



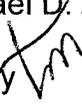
**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-2766
PHONE: (213) 974-8301 FAX: (213) 626-5427

J. TYLER McCAULEY
AUDITOR-CONTROLLER

May 10, 2007

TO: Supervisor Zev Yaroslavsky, Chairman
Supervisor Gloria Molina
Supervisor Yvonne B. Burke
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: J. Tyler McCauley 
Auditor-Controller

SUBJECT: AUDIT REPORT ON COUNTY FISCAL OPERATIONS

In conjunction with the annual audit of the County's financial statements, a review is made of the County's systems of financial internal control. Enclosed is the independent accounting firm's internal control report on Los Angeles County's operations for fiscal year 2005-2006. The audit report on the financial statements was previously sent to your Board.

The County departments' responses are included and recommendation implementation will be tracked as part of our established follow-up system.

Submission of this report to your Board completes the County's financial and grant audit requirements for fiscal year 2005-2006.

JTM-JN-CY:bh
Admin\management letter 05-06

Enclosure

c: David E. Janssen
Sachi A. Hamai
County Counsel
Audit Committee
Public Information Office
Affected Department Heads
Federal Audit Clearinghouse
State Controller's Office – Division of Audits

"To Enrich Lives Through Effective and Caring Service"



KPMG LLP
Suite 2000
355 South Grand Avenue
Los Angeles, CA 90071-1568

Telephone 213 972 4000
Fax 213 622 1217
Internet www.us.kpmg.com

January 22, 2007

Board of Supervisors
County of Los Angeles
500 West Temple Street
Los Angeles, CA 90012

Ladies and Gentlemen:

We have audited the financial statements of the County of Los Angeles (the County) as of and for the year ended June 30, 2006, and have issued our report thereon dated January 22, 2007. In planning and performing our audit of the financial statements of the County, we considered internal control as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County's internal control.

During our audit, we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized as follows:

(1) Logical Access Security to the Mainframe (IBM OS/390)

Observation

We noted that the mainframe's password configurations are not consistent with industry best practice guidelines. Presently, passwords are not required to include both alpha and numeric characters, the password history feature is not enabled, and user session time-out value (between transactions) equals to 45 minutes.

Impact

Without implementing strong authentication controls, the government agency's sensitive data may be exposed to unauthorized users.

Recommendation

To prevent the risk of unauthorized access, we recommend the following:

- 1) The County should enable password complexity within the mainframe systems environments. Password complexity parameter increases the number of password combinations and prevents users from creating easily guessable password.



Board of Supervisors
County of Los Angeles
January 22, 2007
Page 2

- 2) The County should also implement the password history feature that enables the system to keep a record of the previous passwords and prevent the user from repeatedly using the same passwords within a specified number of cycles.
- 3) The County should shorten user session time-out value (between transactions) from 45 minutes to 10 – 15 minutes. The increased session time-out value increases the risk of unauthorized access.

Management's Response

Internal Services Department (ISD) Information Technology Service (ITS) agrees with the recommendation. .

ITS will enable password complexity on the IBM mainframe. ITS will develop a plan by July 2007 which will outline an implementation strategy for password complexity. This plan will also include implementation of the password history feature, as well as an evaluation of the negative customer impact of shortening the session time out.

(2) Logical Access Control over the Security Administration functions in eCAPS

Observation

During our review of security in the eCAPS system, we observed inappropriate user accounts with access to security administration functions. Below is the list of the issues we encountered during our review:

- One user account, "Conversion", with security administrative access was deemed inappropriate, as the user account was used during the implementation of the eCAPS system to convert data from the old CAPS application to eCAPS. We noted the level of access granted to the "Conversion" account is excessive in relation to this function.
- Three user accounts with security administrative access were deemed inappropriate by management, as access is not commensurate with their job responsibilities.
- One user account with security administrative access appears inappropriate. The security administrative access does not appear to be commensurate with the Assistant Auditor-Controller's job responsibilities.
- One user account, "Offline" with security administrative access was deemed inappropriate by management. The user account was used by eCAPS to load documents into eCAPS. We noted the level of access granted to the "Offline" account is excessive in relation to this function.

