Office of the Auditor

IT Software Controls Audit Follow-up

Progress made on recommendations

Michael Anderson
Senior Management Auditor

July 24, 2013

Background

Metro employees rely on information technology (IT) to do their jobs. The agency's work depends on creating, collecting and maintaining data. This data is used by the agency to inform decision making and provide effective and efficient governance.

In 2009, the Metro Auditor released an audit report with recommendations to improve Metro's management of IT resources. The audit found that Metro needed to define an IT framework and processes, clarify roles and responsibilities, and commit sufficient resources for these efforts. Six recommendations were included in the report (see Status of Recommendations on page 5). The recommendations focused on:

- creating a governance framework and establishing roles and responsibilities;
- moving the agency towards enterprise data management;
- standardizing the software development process;
- collecting data to evaluate the total cost of ownership for IT systems;
- developing employee training plans, and;
- implementing an agency information security policy.

In May 2011, the Auditor's Office completed an evaluation of Metro's management of its IT resources that used a modified version of the US Government Accountability Office's (GAO) high-risk criteria. The GAO developed criteria to identify weaknesses within the federal government that make programs particularly vulnerable to fraud, waste, abuse and mismanagement. The GAO's focus was to find the root causes of the weaknesses and to direct management to those problems. This office found that additional work was needed. It was unclear if Metro's management of its IT resources created a weakness across departments that increased the risk of fraud, waste, abuse and mismanagement.

This follow-up audit included steps to determine if an analysis based upon GAO's high-risk criteria should be applied to Information Services. Based upon the improvements we found, these steps were not completed.

Summary

Progress was made on the recommendations from the 2009 audit, **IT Software Controls:** *Agency-wide approach needed to ensure data accuracy.* We found that of the original six recommendations, one was implemented and the other five were in process.

SUZANNE FLYNN

Metro Auditor
600 NE Grand Avenue
Portland, OR 97232
tel: 503-797-1892
fax: 503-797-1831
www.oregonmetro.gov/auditor

Scope and Methodology

This audit had two objectives. The first objective was to determine the status of recommendations from the 2009 audit. We did not look at the status of the software controls for three IT systems evaluated in the original audit. We interviewed management and employees. We reviewed the department's strategic plan, employee training plans and information security policies. We reviewed IT project management materials including project proposals, work plans, status reports and closeout documents used by the department. We also reviewed charters, agendas, and meeting materials and minutes for committees which influence the department's priorities and work flow.

The second objective was to determine if the agency would benefit from a high-risk audit of the management of Metro's IT resources. A high-risk audit is a traditional performance audit that is focused on identifying areas that are especially vulnerable to fraud, waste, abuse or mismanagement. When high-risk areas are identified, actions to correct the problems are proposed and a formal monitoring process is implemented.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results

Metro's recent IT improvements could enable the department to implement the recommendations from the 2009 audit of IT software controls. Metro created a governance structure that should improve the management of IT resources. The newly created Project Management Office has standardized software development, and a recent enterprise review has provided a structure that will help the agency move towards enterprise data management. More work can be done to develop training plans for IS staff, implement a security policy for the agency and track the total cost of ownership for IT systems. The department needs time to fully implement these changes. As a result, of the six recommendations in the original audit, we found one recommendation was implemented and the other five were in process.

Progress made, more work needed

Governance structure

Information Services implemented several improvements to enhance its management of IT resources. The department developed a draft, 5-year strategic plan that will be revised later this year. The plan provided a clear description of the values, mission and goals for Information Services. The plan also included a detailed list of work activities to implement the plan. The department already completed some of them and was in the process of completing the rest. Although it is still a draft, the Information Services strategic plan provides general guidance and includes a specific work plan to implement its strategy.

Information Services also improved the management of IT resources with the Project Management Office (PMO), which was created to help process and prioritize IT projects. The PMO used a Prioritization Committee to review and approve certain projects. The seven-member committee is made up of directors from several Metro departments. The committee is responsible for ensuring

that IT projects achieve the strategic goals of the agency. The committee took an active role in the review process. For example, it declined to prioritize projects when there was inadequate budget information or because a large proposal needed to be broken into smaller steps.

