




Office of the City Manager

INFORMATION CALENDAR

May 22, 2007

To: Honorable Mayor and
Members of the City Council

From:  Phil Kamlarz, City Manager

Submitted by: Chris Mead, Director, Department of Information Technology

Subject: Update: Implementation of Information Systems General Controls Audit
Recommendations (CF 69-04)

INTRODUCTION

In response to a request by the Director of Information Technology (IT) and the City Manager, in FY03 the City Auditor conducted an Information Systems General Controls Audit. The purpose of the audit was to determine whether or not the City's information technology infrastructure provided adequate physical, inventory, environmental, disaster recovery, and security controls.

The Audit findings and recommendations were presented to Council on September 16, 2003; the third update was provided from the Department of Information Technology on March 21, 2006, and can be found at: <http://www.ci.berkeley.ca.us/citycouncil/2006citycouncil/packet/032106/2006-03-21 Item 29 Implementation of Info Systems Controls Audit.pdf>

This update is meant to keep Council informed of our progress in implementing the outstanding recommendations. Another progress report will be delivered to Council in December 2007.

CURRENT SITUATION AND ITS EFFECTS

The following reports on progress regarding each outstanding recommendation.

Finding 2: Current password composition does not offer strong password protection and network passwords never expire.

According to A.R 4.2 that governs electronic mail, "Employees shall protect the City's security by regularly changing their private passwords." However, this policy is not enforced because passwords are set to 'never expire'. Users are not required to change their passwords periodically. In addition, the network passwords are set to have a minimum of five characters. This is not in accordance with the "best practices" published by Microsoft which recommends strong passwords be of at least seven characters consisting of letters, numerals, and symbols. There is also no composition requirement for the FUNDS\$ passwords, although users are required to change their passwords every six months because they expire. In addition, ten unsuccessful login attempts are allowed before the passwords are deactivated, exceeding the general practices of three to six attempts. Strong passwords are important because computer hackers continue to improve their

tools for cracking passwords. Weak passwords can be cracked in minutes by experienced hackers, increasing vulnerability to unauthorized access.

Recommendation 2:

- 2.1 Require all passwords to have at least seven characters consisting of letters, numerals, and symbols in accordance with Microsoft's 'best practices' standards.
- 2.2 Require users to change their network passwords every three to six months.

5/22/07 City Manager Response:

IT agrees with the audit finding and recommendations.

- 2.1 **Partially Implemented** FUNDS\$ password requirements have been strengthened since November 2003. Although migration to strengthened passwords had originally been scheduled for completion by 12/31/06, a critical staffing shortage related to unplanned medical leave necessitated that the project completion date change to May 16, 2007. In a memo dated 4/25/07, the City Manager notified all City staff that, beginning 5/16/07, network login will require strengthened passwords as described in Finding 2.
- 2.2 **Partially Implemented** As of 5/16/07, the network's authentication system will require employees to change network passwords every six months.

Finding 6 Activity or event logs are not reviewed regularly for possible security violations or system errors, reportedly due to limited staff resources.

Controls should be in place to ensure that a secure computer environment is maintained. One good control is the auditing function that is available in most operating systems. This function generates logs or reports that record activities or events such as access attempts, login failures and system performance that occur during the day or within a specified period of time. It is a tool that can be used to alert system administrators of system underperformance and possible security breach. A log can be configured to focus on particular users, objects or processes to serve a specific need. Currently, there is no procedure in place requiring these logs be reviewed regularly and it appears that existing activity data are not configured properly to facilitate meaningful review. Some logs are set up but are reviewed only when a problem occurs or is reported. The task of reviewing these logs can be personnel intensive. However, without the review, security violations and system underperformance may not be detected and rectified timely. Microsoft advocates the use of audit logs as an effective security monitoring tool: *"Some good controls include violation and exception reports that help management determine, at a glance, whether their systems are being compromised. Many times, corporations run reports that log violations; however, running these reports in itself does not satisfy this control. Either the report is gathering too much information, the proper violations are not being filtered, or no one is reviewing the reports. These reports are another set of controls that help mitigate security risks throughout the corporation, but we often see them overlooked."*

Recommendation 6:

Configure event logs and exception logs and review them on a regular basis. According to Microsoft's best practices, "... Auditing the system is not enough. In addition, the logs that hold the auditing information should be secured and maintained. In other words, security controls should be placed on the actual log files themselves to ensure confidentiality and availability when they are needed. ...The best way to secure these files is to create an auditor group that has access to these files, and then take it away from all other groups. The people assigned to the auditor group will be responsible for maintaining the data within the logs." ² Therefore, access to these logs should be restricted to personnel that are assigned to maintain and review the logs.

5/22/07 City Manager Response:

Partially Implemented IT agrees with the audit finding and the recommendation. However, budgetary constraints have slowed implementation of the staffing and tools necessary to complete comprehensive log analysis. Funding for improved log analysis tools has been secured and implementation has begun. Project completion is expected by November 2007.

Finding 7: Security controls over access to the City's network through the Internet are not adequate.