Impact

The lack of adequate security and controls relating to users with security administrative access can potentially expose the County to an increased risk of unauthorized access to transactions and data in eCAPS.

Recommendation

We recommend that the appropriate individuals perform a detailed review over the validity of all users with security administration access to the eCAPS system. This review should be conducted to verify that



Board of Supervisors
County of Los Angeles
January 22, 2007
Page 3

only appropriate users have security administration access and their access is in line with their job responsibilities. Security administration access should be revoked for those users that should not have it.

Management Response

The Auditor-Controller concurs with KPMG's recommendation that the County review the administration access to eCAPS.

There are two levels of access inferred by using the term "security administrative access". The granting of the ADMN security role enables the user to bypass security restrictions normally invoked by a security role. These restrictions typically limit a user to inquire only, edit a table or document, and or approve documents. In this context, the users that are assigned this role are limited to within the Auditor-Controller's office. These users are upper-level management and they were assigned these roles on an interim basis as a safeguard to ensure that the County was able to conduct transactions in a seamless manner when eCAPS was implemented. We are in the process of working with management to define the access that is needed at their level to meet the business objectives of the County of Los Angeles while still maintaining an appropriate level of access via defined security roles.

The other level of access is the ability to modify user access by being assigned the ADMN security role. In order to modify user access, a user must have a security role that would enable them to do so (i.e. ADMN) as well as authority to access the Administrative database which is separate from the Financial Application. It is the combination of these that is required in order for a user to have the access to the tables to make such a modification. We have reviewed this combination and removed all users for which this was deemed inappropriate. In addition, we have configured a security role that grants inquiry access only to the security related tables. This security role has been assigned to a limited number of users within the Auditor-Controller's Audit Division so that they can also oversee user access levels. Furthermore, we are testing various security role configurations to determine how to grant access to execute online batch jobs, inquire on batch jobs, and perform other functions that at this time can only be done with ADMN rights. Testing should be completed by November 17, 2006 and implemented with the upgrade of the system to 3.6.

The ID "Conversion" has had all access to any security role removed in addition to being locked out of the system. The ID needs to remain for any open transactions that have not been finalized. This is required as the system verifies that the user ID is still valid when completing a transaction. In addition, the Audit Division within the Auditor-Controller is requesting that we do not delete any user IDs from the system until the full impact of such an action can be determined.

(3) Generic User Account

Observation

The County uses a generic "Dummy User" account to provide production support to its employees. Based on our review, the County does not maintain records tracking the activities of the users of the generic account and the security liaison approving the user access.

Impact

Generic user accounts make it difficult to assign accountability for actions associated with its use.



Board of Supervisors
County of Los Angeles
January 22, 2007
Page 4

Recommendation

We recommend that the County implement a tracking mechanism such as a log to track the users of the generic account as well as the security access provided to the users by the security liaison approving the user access.

Management Response

We agree with the recommendation and will develop a logging mechanism that identifies the user of the generic account, the time frame for which the account was used, and a description of the problem or issue that required resolution.

(4) Logical Access Controls over eCAPS – Revocation of Access Rights for Terminated Users

Observation

Based on our initial review of security in the eCAPS system, we observed that 65 active user IDs in eCAPS were related to employees that were terminated from the County during the period under review.

Subsequent to our review and discussions with management, we noted that 47 users had in fact had their roles revoked or accounts blocked. For the remaining 18 users, we confirmed that no inappropriate activity was performed by any of these users for the period under review.

Impact

Lack of effective controls over system access can potentially expose the County to an increased risk of unauthorized access to transactions and data in the eCAPS system.

