METRO

Financial Statement Audit Management Recommendations

April 2005

A Report by the Office of the Auditor

METRO

PEOPLE PLACES
OPEN SPACES

Alexis Dow, CPA
Metro Auditor

600 NORTHEAST GRAND AVENUE | PORTLAND, OREGON 97232 2736
TEL 503 797 1540 | FAX 503 797 1793

METRO

OFFICE OF THE AUDITOR

April 6, 2005

To the Metro Council and Chief Operating Officer:

As a by-product of their audit of Metro's financial statements, Grant Thornton LLP made observations related to Metro's internal control and other accounting, administrative or operating matters. The accompanying report describes their observations and related recommendation.

Grant Thornton LLP recommends action in the following area:

- Metro's Information Technology department should develop and implement a process to prepare and review network security logs as well as document the performance of this review.

The report also presents management's response to this recommendation.

We appreciate the cooperation and assistance provided to Grant Thornton LLP by staff in the Business Support, Finance and Information Technology departments.

Very truly yours,

Alexis Dow, CPA
Metro Auditor

Grant Thornton

Accountants and Business Advisors

March 14, 2005

Councilors, Council President and Auditor
Metro
600 Northeast Grand Avenue
Portland, Oregon 97232-2736

Ladies and Gentlemen:

In connection with our audit of the financial statements of Metro as of June 30, 2004, we noted certain matters that we believe you should consider. Our observations were formed as a by-product of our audit procedures, which did not include a comprehensive review for the purpose of submitting detailed recommendations. The matters discussed herein are those that we have noted as of November 15, 2004 and we have not updated our procedures regarding these matters since that date to the current date.

Network Security Logs

Observation:

During the audit we became aware that there is no regular review of network security logs. Network security logs document events that could have an impact on the security of the network system, such as hardware failure, virus activity, and unauthorized access or intrusion attempts. The review of security logs, though it will not prevent unexpected or unauthorized activity, may assist in the detection and timely identification of potential problems. The lack of such review could result in unexpected or unauthorized activity going undetected which potentially may allow the breakdown in the integrity of or loss of important data or other assets.

Recommendation:

We recommend that Metro's IT department develop and implement a process to prepare and review network security logs as well as document the performance of this review. Maintaining and reviewing the logs can be useful in identifying and monitoring any unusual network activity and may further identify problem trends in the network. Metro should develop written policies and procedures to establish the timeliness of reviews, what types of events the reviewers are looking for, and what actions should be taken for certain types of events. We recommend that Metro log and review failures on account logon events, directory service access, dial up access, object access, privilege use, system events, unusual events, and both success and failure on account management and policy changes.

We understand the IT department is currently developing a network monitoring system to address this issue.

Suite 800
111 S.W. Columbia
Portland, OR 97201-5864
T 503.222.3562
F 503.295.0148
W www.grantthornton.com

Grant Thornton LLP
US Member of Grant Thornton International

Management Response:

We are deploying an open source network monitoring system that will help us identify anomalous network activity (virus or hardware failure). All network devices within the Metro Regional Center and Oregon Zoo are configured for SNMP ("simple network management protocol"), and the network monitoring system is configured to be our centralized system log ("syslog") server. Various scripts will parse the syslog database and send email alerts. This project completion is expected by March 1, 2005.

The same network monitoring system will perform a worm scan of the collected SNMP data that can detect intrusion behavior based on trend data. This is in lieu of Metro upgrading it entire network core to have a dynamic defensive response hardware layer.

We run the "snort" intrusion detection system, and have its log files available for inspection if we are trouble-shooting or tracking an incident.

A number of internet/intranet servers currently send their log files to the "Superuser", which is examined by Brian Arthur and John Miller daily.

****

Should you desire further information concerning these matters, we will be happy to meet with you at your convenience.

Very truly yours,

Grant Thornton LLP

Metro

People places • open spaces

Clean air and clean water do not stop at city limits or county lines. Neither does the need for jobs, a thriving economy and good transportation choices for people and businesses in our region. Voters have asked Metro to help with the challenges that cross those lines and affect the 25 cities and three counties in the Portland metropolitan area.

A regional approach simply makes sense when it comes to protecting open space, caring for parks, planning for the best use of land, managing garbage disposal and increasing recycling. Metro oversees world-class facilities such as the Oregon Zoo, which contributes to conservation and education, and the Oregon Convention Center, which benefits the region's economy.

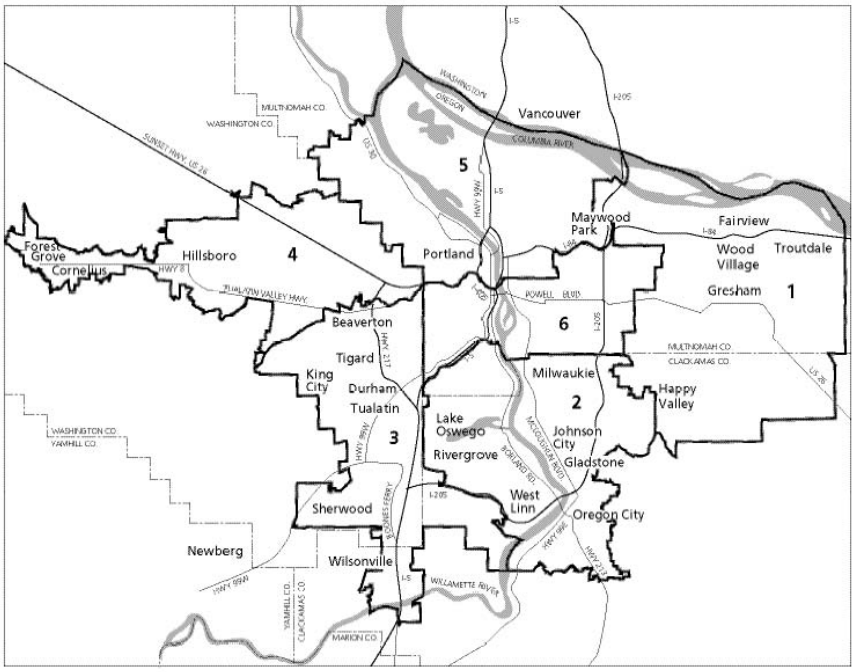
Your Metro representatives

Metro Council President – David Bragdon

Metro Councilors – Rod Park, District 1; Brian Newman, District 2; Carl Hosticka, District 3; Susan McLain, District 4; Rex Burkholder, deputy council president, District 5; Robert Liberty, District 6.

Auditor – Alexis Dow, CPA

Web site: www.metro-region.org



Council districts

You are welcome to keep this copy if it is useful to you.
If you no longer need this copy, you are encouraged to return it to:

Metro Auditor
Metro Regional Center
600 NE Grand Avenue
Portland, OR 97232-2736

If you would like more information about the Office of the Auditor
or copies of past reports, please call
Metro Auditor Alexis Dow, CPA
(503) 797-1891

Metro Auditor Suggestion Hotline:
(503) 230-0600 ♦ MetroAuditor@metro-region.org