Information Services also uses Memorandums of Understanding (MOUs) to outline the service level roles, responsibilities and objectives of Information Services and client departments. We reviewed ten MOUs and found that each one included language describing the agreement's purpose, background and goals, as well as time tables and a description of what services were not covered under the agreement. The MOUs also described how resources will be allocated and included dispute resolution language for senior management.

While MOUs described the services that Information Services agreed to provide, a separate Roles and Responsibilities document described which employees are responsible for the services listed in the MOU. We reviewed three roles and responsibilities documents. Each one described who was specifically responsible for maintaining system hardware and software, ensuring staff were properly trained, interacting with customers and billing for services. Some of the MOUs and roles and responsibilities documents were still in draft form and additional work was required to complete them.

Software development

The PMO also implemented a framework standardizing the process used to create or modify new software or hardware systems. While many IT projects went through the PMO before they were approved, some did not. For example, some renewal and replacement IT projects may bypass the PMO, possibly undermining the software development framework used by the department.

For projects that were reviewed by the PMO, a standardized intake form was used to collect key project details from the project manager. The details included information on the project's manager, sponsor, objectives, deliverables, milestones, the problem to be addressed and an estimate of the resources needed to complete the project. Once the project was defined, it was reviewed by the Prioritization Committee, which approved or denied the project. If a project was approved, the project manager executed it with support from the PMO.

Enterprise data management

Metro recently completed a review of its key technology systems. The first step of the two-part review focused on evaluating Metro's current IT systems and needs. The second step was a discussion of system improvement recommendations and an implementation work plan. Some of the recommendations addressed issues identified in the 2009 audit. For example, the review included detailed enterprise data management recommendations to reduce side systems and enhance Metro's existing accounting system to satisfy unmet needs and track costs. The department is in the process of creating a capital budget to implement key aspects of the plan.

Training plans

The department made progress developing training plans, although additional work is needed. Management made an effort to assess employee skill gaps and provide training opportunities to address those gaps. However, the quality of these efforts varied and there was not a clear connection between skill gaps and training opportunities. Management could develop a more systematic and consistent human capital management system that identifies and addresses skill gaps.

Security policy

The department had an acceptable use policy with security controls, but it was a draft that was waiting final approval. The plan generally assigned standard setting responsibility to Information Services and individual departments were responsible for ensuring that employees followed the policy. In addition, some of the security issues identified in the 2009 audit, such as user management policies for the agency's grant management system or security improvements to the Zoo's attendance and revenue systems, have not been completed. The recently completed review included recommendations to address these security issues, and the department was in the process of developing a budget to fund security improvements.

Cost of ownership

Information Services improved its ability to track the time and money spent on IT investments. The department was in the process of developing tools to determine the impact that new technology projects will have on staff resources. Some costs for large IT projects were tracked by the agency's finance department and Information Services. The department needs to continue to develop and apply a standard approach to track the total cost of IT ownership.

STATUS OF METRO AUDITOR RECOMMENDATIONS

2009 Recommendations	Status
1. In order to improve management of IT resources, Metro should define processes, organization and relationships of IT management, which includes assigning leadership, creating a governance framework, establishing roles and responsibilities and committing sufficient resources.	*IN PROCESS*
2. In order to create a strategic plan to gradually improve the effectiveness and efficiency of IT management in each of five key management areas, Metro should:	
a. Take steps to move the agency toward enterprise data management.	*IN PROCESS*
b. Collect data to enable departments and IT governance to evaluate the total cost of ownership of IT systems.	*IN PROCESS*
c. Standardize software development processes and procedures.	*IMPLEMENTED*
d. Develop written procedures and training plans.	*IN PROCESS*
e. Update and implement the information security policy for the agency.	*IN PROCESS*

600 NE Grand Ave.
Portland, OR 97232-2736

www.oregon**metro**.go

Metro | *Memo*

Date: Wednesday, July 17, 2013
To: Suzanne Flynn, Metro Auditor
From: Rachel Coe, Information Services Director
            Scott Robinson, Deputy Chief Operating Officer
Subject: Management Response to Information Services Audit

This document contains management's response to the IT software controls follow-up audit that will be issued by your office in July of this year. The Information Services department (IS) is committed to creating an environment in which Metro's information assets are useful, protected and effectively managed and that public dollars are spent wisely. While we have made great strides in these areas, we will continue to work towards our values of public service and excellence.