Recommendation

We recommend that appropriate individuals perform a review to validate active user IDs in eCAPS that belong to terminated County employees are removed. Based on the results of the review, management should undertake appropriate steps to remove eCAPS user IDs that belong to terminated employees and implement monitoring controls to validate user IDs related to terminated employees are removed.

Management Response

We concur with the intent of the recommendation.

The roles for the 18 employees terminated from County service were inquiry or data entry only. In addition, employees who have left County service have their access to the County's Network Enterprise removed and, thus, are outside the County's firewall.

We are currently in the process of developing an interface between the CWTAPPS and eCAPS to identify any employees who have left County service and still have active roles in eCAPS.

(5) Logical Access Controls over CWTAPPS – Granting User Access Rights

Observation

We noted that the County is not enforcing the policies and procedures for the management of users and user access rights within the CWTAPPS application. A review of the 'CWTAPPS User Enrollment Form'



documents for each of the sampled employees and the 'CWTAPPS Signature Authorization Form – System Access' documents for the Authorized Signatories on the 'CWTAPPS User Enrollment Form' revealed the following exceptions:

- 1) For one employee, the 'CWTAPPS User Enrollment Form' access was signed by the user's manager who is not an Authorized Signatory.
- 2) For two user's, the 'CWTAPPS User Enrollment Forms' were approved by an individual who was not yet an Authorized Signatory or the Authorized Signatory list had not yet been updated.

Impact

Weak logical access controls increase the risk of unauthorized users obtaining access to application and data, and modifying or disclosing them inappropriately.

Recommendation

We recommend that appropriate individuals perform a review to validate the CWTAPPS' Authorized Signatories are appropriate and effective means of communications are put in place so that the security administrators that assign the access rights are aware of the Authorized Signatories.

Management Response

We concur with the recommendation.

The policies and procedures for managing user access to CWTAPPS are strictly enforced. Our policies require proper documents to have appropriate signatures prior to granting access to requestors.

Each department has designated employees who are authorized by their department head to sign CWTAPPS access forms. Signature authorization forms are kept on file and signatures on access forms are compared to the signatures of authorized signers to ensure the access forms are approved by the appropriate individual.

We have implemented procedures, which require a signature authorization form to be on file at all times. Any misplaced form must be replaced before the processing of any further access forms authorized by that individual.

(6) Controls over the Change Process for eCAPS

Observation

Based on reviews of supporting evidence for a selected sample of eCAPS changes, we noted that documented evidence of testing and sign-offs could not be obtained for 3 samples of eCAPS changes selected.

Impact

Weaknesses in change management compromise system integrity and availability. Once a system is operational, further enhancements are usually required to meet the changing needs of the business. Such changes should be subjected to controls as stringent as those used in the development or implementation of



Board of Supervisors
County of Los Angeles
January 22, 2007
Page 6

a new system. If there is no control over system changes, the benefits originally gained by controlling the systems' implementation are lost as subsequent changes are made.

Testing of changes may reveal specification problems where the system's facilities do not really meet the user's needs or that the system performance is unacceptable. Therefore, the absence of documented evidence and sign-offs for testing of changes for eCAPS increases the risk that changes put through to eCAPS do not meet business requirements.

Recommendation

Adequate change management procedures should be implemented and monitored so that changes to the eCAPS system are made in a controlled manner. We recommend that the organization continue to employ its existing policies and procedures for introducing new changes, prioritizing changes, logging changes, maintaining a segregation of duties over promoting changes to the production environment, maintaining evidence of these elements, and continuing to enhance these policies and procedures as the business environment changes. We also recommend that appropriate personnel periodically review the changes made to eCAPS to verify that all changes are appropriately approved, tested, and authorized for migration.

Management Response

ISD ITS agrees with the recommendation.

ITS will continue to employ our existing policies and procedures, and re-iterate the need for compliance and will periodically review the change management processes.