According to the Network Administrator, an employee who has to perform a City task from a location that is not connected to the network can request permission to access the network remotely by completing an authorization form. The form must be approved by his or her department director or the IT Director. All IT personnel are exempt from this requirement and are granted access automatically since their job duties often require them to access the network remotely. There are 47 approved authorization forms filed with the IT department. However, over 150 users including IT personnel have accessed the network remotely according to a system report. Out of the 150 users, the auditor reviewed the employment status of 40 users. One user had been terminated in 1998 and three users had been terminated in 2002. The user profiles of these four employees indicated that they continue to have remote access capability to the network. Since "auditing" was not turned on at the time of the fieldwork, the auditor was not able to determine if these employees had accessed the network after they were terminated. "Auditing" was turned on by the Network Administrator in response to the auditor's request. In addition, most City employees have remote access to their e-mail through the Internet. The remote e-mail server is located in the internal network. This setup opens a point of entry to the City's information resources from outside. The auditor found that any employee can log into the network through the Internet only if he or she knows the Uniform Resource Locator (URL) of the remote access server. The URL can easily be obtained from a co-worker who has the information. It appears that this information may have been shared by City employees since the number of users (150) greatly exceeded the number of authorization forms (47). This condition, coupled with weak password protection (Finding 2), terminated employees' user accounts not being cancelled promptly (Finding 4) and "auditing" not being turned on, cause the City's information resources to be very susceptible to unauthorized access.

Recommendation 7.2:

Review the remote access audit logs regularly to ensure only authorized employees have accessed the network from the Internet.

5/22/07 City Manager Response:

Implemented As of August 2006, all remote access logs are reviewed on a weekly basis as part of the technical policies committee meeting.

Finding 10: Fire protection for the computer room is inadequate and the air conditioning may not be functioning properly.

According to the Capital Improvement Programs Manager, the only fire protection devices in the Civic Center computer room are water sprinklers and smoke detectors. These are “general purpose” fire detection devices that are also installed in the rest of the building. Although water is an excellent fire suppressant, it also dampens sensitive computer equipment and is likely to cause irreversible damage. It does not appear to be the optimal solution for protecting computer equipment. In addition, the computer room generally has higher airflow meaning more smoke dilution than the rest of the building. A more sensitive detection device may be needed to provide early detection of a fire.

The air conditioning in the computer room may not be functioning properly to keep the room temperature at a desirable level. The optimal computer room temperature recommended by many experts is between 60°F and 70°F. One day the auditor observed that the outdoor temperature was around 65°F and the thermostat on the wall inside the computer room indicated 80°F. It was also noted that the temperature at the back of the room was even higher. Computer equipment is more prone to failure in high heat.

Recommendation 10.3:

Perform a risk analysis to determine an appropriate level of protection for the computer equipment. With budget limitations and other constraints, there may be conflicting priorities on expenditures. The cost of accepting a greater risk resulting from reduced expenditure must be carefully evaluated.

5/22/07 City Manager Response:

Not Implemented IT agrees with the audit finding and recommendations. However, budget and staff constraints have prevented a formal risk analysis. This item will be proposed as part of the Department of Information Technology's FY08 work plan, with an update to council no later than December 2007.

Finding 11.2 System servers located outside the Civic Center building may not be secured.

The auditor visited the Corporation Yard and observed that the servers were stored in an unlocked open area, increasing the risk for unauthorized access and theft. The same condition may exist in other locations.

Recommendation 11.2:

Require all servers to be locked in a cabinet at the minimum if a secured storage room is not available. Physical access should be monitored and limited to authorized personnel.

5/22/07 City Manager Response:

Partially Implemented IT agrees with the audit finding and the recommendation. Whenever a server is installed at a remote site, IT requests that a secure, ventilated closet be provided. Public Works plans to install a vault to secure the existing servers located at the Corp Yard as part of the Corp Yard renovation project. In addition, infrastructure and connectivity upgrades have facilitated the centralization of many remote servers into our centralized data center. We hope to continue our server consolidation and physical security upgrades, with a progress report to council by December 2007.

Finding 12.1 There is not a complete and accurate inventory of the City's computer equipment and software.

The auditor requested an inventory list of the City's computer equipment and software from IT. According to the Senior System Analyst, IT is working with each department to prepare a complete inventory of all desktops and printers. According to IT, the inventory list was approximately 50 to 60 percent complete as of May 2003. If the City does not keep track of the computer equipment it owns, it is very difficult to effectively safeguard its assets.

Recommendation 12.1:

Complete an inventory of the City's computer equipment, including desktops, printers, laptops, firewalls, routers, servers and software etc. The inventory report should contain a unique identification number or serial number for each item and the report should be updated once a year. In addition, if unused or obsolete computer equipment is identified during the inventory process, IT should make appropriate arrangement to dispose the equipment as prescribed by A.R. 3.5 – Disposal of Surplus Property.

5/22/07 City Manager Response:

Implemented IT agrees with the audit finding and the recommendation. Since 2005, DoIT has provided an online inventory of all desktop and network equipment (including servers, routers, switches, etc). In March 2007, DoIT instituted an online software inventory.

BACKGROUND

The Department of Information Technology is the custodian of all City computer hardware and software equipment. The feedback contained in the September 16, 2003 audit report served not only to validate previous managerial restructuring in the department, but also provided a framework for reporting additional network infrastructure and security improvements.

POSSIBLE FUTURE ACTION

The Department of Information Technology continues to upgrade network security and infrastructure improvements. Another progress report will be delivered to Council in December 2007.

FISCAL IMPACTS OF POSSIBLE FUTURE ACTION

None.

CONTACT PERSON/S

Donna LaSala, Supervising Systems Analyst, Department of Information Technology 981-6541.
Keith Skinner, Supervising Systems Analyst, Department of Information Technology 981-6551