Metro

Administrative Services Department

Review of General Information System Controls

September 1998

A Report by Deloitte and Touche LLP
Issued by the Office of the Auditor

METRO

1998-10134-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

September 28, 1998

Councilor Jon Kvistad, Presiding Officer
Councilor Patricia McCaig
Councilor Ruth McFarland
Councilor Susan McLain
Councilor Rod Monroe
Councilor Don Morissette
Councilor Ed Washington
Mike Burton, Executive Officer

Re: Review of general information system controls

As part of their audit of Metro's financial statements, Deloitte & Touche studied Metro's internal control systems, focusing on general information system controls. They also performed procedures related to certain newly implemented PeopleSoft modules as well as operating systems and desktop software. At my request, they prepared this report describing their observations.

The report includes observations and recommendations addressing adequacy of staffing, information systems security, disaster recovery planning and help desk management.

We reviewed this report with the Executive Officer, Chief Financial Officer, Information Management Services Division Manager and other applicable staff. The written response of Executive Officer Burton follows the Deloitte & Touche report.

Metro staff responsible for implementing and operating the PeopleSoft modules and other systems have worked, and continue to work, diligently and intensely. Deloitte & Touche's observations suggest that additional resources are necessary to adequately staff continuing implementation efforts and, possibly, day-to-day demands of operating these systems. I concur with this suggestion and support the actions outlined in the Executive Officer's response. I

encourage Metro to continue to provide adequate information system resources to ensure satisfactory security for Metro's assets and systems and to ensure that information system long-term benefits are realized.

We appreciate the cooperation and assistance provided by staff in the Administrative Services Department.

Very truly yours,

Alexis Dow, CPA
Metro Auditor

AD:ems

Auditor: Deloitte and Touche LLP

Deloitte & Touche LLP

Suite 3900
111 S.W. Fifth Avenue
Portland, Oregon 97204-3642

Telephone: (503) 222-1341
Facsimile: (503) 224-2172

July 1, 1998

Ms. Alexis Dow, CPA
Metro Auditor
Metro
600 N.E. Grand Avenue
Portland, Oregon 97232-2736

Dear Ms. Dow:

As part of our audit of Metro's general purpose financial statements for the year ended June 30, 1998, we are in the process of obtaining an understanding of internal control, including information system controls, in order to determine the nature, timing, and extent of our audit procedures. To date, we focused attention on general information system controls, specifically those around the newly-implemented PeopleSoft system concentrating on related internal controls as defined by existing policies. We performed procedures related to the PeopleSoft modules operating on the HP 9000 systems, and the associated UNIX operating system, Novell operating system for the network servers, and the Windows 95 client software.

As of May 1998, Metro utilizes the following PeopleSoft modules:

- General Ledger;
- Accounts Payable;
- Purchasing;
- Payroll; and
- Human Resources

Metro plans to implement the Billing and Accounts Receivable components in the fall of 1998. Also planned is an upgrade to version 6.0 for the General Ledger, Accounts Payable and Purchasing modules. Project costing, asset management, budget, and time and labor will be completed pending the release of PeopleSoft version 7.5.

Our work was conducted in June 1998 and included tests of selected records, program processing and system changes, and user access and management reports.

We focused on procedures to determine whether:

- input and output controls ensure that daily and converted data are entered and processed accurately and completely, and that the information output is reliable;
- reconciliations of numerical data, communication of system processing messages, and validation routines take place regularly;
- program change management includes appropriate authorization and documentation;
- backup and recovery procedures ensure that the system can be restored in the event of a system failure;
- controls over information security, confidentiality, and remote access are adequate;
- system documentation and user training are current, accurate, and complete; and
- adequately documented procedures are in progress to address the Year 2000 issue, planning, management notification, and system reviews.

Our observations resulting from the above focused procedures are set forth in the attached Appendix. Our observations relate to:

- Staffing adequacy;
- Development and monitoring of information systems security policies and procedures;
- Disaster recovery planning; and
- Help desk management.

