does not maintain a business strategic plan. Additionally, the information security policies and procedures handbook has not been updated since 1997.

Implications: A lack of effective strategies and long-range information system plans linked to a business strategic plan can result in (1) information systems operating independently of the business, (2) information systems not being supportive of the business, (3) top management lacking confidence in the ability of information systems to support and add value to the business, and (4) information systems not operating as effectively and efficiently as possible. Without updated policies and procedures, an organization is susceptible to security breaches and unauthorized access.

Recommendations: We recommend Metro develop an organization-wide business strategic plan which links its information systems strategic plan objectives and goals to the business strategic plan.

The effectiveness of information systems in an organization can be defined as the extent to which it supports and services the information systems needs of the organization's operations and accounting functions. These needs are defined within the information systems long-range and short term-range plans. As such, the long- and short-term plans need to be dynamic; accordingly, mechanisms for review and update of the plans should be in place. Monitoring of all services rendered and implementing changes as required by the plans are key control elements to ensure the effectiveness and efficiency of the information systems organization.

All affected parties should ordinarily participate in the selection of service criteria that will be monitored, and the frequency and level of detail for reporting on the actual services rendered.

We recommend Metro review the current information security policies and procedures as documented in the Computer Users' Handbook, and update the information with current policies and procedures to include:

Policies

- Responsibility for protecting information
- Importance of information to the business
- Management support for controls
- Compliance and accountability

Control Procedures

- Acquisition and development of software
- Protection of information
- Environmental controls
- Network security
- Physical security
- Incident response

2000 Status Update: In Process. A committee of the Information Technology Steering Committee ("ITSC") is working on an IT Security Policy, is nearing completion, and will present a final draft of the security policy to the ITSC for review and implementation.

> ***Management's Response:*** Both Information Technology and executive corporate management recognize the critical need for business-wide planning in Metro computing. Using departments' work plans and business goals, Information Technology does long range planning to the extent possible.
>
> A current example is the proposed 2040 Plan Re-engagement. To successfully accomplish the goals of that project will require a stronger Metro web presence than is currently the case. The Information Technology department and Creative Services unit jointly developed a budget proposal to have the appropriate technology and resources in place. Another example is sizing network attached storage acquisition in the Data Resource Center purchase to meet future file storage needs of the entire agency.
>
> Short of a long range information technology plan based on an agency-wide strategic business plan, tying long range technology direction to department plans as defined by the department's management succeeds in accomplishing a dynamic and controlled synchronicity between the two.

The Computer User's Handbook is in the first stages of revision, and will include updated elements of both existing and new topics appropriate to the Handbook (as implemented through Executive Order 76). When completed, IT will post it on the agency's Intranet for easy access by employees, and to allow for simpler and timely updates.

The security policy mentioned in the 2000 Status Update is complete and was adopted agency-wide in November 2000 via Executive Order 76. The original intent of the security policy was expanded to become a "Network Access Policy". It covers physical access to computers, network access, passwords and user identification, virus protection, software, email and Internet use, and remote access. The Executive Order stresses the issues of information protection, employee responsibility and accountability for use of Metro resources.

Business-Wide Planning for Computing Operations

Observation: Metro does not maintain an IT recovery plan or a detailed business-wide plan for recovering critical business functions in the event of an entity-wide disaster.

Implication: Absent entity-wide strategic plans to recover from a disaster and restore normal operations, restoration of business processes and information systems will likely be delayed, and the organization is likely to incur unnecessary financial losses in the event of an emergency or other unplanned interruptions. Such losses include lost resources and/or unnecessary expenses, due to the need to expedite restoration of services.

Recommendation: We recommend that management develop a business-wide continuity plan that includes in it a disaster recovery plan as an element or subset of that plan. Elements of a plan may contain these elements:

- Business strategy and mission
- Critical business functions and priority for restoration
- Key contacts with roles and responsibilities
- Procedures for restoring critical business functions
- Plans and documentation for testing the overall plan including all elements
- Other necessary information for overall business recovery

Metro should develop a business continuity awareness program that includes distributing the plan to employees, and outlining parameters for testing the plan.

Management's Response: A complete review and management analysis of existing disaster recovery plans for information technology in Metro will begin in FY01-02. While limited funding will hamper efforts to provide a solid approach, a design of a minimally appropriate plan for recovering critical business functions will result.

Information Systems Communication Procedures

***Observation**:* We observed two information technology groups at Metro: Data Resource Center (DRC) and Information Management Services (IMS). These groups do not adequately communicate with each other to ensure proper control over the use of hardware, software, and network connectivity. Although DRC supports specialized business applications (e.g. mapping and graphical information tools, transportation and growth statistical packages) and IMS provides full desktop support (e.g., word processing, email, Internet connectivity, and access to the essential financial systems) both groups share the same network and server hardware. As a result, the operations of one group directly affects the operations of the other.