(7) Controls over the Change Process for eCAPS – Access to Perform Changes in the Production Environment

Observation

Based on our review of security in the UNIX environment on which the eCAPS system runs, we noted that two individuals share the default UNIX 'root' account to perform their change management function of making changes to the Production environment of eCAPS.

Impact

Changes in Production using the shared user account may be unauthorized or inappropriate and can potentially expose the County to an increased risk of compromised system integrity and availability. Shared user accounts makes it difficult to assign accountability for actions associated with use of the shared user account. As such, if an unauthorized Program Change was performed to the eCAPS application, the Program Change would be difficult to audit.

Recommendation

We recommend that all user accounts be assigned to one user and the sharing of user accounts should be prohibited. Users could potentially 'SU' into root. In circumstances where there is business need for the root account, we recommend that management monitor and review the root account activity at least on a monthly basis.



Board of Supervisors
County of Los Angeles
January 22, 2007
Page 7

Management Response

ISD ITS agrees with the recommendation.

ITS will evaluate the options and alternatives that will provide for the management and monitoring of root account activity along with individual accountability.

The preliminary plan will be developed by July 2007 to address:

- Defining and implementing the new 'root' access policies and procedures
- Evaluating and selecting a UNIX auditing software product to assist in logging 'root' activities
- Implementation of the UNIX auditing software product

The comprehensive detailed plan will be completed by August 2007.

(8) Controls over the Change Process for eCAPS Database – Access to Perform Changes in the Production Environment

Observation

Based on our review of security in the Oracle database on which the eCAPS system runs, we noted that four individuals share the default Oracle Database Administrator user account.

Impact

Changes in production using the shared user account may be unauthorized or inappropriate and can potentially expose the County to an increased risk of compromised data integrity and availability. Shared user accounts makes it difficult to assign accountability for actions associated with use of the shared user account. As such, if an unauthorized program change was performed to the underlying database to the eCAPS application, the program change would be difficult to audit.

Recommendation

We recommend, where feasible, that individual Oracle user accounts with an appropriate level of access privileges are created and assigned to appropriate individuals to assign accountability for actions associated with use of the user account. We recognize that in certain environments within Oracle individual user accounts cannot be created. We therefore recommend that management enable the logging feature within Oracle and perform a monthly review of user logs to ensure that inappropriate or unauthorized activity is detected early.

Management Response

ISD ITS agrees with the recommendation.

ITS agrees with the recommendation that individual accounts be created when it is feasible. However, a shared user account is required to provide standardization of installation, patching, and production scripting across all Oracle databases in the data center. ITS agrees to explore the feasibility of the Oracle logging feature in such instances.



For database access outside of installation, patching, and production scripting, separate user accounts will be created for each Oracle Database Administrator as suggested.

The preliminary plan will be developed by July 2007 to address:

- Defining and implementing the new 'Oracle' access policies and procedures
- Evaluating the feasibility and implementation of enabling the Oracle auditing and logging features
- Implementation of individual user accounts for Oracle Database Administration

The comprehensive detailed plan will be completed by August 2007.

(9) Segregation of Duties Conflict – Programmer Access to Migrate Changes into Production

Observation

During our review of logical access to IT resources, application and data, we noted that there is no formal review of Segregation of Duties performed by the County's management. Accordingly, a review of users with access to migrate Natural modules to the CWTAPPS production environment revealed that the four user accounts that have access to migrate changes also have developer access to perform Program Changes directly in the CWTAPPS production environment.

Impact

Access to promote programming changes into production environment is a function performed at the request of the business owner by an individual without developer access to the system. This is to prevent a user from performing unauthorized changes to the production environment and, in turn, compromising the integrity of the organization's systems and data. Without proper Segregation of Duties provisions there is an increased risk for fraud as users have excessive or overriding access to the systems and data.