These observations were reviewed with Karla Lenox, Supervisor, Financial Control and Reporting; Carl Basl, Senior Program Supervisor, Application Services; Joe Gross, Senior Program Analyst, Computer/Network Services; and Scott Moss, Manager, Risk, Contracts, Purchasing, Benefits and Emergency Services.

We also discussed with management the following observations for improving PeopleSoft and related information systems, as well as recommendations to further strengthen internal controls. Specifically, Metro should:

- Implement the on-line purchase system protocol for all departments; and
- Provide the purchasing staff with the PeopleSoft matching software (i.e., program which matches vouchers and purchase orders and removes disagreements prior to final processing) instead of being dependent on IMS to run the matching software.

This report is solely for the use of the Metro Council, the Metro Auditor, the Metro Executive Officer, and management.

Yours truly,

Deloitte + Touche LLP

STAFFING

Observation: Four Information Management Services (IMS) staff provide all PeopleSoft, UNIX and Informix support, while eight other IMS staff provide network administration and security support to approximately 500 users. Current department responsibilities include system maintenance, computer operations and security administration for the HP, NT, Novell, PeopleSoft (General Ledger, Accounts Payable, Purchasing, Human Resources, and Payroll), and desktop systems. Administration includes user account maintenance (e.g., establishing/ removing users), evaluating security audit logs, implementing necessary security (e.g., changing passwords, network drive access), applying fixes to PeopleSoft (e.g., troubleshooting), completing file and database backups/restores, and configuring new systems.

Given the limited number of Metro IMS staff, we observed:

- Limited formal documentation of policies and procedures (e.g., process flow diagrams, security policies);
- No re-definition of job responsibilities given the migration from mainframe to client/server;
- Limited cross training resulting in knowledge gaps and insufficient technical depth to support the PeopleSoft system and its pending upgrades; and
- Single person reliance for critical systems (e.g., database administration).

Implication: With limited IMS staff, and uncertainty with new job responsibilities, critical tasks may go uncompleted, system operations may be jeopardized, and data integrity could be compromised. For example, current user access rights might not reflect actual job responsibilities. Therefore, users with higher than appropriate access might implement unauthorized system modifications. Moreover, with a thin staff, less proactive monitoring (i.e., staff notified of system changes or detecting unusual system performances) takes place. Thus, the organization would respond to possible problems reactively, and often more expensively than proactive monitoring or outright prevention. Finally, with minimum documentation and single person reliance, when problems arise staff may not respond timely or properly, and critical tasks could be left incomplete.

Recommendation: Responsibilities and resource levels necessary to support critical business functions on all platforms should be evaluated. This process should ensure adequate resource levels are available to satisfy user demands while minimizing internal control related risks. This review should consider changes in the information systems environment from mainframe (i.e., typically fewer responsibilities through centralized operations) to client server (i.e., greater responsibilities resulting from a de-centralized network and applications management).

At least two staff members should be able to provide fundamental technical services for information systems essential to Metro's operations. Where double coverage is lacking, management must initiate cross training, additional hiring, outsourcing, developing detailed documentation materials, or other remedial actions.

Where Metro might implement automated tools to augment single person reliance, suitable personnel resources should still exist thereby ensuring proper testing, installation and deployment, training, and on-going maintenance.

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES

Observation: We observed that Metro has a Computer Users Handbook, which was last updated in May, 1997. However, the handbook does not contain documented system policies such as equipment and applications usage, passwords and user naming conventions, or new user configurations for the PeopleSoft application and the network. Procedures describing removing or modifying network or PeopleSoft access are also absent. Rather, new user access to PeopleSoft is established through an unwritten policy developed between IMS and the functional leads. Thereafter, user requests are haphazardly logged and monitored.

We further observed that the procedures to ensure timely removal or modification of access privileges for terminated, transferred employees or outside contractors are not routinely followed.

Human Resources produces a terminated or transferred employee listing indicating those Metro staff no longer with the organization or staff whose positions/responsibilities changed. However, IMS does not regularly receive this list, so timely updates are not performed.

Implication: Without formal information systems policy documentation and routinely communicating polices to end users, inappropriate system usage can take place. Users who are not removed from the system in a timely manner may cause unauthorized transactions or system changes.