Additionally, we observed no overall strategy exists to ensure that both groups together operate in a manner consistent with Metro's overall business goals and objectives. For example, each group may purchase substantial computer equipment for a specific need, and not communicate these purchases in a timely fashion to the other group. As well, no formal standards or strategy guide either group.

***Implications**:* Without proper communication between these groups about operations, infrastructure changes, strategy and acquisitions, the overall ability to monitor and control the network, administer access, ensure authorized access, and restore systems in the event of an emergency can be jeopardized. Considerations include:

- Lack of common hardware and software standards
- Unknown physical access to computer hardware
- Undefined administration procedures over access to application systems
- Lack of a common information systems strategies and plans

Additionally, when DRC and IMS do not communicate, efficiencies and economies achieved by sharing resources are lost. For example, while both IMS and DRC share the same network and computer room, they share almost none of the hardware or software components. When one department may need more server capacity, they simply have to buy a new server instead of sharing unused space on an already purchased server owned by the other department.

***Recommendation**:* We recommend Metro leverage the existing ITSC to facilitate the routine communications between IMS and DRC thereby ensuring common standards are used. The ITSC should monitor that new purchases, infrastructure changes, and operations procedures are adequately communicated between the two groups to ensure proper use of organizational resources.

> ***Management's Response:*** Integration of the DRC and Information Technology Department needs, resources and staff is occurring on many fronts. Two positions from the IT Systems and Network Division now support the Data Resource Center computing base-both desktops and servers. A proposal to the agency to energize Metro's Web presence includes the transfer of a DRC FTE to IT for the programming and support.

An upcoming upgrade of the main data storage device in DRC will incorporate agency-wide needs. The Information Technology Steering Committee serves as a conduit of information for all departments, and the result is DRC and IT Department representatives always work on projects together.

Logical Security-Unix and Novell

Observation: We observed several opportunities to modify Metro's system security parameters to strengthen security over unauthorized access.

For example, in the Unix (PeopleSoft) system, we observed the following:

- Ten accounts are disabled. Most of these accounts are system/pseudo-ids;
- Five accounts have trivial or no passwords assigned to them;
- Passwords for all accounts have never been changed. Password aging features are not used on the machine so the system does not store the last password change date;
- Several sensitive files with world-writeable permissions on them. These accounts should be examined, and the associated permissions reviewed; and
- The powerful accounts (e.g. those with a UID = 0) can access the system via *ftp*.

We also observed these Novell (user log-ins) system security parameters:

- Eleven user accounts with one or more Supervisory rights;
- Eight users with *direct* security equivalence privileges to *Admin*, seven users who are members of Administrators Group, which has supervisory rights over [Root], and five users are members of Admin Wannabees Group, which has supervisory rights over [Root];
- Passwords for 35 accounts can only be changed by a security administrator;
- Although the minimum password length required is 5 characters, 154 accounts are allowed to select a zero-length (null) password;
- Password changes are not enforced for 219 users. This includes users with security administration privileges;
- Old or previous passwords can be reused for 258 of accounts;
- Users are allowed to sign-on to the system via multiple devices at the same time; and
- 248 accounts have not been used in the last 3 months.

Implications: Without consistent and robust user account privilege controls, unauthorized users can enter the system thereby accessing confidential data, and other proprietary systems.

Recommendation: We recommend Metro review those accounts with [Root] and administrative access and determine if these privileges are appropriate. Metro should ensure all accounts are uniquely identified with user names and passwords. Those accounts lacking password expiration parameters should be modified and password aging features enabled. Routine password aging, password expiration, and denial of account access should be enforced for all users. Inactive accounts should be removed.

2000 Status Update: In Process. In the past year, IT has focused heavily on system security in both the Unix and Novell environments. Practices, such as password aging and limiting account access, have been implemented to maintain a secure environment. IT will be better positioned to address the remaining security issues with an upgrade to Novell's eDirectory. Access review is an ongoing responsibility of IT's new security analyst.