We want to thank the Metro Auditor for following up on this important topic and appreciate the recognition of the improvements made in both our processes and the integrity of our systems. We have taken some big steps to ensure the agency has visibility into how the resources in IS are used and have given the agency the ability to align the department's projects with the goals of the agency. We will continue to refine our systems with the intent of creating even greater transparency and accountability.

Below are management's response to the six recommendations submitted by the Auditor.

- Governance Structure and Software Development (in process)

Response:
As is mentioned in the audit report update, Information Services has created a governance structure for the department that includes a Project Management Office (PMO), a Prioritization Committee comprised of directors from departments across the agency, a 5-year strategic plan that outlines our department's approach to technology and a 5-year tactical plan, as well as Memorandums of Understanding (MOU's) with many of the technology stakeholders to help clarify service levels and roles and responsibilities. The department also created a list of software development standards for use on the web re-design project. This was necessary to ensure consistency from vendors.

Next Steps:
Information Services will refine and adopt a final version of its strategic plan in the current fiscal year. This will include stakeholder input and a communication plan. The PMO will complete a contracted development process for applications to give departments the option of working with outside vendors, but in a way that ensures Metro's standards are followed. This process will include our not only software development standards, but also a list of standard application platforms. As projects near completion, IS will work with contractors and stakeholders to develop MOU's that describe roles and responsibilities for the software, security, data ownership and integrity.

- Enterprise Data Management (in process)

Response:
In December, the review of Metro's technology systems was completed. The final report recognized the value of both our event management system and our financial accounting package. The recommendation was that retain both systems, but upgrade the financial system to take advantage of a number of functionality enhancements, further implement unused functionality and improve integration and reporting. IS and the Finance and Regulatory Services department (FRS) are currently developing a project plan for moving forward on these recommendations in the current fiscal year. We anticipate the plan to include a fit/gap analysis to determine highest priority enhancements, followed by an upgrade. Functional training for end users and updated user documentation will also be included in the project plan.

Next Steps:
Metro is also continuing to move forward on the web update project. This project continues to standardize not only Metro's web platform, but development for software programs on the web. Each of the applications currently on the site are being re-written for the new platform. They will each follow the same software development standards.

Finally, the Application Development and Maintenance group will be creating a roadmap for the most significant applications within the agency. This roadmap will not only help the organization understand the maintenance needs for these products, but will also help us engage in a dialog with the agency about where the highest priority enhancements should occur.

- Training Plans (in process)

Response:
A major goal of the IS department this year will be to identify primary and secondary responsibilities for systems and applications and to identify gaps in coverage and skill sets. We will then create staff training plans to address those gaps. For some operational gaps, we may propose other methods of coverage, such as contracted services or the addition of temporary resources. This project addresses one of the eight focus areas within the IS strategic plan.

- Security Policy (in process)

Response:
The acceptable use policy drafted in 2011 is in the final stages of the approval process and is expected to be adopted in August 2013.

Next Steps:
To address security needs for applications, IS is taking a couple of approaches. The Zoo attendance and revenue as well as the grants management systems will be included in the project plan to move forward on the recommendations from the technology review completed earlier this year. That plan is currently being developed by IS and FRS for the current fiscal year.

For all other software systems, IS is drafting a framework for application security. The document will provide guidance on principles of least access and the need for segregation of duties as well as user management procedures, including the need to review access privileges on a regular basis and removal of privileges when an employee is terminated or no longer needs them. This framework can be applied to all applications, including applications not directly administered by IS.

- Cost of Ownership (in process)

Response:
Many improvements have been made in our ability to track time and money spent on IT investments. Larger projects are identified early on and are given a project code in the finance system. These codes are used for both expenses related to the project and staff time. Currently, only IS staff time is being tracked on a regular basis.

Next Steps:
IS is working in cooperation with the Construction Project Management Office (cPMO) to provide additional tracking of resource availability and staff time spent on projects. The new budget software should also provide additional reporting capabilities and visibility for the cost of IS-related projects.

We would like to thank the Auditor and her staff for their efforts in following up on the audit from 2009 and in helping the Information Services department in our efforts to attain the agency's goal of responsible operations.

cc: Martha Bennett, Chief Operating Officer