Recommendation: A policy and procedure document should be developed, distributed and acknowledged by all computer users. For example, this document should include but not be limited to the following:

- Procedures for adding new user and temporary employee access, if any; for removing terminated employee access; and for changing access privileges when job functions change;

- Password usage standards (e.g., naming conventions, minimum password length, periodic password change requirements, confidentiality of passwords, expiration and changing);

- Procedures for reviewing potential security violations; and

- Procedures for periodic review of network security, shared network drive access and specific user entry privileges.

Once policies and procedures are developed, they could be posted in the existing Lotus Notes databases or on Metro's intranet web site. These documents would then be available to all users, and could be dynamically updated to reflect system changes.

Security administration personnel should monitor for policy compliance. The policy should be periodically reviewed to ensure adequacy in light of changes in technology or operations. These policies should be evaluated along with the Metro's strategic plan for consistency.

DISASTER RECOVERY PLANNING

Observation: We understand an initial disaster recovery plan was created in 1995. However, the plan has not been updated, and several critical components are missing. For instance, no detailed references discuss tape locations, critical staff contact numbers, descriptions of key programs and libraries, system backup procedures or system restart documents exist. Furthermore, system-wide disaster recovery testing has not occurred. Consequently, it is difficult to determine whether or not Metro's current arrangements, discussed below, are adequate to sustain an unexpected disaster.

Metro has an off-site tape backup agreement with File Pro-Tech. File Pro-Tech picks up tapes daily comprised of network data. However, a similar process does not routinely occur for Metro's other systems (e.g., PeopleSoft, UNIX or Informix).

Also, Metro maintains service level agreements with critical vendors in the event hardware or software replacements are needed. However, a more comprehensive remedy should be considered, such as maintaining secondary hardware at an alternative site to run all critical business applications.

Implication: With many new business applications and processes introduced over the past year, a fully integrated test of the recoverability of all significant business applications and telecommunications connectivity has not been performed. As a result, it is unknown whether full information system and data recoverability is possible. Without a well defined disaster recovery plan, activities to be followed in the event of an outage or disaster are not available, and Metro may be unable to continue its processing in a timely and routine fashion. If data is not routinely backed up to tape, in the event of drive failure, critical data may be unrecoverable.

Recommendation: We suggest Metro review its existing service level agreements (hardware and software) for length of coverage and terms for replacement. We also recommend Metro develop and document a comprehensive disaster recovery plan. This plan would facilitate alternative processing capabilities should a disaster occur. The plan should include information systems and information services, such as computer hardware, software and telecom facilities. Once developed, the plan should be tested on a yearly basis.

In light of maintaining secondary hardware at an alternative site, we encourage Metro's IMS group to continue pursuing technologies such as duplicate drives, drive mirror capabilities (e.g., RAID-5 coverage), or writing data to a secured remote location.

HELP DESK

Observation: We observed IMS uses a Lotus Notes database for its help desk function. The help desk operator has numerous responsibilities (e.g., Administrative Secretary for the IMS Division) and handles approximately 400 non-PeopleSoft and 20 PeopleSoft user requests monthly. The Lotus Notes database produces a status report, which documents all calls, calls assigned, and performance statistics (e.g., number of calls, time spent resolving problems), however, a formal call prioritization (i.e., 1 equals most critical and 5 equals least critical) is not included in the status report. We also observed these status reports are reviewed, however only in an intermittent fashion.

Implication: Without consistent help desk prioritization, problems may be resolved in an inefficient manner, (e.g., common problems may be addressed multiple times instead of developing a common solution). Additionally, some calls may remain unanswered for an extended time period, and help desk assignments may take priority over other work responsibilities. As a result, other systems work remains incomplete.