> ***Management's Response:*** In the coming year, the Network and Security personnel will do a comprehensive security review to revise and improve the methodology used to establish security permissions. This is both to resolve this issue, and to prepare for the changeover from Novell to a Unix-based network operating system.
>
> There are some specific responses important to note regarding audit comments.
>
> *PeopleSoft Unix system*
>
> - 10 accounts are disabled.
>   - These are required system accounts.
> - 5 accounts have trivial or no passwords assigned.
>   - There is now only 1.
> - Passwords have never been changed.
>   - Password aging is now running for all user accounts with passwords expiring every 60 days. The system administrator will manually change system accounts on an individual basis.
> - Sensitive files with world-writeable permissions.
>   - Permissions were changed on. profile, .login, /etc/default/login, /etc/passwd, etc/exports, /etc/services, etc/hosts.equiv, /etc/inetd.conf and ~/.rhosts. Additionally, the Security Administrator disabled some of the 21 active network services, changed permissions on the trusted hosts file including removing the '+' symbol and reduced the 12 .rhosts files to 7.
> - Powerful accounts with UID = 0 can access the system via ftp
>   - The number of people able to do this has been reduced from 17 to 5. These five people are responsible for PeopleSoft maintenance, upgrades, etc. and are required to have this access.
>
> *Novell Network*
>
> Password aging is now set to 30 days (from the previous 60 days). All user accounts now have a minimum password length of 6 characters and the last 10 passwords cannot be reused. Intruder Lockout is set to logout a user for 30 minutes after 6 invalid login attempts in 15 minutes.
>
> The Security Administrator has a process in place for dealing with terminated accounts. Information comes from Human Resources on terminations and the Administrator then disables those accounts immediately. Accounts initiated from sources other than Human Resources (as new hires) are set up with an expiration date. This ensures that the account will expire automatically.

ACCOUNTING AND ADMINISTRATIVE

NEW COMMENTS

MERC

Observation: During our procedures, we noted that there had been significant turnover in the higher-level management of MERC. Such high turnover of management coupled with significant transactions (e.g., the concession contract with Aramark) increases risk. The turnover has also affected the progress of account reconciliation clean up and has resulted in excess time spent by Metro explaining the position of the accounts and the necessary steps to resolve the issues.

Recommendation: We recommend that Metro management increase its oversight of MERC during this transition period. We further recommend that MERC strive to create a work environment that will increase the retention of higher-level management and personnel within the accounting group.

> ***Management's Response:*** The transition period is complete with the necessary elements of the transition in place. In order to address the historical financial reporting challenges, MERC Administration staffing was restructured. The restructuring adds additional strength to MERC financial and accounting services. MERC has filled key financial positions with staff with specialized expertise, including a Director of MERC Administration with over ten years of governmental finance, the last seven years overseeing, on behalf of the City of Portland, Oregon, the largest multi-sports and entertainment facility in Oregon, the Rose Garden. In addition, the staff includes an Accountant who has ten-years of previous Metro experience in accounts receivable, with an emphasis on reconciliations. Also, to ensure the timeliness of information between facilities, MERC, and Metro, two experienced Administrative Technicians were added to the staff.

Zoo Foundation Contributions

Observation: The Oregon Zoo Foundation contributions are not remitted to Metro by the Foundation in a timely manner. During our analysis of revenues for the year ended June 30, 2000, we noted that $337,500 of revenues received by the Foundation during the fiscal year ended June 30, 1999 were not remitted to Metro until September 1999 (fiscal year 2000). Furthermore, Metro was not aware of the contributions until they were received. We also noted that Metro does not currently reconcile the general ledger account balances to the Oregon Zoo Foundation contributions.

Recommendation: We recommend that Metro reconcile the general ledger account balances to contributions reported by the Zoo Foundation on at least a quarterly basis. Furthermore, we recommend that Metro send the Oregon Zoo Foundation cut off inquiries at the end of each quarter requesting information on funds received by the Oregon Zoo Foundation but not yet remitted to Metro.

Management's Response: Metro must first identify the remittance requirements from the Oregon Zoo Foundation to the Oregon Zoo. Metro has identified that the existing contract with the Friends of the Zoo (now the Oregon Zoo Foundation) is over 15 years old (dated March 29, 1985). Within this existing contract, only two payments to Metro are required and are annual payments– a five dollar reimbursement to Metro for each membership (paid in the first month of each fiscal year) and an annual fee of $100 for reciprocal admittance. Metro will establish procedures to reconcile these amounts annually, if they are found to still be applicable. There is no current contractual requirement for the Oregon Zoo Foundation (OZF) to remit other contributions to Metro at specified times. Therefore, additional reconciliation procedures will await development and implementation of any new or revised contract provisions between the Oregon Zoo and OZF (or identification of assertions made by OZF's bylaws). The Oregon Zoo will investigate with OZF and Metro's Counsel and Contract offices the development of a new or revised contract stating these requirements, as needed.

RECURRING COMMENTS

New Reporting Model

***Observation**:* In June 1999, the Governmental Accounting Standards Board ("GASB") issued its Statement No. 34, *Basic Financial Statements – and Management's Discussion and Analysis – for State and Local Governments.* This statement will require dramatic changes to the way that Metro collects information about transactions, records certain transactions in its ledgers, and reports its financial information in accordance with generally accepted accounting principles. Such changes will be effective for Metro's fiscal year ending June 30, 2002.