Recommendation

We recommend that management create a role-based access matrix, which should list, at a minimum, the transactions that should not be grouped together and profiles that should not be assigned together to prevent segregation of duties conflict. This matrix should be reviewed during the creation of profiles, during the assignment of user access, and during the review of user access.

A detailed review should be performed over the validity of all users and their access to the critical systems. This review should be conducted so that only appropriate users have access to the systems and their access is in line with their job responsibilities. In addition, users' access should be reviewed against the access matrix to ensure that user access is in compliance with the County's segregation of duty policies. Compensating controls should be implemented in situations where users may have segregation of duty conflicts, but are required to have the access to perform their jobs. Based on the results of the review, management should undertake appropriate steps to mitigate segregation of duties conflicts and make the necessary adjustments to such systems that impact the financial reporting process.

Management Response

ISD ITS agrees with the recommendation.



ITS will develop a role-based access matrix in conjunction with the Auditor-Controller that identifies the transactions and profiles that should not be assigned together in order to prevent segregation of duties of conflicts for financial applications. The matrix will be reviewed by ISD Applications and Production Control staff along with the Auditor-Controller Systems staff responsible for CWTAPPS.

(10) Controls over the Tape Restoration Process

Observation

During our review, we noted that while the County is in the process of implementing a new process for data storage, the County's business recovery testing consists of loading tapes and testing the restoration for a minimal number of production applications. The IBM recovery center testing is conducted over four (4) days each year by the County's Internal Services Department. Most of this time is taken up with tape recoveries. As such, many of the County's critical applications could remain untested over an extended period of time and the data related to those applications may not be able to be restored in an event of an actual disaster.

Impact

The purpose of a restoration test is to validate the data saved onto backup media and stored offsite is recoverable in the event of an actual disaster. Without a periodic test of the restoration process, the County increases its risk of not being able to restore its data that was previously backed up onto tape media where information cannot be restored in the event of an actual disaster where financial information is lost.

Recommendation

We recommend that the County implement a test over the restoration of backed up data from tape media for all applications that has a financial impact on the organization on an annual basis.

Management Response

ISD ITS agrees with the recommendation.

ITS's disaster recovery process is based on disk replication technology. In August 2006, two major disaster recovery tests were performed. The first test from July 31, 2006 to August 11, 2006 was a complete disk recovery of the IBM mainframe data where the CWTAPPS and CWPAY applications performed a successful recovery test. Later in August, 2006 a recovery test for the eCAPS Financial midrange data was also successfully completed. To ensure disaster recovery processes are in effect, testing will be scheduled at least annually for both platforms.

(11) Physical Security Controls over the Data Center

Observation

We reviewed the physical security controls over the County's data center in Downey. Our review of user groups with access rights to the Downey Data Center's Tape Library Room revealed that thirty-three (33) user groups have access to the backup tapes stored on-site. Review of the user groups revealed that access to the on-site storage facilities was not restricted appropriately.



Board of Supervisors
County of Los Angeles
January 22, 2007
Page 10

Impact

Poor physical access controls to the County's data center could lead to unauthorized access and consequent damage, theft or misuse of the County information system resources. Access to the computer room should be safeguarded to reduce the risk of destruction of valuable hardware, software or critical data files.

Recommendation

We recommend that the appropriate individuals review the list of user groups and the users assigned to each user group and, based on the review, remove the inappropriate user groups and individuals. In addition, the user groups and individuals assigned to each user group should be reviewed on a periodic basis to reduce the risk of unauthorized access to the County's data center, and the Downey Data Center's Tape Library Room that is within it.

Management Response

ISD ITS agrees with the recommendation.

Operations will continue to perform a regular review and updating of Data Center access lists.

(12) Access Controls over the Ability to Recall the County of Los Angeles' Backed up Data from its Off-Site Storage Vendor's Facilities

Observation

During our review of those users with access to request backup data tapes from recall, the third-party off-site storage vendor, revealed that user access to request backup media stored off-site was not restricted appropriately. We observed two terminated employees had access to recall backup media from Recall.