Recommendation: We encourage the IMS group's purchase of automated help desk tracking software. In conjunction with the software purchase, we recommend Metro consider establishing help desk procedures for allocating and prioritizing help desk calls, cross train others within the IMS group, and thoroughly document procedures. In the interim, we suggest Metro routinely review the help desk generated reports, and perform problem analyses. In addition, a formal and central help desk function should publish monthly statistics listing common user/branch problems and solutions. With this statistical information, common questions can be identified, prompt responses prepared and specific training sessions can be developed. Metro might consider placing these frequently asked questions and solutions on their intranet web site.

Response to the Report

M E M O R A N D U M

METRO

Date: September 25, 1998

To: Alexis Dow, CPA, Metro Auditor

From: Mike Burton, Executive Officer

Re: Response to Deloitte and Touche Letter Regarding PeopleSoft Implementation and Internal Controls

I received the audit letter prepared by Deloitte and Touche regarding internal controls and implementation of PeopleSoft dated July 1998. The following constitutes a response to the four recommendations, a proposed action plan and timetable.

1. **Staffing Recommendation**: *"Responsibilities and resource levels necessary to support critical business functions on all platforms should be evaluated."*

- Agreement with Recommendations: Agreed.

- Proposed Action Plan: IMS has already begun a review of staff responsibilities in the Network, Helpdesk, and Applications support areas which will be coupled with an analysis of skill sets of current staff. IMS has lost critical staff over the past two years and this has seriously affected the IMS knowledge base. The IMS Manager has been working closely with Human Resources to develop more effective recruitment and retention strategies for staff while at the same time assessing the financial and organizational practicalities of using more contractor staff. . Concurrently, IMS has been investigating automated tools in each of the above support areas. This critical area is also addressed in the recently released draft of the Information Technology Strategic Plan.

- Proposed Timetable: The review and analysis of responsibilities and skills coupled with an assessment of appropriate automated tools will be completed by December, 1998. Ensuring appropriate resource coverage through highly skilled staff will continue to be an issue. The IT team will be presenting Metro's draft I.T. Strategic Plan to me in October.

2. **Information Systems Security Policies And Procedures Recommendation**: *"A policy and procedure document should be developed, distributed, and acknowledged by all computer users."*

- Agreement with Recommendations: Agreed.

- Proposed Action Plan: IMS currently has an outdated IT security policy and procedure document. However, it will provide an adequate baseline for developing a more robust and updated document that reflects many of the recent security demands of PeopleSoft. This document will then be available in hard copy and eventually on a Metro intranet helpdesk page. This would be an appropriate project to outsource along with the Disaster Recovery Plan discussed below should appropriate funding be available. This critical area is also addressed in the recently released draft of the Information Technology Strategic Plan.

- Proposed Timetable: The development of an IMS Systems Security Policy and Procedure will be completed by December, 1998.

3. **Disaster Recovery Planning Recommendation**: *"We suggest Metro review its existing service level agreements (hardware and software) for length of coverage and terms for replacement. We also recommend Metro develop and document a comprehensive disaster recovery plan."*

- Agreement with Recommendations: Agreed.

- Proposed Action Plan: IMS will be developing a disaster recovery plan that reviews both application and network issues. IMS currently has a contract with Applied Information Services to inventory and analyze Metro's network infrastructure. The inventory phase has been completed and the next phase will make recommendations for a server consolidation process that will include a review of system robustness, mirroring capabilities, etc. This information will provide the basis for preparing a Disaster Recovery Plan.

- Proposed Timetable: A Disaster Recovery Plan will be completed by March, 1999.

4. **Help Desk Recommendation**: *"We encourage the IMS group's purchase of automated help desk tracking software. In conjunction with the software purchase, we recommend Metro consider establishing help desk procedures for allocating and prioritizing help desk calls, cross train others with the IMS group, and thoroughly document procedures."*

- Agreement with Recommendations: Agreed

- Proposed Action Plan: IMS is already analyzing the feasibility of an automated help desk-tracking package. Soon a request for information (RFI) will be issued to gauge the market for this software. IMS has also created a help desk procedure manual which we will be continuously enhanced and updated.

- Proposed Timetable: IMS expects to issue an RFI for automated help desk software in October and with a 30 to 45 day response window. Further actions will depend on responses received, cost, and staff availability for set-up, training, and implementation.