Statement No. 34 changes the framework of financial reporting for state and local governments and represents an important change in the history of accounting and financial reporting for state and local governments. A partial list of the requirements of this new standard follows:

- Reporting of Management's Discussion and Analysis ("MD&A") as required supplementary information – similar to what is required for public companies when reporting to the Securities and Exchange Commission

- Reporting of government-wide financial statements on a full accrual basis

- Presentation of statement of activities on a "cost of service" basis

- Reporting fund financial statements on a modified accrual basis with separate reporting of major funds

- Redefinitions of certain fund types

- Preparation of cash flow statements using the direct method

- Reporting of all capital assets and recording depreciation in the government-wide financial statements

- Elimination of interfund loans, services and uses, and transfers in the government-wide financial statements

Several of these changes may require significant research and preparation on the part of Metro prior to the year of implementation.

Recommendation: Management should obtain an understanding of the provisions of GASB Statement No. 34 and determine a plan of action with regard to implementation. The plan might include such things as: redefining the funds used by Metro, the availability of data (for example, the cost of fixed assets), the ability of Metro to collect and summarize the necessary data (for example, direct and indirect costs of activities for reporting on the statement of activities), and the expected timeline for gathering this information and the resources available or to be procured to achieve that timeline. Should additional resources be determined to be necessary, appropriate funding and budget adjustments should be pursued.

> ***Management's Response:*** Metro recognizes the significant work effort to implement this required standard. Given current and proposed budget scenarios for Administrative Services that do not provide for outside assistance, implementation of this standard will continue to be a challenge unless other currently assigned work is deferred. Accounting staff has begun developing an implementation plan and will work on this project as priorities permit, beginning in February 2001.

Fixed Assets

Observation: Metro has not performed a complete inventory of its fixed assets in more than nine years. Furthermore, Metro has not tagged fixed asset additions, except for Metro Regional Center assets, in the last six years. This increases the risk of unrecorded disposals and lends to weakened property management.

Recommendation: We recommend that Metro perform a complete physical inventory of all fixed assets at least biannually. Furthermore, all assets should be tagged with an identification number. This will allow Metro to properly manage its assets.

> ***Management's Response:*** Contractor assistance to conduct a complete physical inventory and tagging of Metro's fixed assets is not possible due to budget constraints. In response, management continues to believe a long term sound approach to resolving this issue is to develop and implement written policies and procedures for on-going tagging (preferably at point of receipt of the asset) , inventory counts and reporting. It is management's intent to assign this project to the Accounting staff in conjunction with implementation of GASB 34 and the new fixed asset reporting requirements. Progress is dependent upon priorities assigned to the Division.

Accounts Receivable

Observation: Several departments do not maintain an allowance for doubtful accounts receivable. We specifically noted that the Solid Waste Fund was the only fund to establish an allowance for doubtful accounts. Based on our analysis of receivables as of June 30, 2000, MERC and the Solid Waste Fund had amounts of $122,517 and $83,227, respectively, which were more than 90 days past due.

Recommendation: We recommend all departments review an aging analysis of their accounts receivable and establish an allowance for those receivables that are potentially uncollectible. Accounting Services should be given the authority to record the allowance for doubtful accounts for financial reporting purposes.

> ***Management's Response:*** As part of its AR system, MERC currently maintains an aging report and makes collection efforts for accounts that are 30 days past due. MERC is developing formal procedures for collection of past due accounts. In addition, MERC is developing a policy for accounting for uncollectibles. MERC will perform an aging analysis of accounts receivable for PCPA, OCC, and Expo and establish an allowance for those receivables based on the past collection history of the organization.
>
> Furthermore, MERC is also taking a pro-active approach by working with Metro's Credit Manager and running credit checks on various promoters prior to renting a space at MERC facilities. This will reduce the likelihood that an account will eventually prove to be uncollectible.
>
> For other receivables, and with the completion of the upgrade to version 7.02 of the PeopleSoft Accounts Receivable and Billing applications in January 2001– Accounting staff will turn its attention to re-engineering of business processes for invoicing of transactions in areas beyond Solid Waste on PeopleSoft. This will enable detailed aging reports, and provide more timely information for conducting aging analysis and establishment of allowances in other areas.

Bank Reconciliations – Reconciling Items

Observation: The bank reconciliations contained several reconciling items. Many of the reconciling items had been outstanding for several months and were under investigation. Based on our analysis of cash as of June 30, 2000, MERC had reconciling amounts of $250,375. The remaining funds, individually, had reconciling items in amounts less than $16,000.

Recommendation: We recommend that Metro investigate and adjust for reconciling items in a timely manner once the details of the difference have been identified. Adjustment of these reconciling items will simplify subsequent bank reconciliations.