Impact

The off-site storage of data that has been backed up onto tape media is essential for safeguarding an organization's data. If the data backed up onto tape media is not stored offsite and there happens to be a disaster that affects the data center, then the backup tapes would be subject to the same disaster that affected the data center. As such, the backup tapes may no longer be available to restore data and resume operations. Poor access controls over the County's data that has been backed up onto tape media also compromises the security that was intended to be achieved by storing the data off-site. Inappropriate access to the data that has been stored off-site could lead to theft or misuse of the County's information system resources in an attempt to conceal fraud or to sabotage the organization's ability to resume operations.

Recommendation

We recommend that the appropriate individuals perform a review of the list of users with access to recall the backup tapes from the off-site storage vendor's facilities. Based on the review the access right to recall the backup tapes should be revoked for inappropriate individuals. The review should also be performed to reduce the number of individuals with access to recall backup tapes to a minimum.

Management Response

ISD ITS agrees with the recommendation.



Operations will continue to perform a regular review and updating of the list of authorized users, while reducing the number of users to a minimum.

(13) Lack of Confidentiality Forms for Internet Users

Observation

All employees with Internet access need to have an approved confidentiality form. We requested a copy of the confidentiality forms for a sample of employees. Of the 60 employees sampled, management was unable to provide 11 required confidentiality forms.

Impact

Information and Communication is an essential element for effective internal controls. If Information and Communication is weak within an organization, and evidence of internal controls being in place is difficult to obtain or not maintained, the perception over the relevance and importance of the internal control could be undermined. In turn, weak Information and Communication could have a viral affect on the organization, weakening other elements of internal controls: Control Activities, Monitoring, Risk Assessment, and Control Environment.

Recommendation

We recommend that the County establish effective means of maintaining evidence related to the effectiveness of the organization's internal controls.

Management Response

ISD ITS agrees with this recommendation.

ITS requires that all registered Internet users sign an "Agreement for Acceptable Use and Confidentiality..." form. The forms are then kept on file. To correct the problem of missing forms for individuals with Internet access, ITS will send forms to these individuals for completion. Once completed and signed, the forms will be maintained on file. This activity will be completed by May 31, 2007. Additionally, ITS will review its current process for maintaining confidentiality forms and evaluate the need to inventory forms for all ITS registered Internet users. This review and evaluation, along with a list of resulting action items, will be completed by July 2007.

(14) Lack of Evidence for Access to the User Maintenance Screen

Observation

To validate access to the User Maintenance screen is restricted appropriately, we requested evidence of approval to submit new and modified user access requests via the User Maintenance screen. The approval for six of the employees could not be confirmed. Documented evidence is not maintained..

Impact

Information and Communication is an essential element for effective internal controls. If Information and Communication is weak within an organization, and evidence of internal controls being in place is difficult to obtain or not maintained, the perception over the relevance and importance of the internal control could be undermined. In turn, weak Information and Communication could have a viral affect on the



Board of Supervisors
County of Los Angeles
January 22, 2007
Page 12

organization, weakening other elements of internal controls: Control Activities, Monitoring, Risk Assessment, and Control Environment.

Recommendation

We recommend that the County establish effective means of maintaining evidence related to the effectiveness of the organization's internal controls.

Management Response

KPMG was informed that most employees were given access to eCAPS before the User Maintenance screen was even implemented. Secondly, the User Maintenance screen is just an online screen, and there is no paper trail required. Security coordinators in each department are authorized to request access to eCAPS for employees and submit them to the eCAPS Security Administrators for approval. This process is done in accordance with the County's Internal Control Plan.

In addition, we identified certain deficiencies in internal control that we consider to be reportable conditions or material weaknesses and communicated them in writing to management and those charged with governance on January 22, 2007.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the County's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of management, others within the organization, and the Board of Supervisors and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP