COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

MARIA M. OMS
CHIEF DEPUTY

ASST. AUDITOR-CONTROLLERS

ROBERT A. DAVIS
JOHN NAIMO
JUDI E. THOMAS

January 31, 2011

TO: Supervisor Michael D. Antonovich, Mayor
Supervisor Gloria Molina
Supervisor Mark Ridley-Thomas
Supervisor Zev Yaroslavsky
Supervisor Don Knabe

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **REVIEW OF THE COUNTY'S RISK MANAGEMENT AND CLAIMS ADMINISTRATION INFORMATION SYSTEM (RMIS)**

As part of our ongoing responsibility to ensure that County resources are safeguarded and that County departments comply with County fiscal policies and procedures, we reviewed the County's procedures and controls over the Risk Management and Claims Administration Information System (RMIS or System) payment processing. Our review included determining if controls were adequate to ensure only valid and authorized payments were made.

The Chief Executive Office (CEO), County Counsel and two contracted Third-Party Administrators (TPAs) use RMIS to manage and pay medical malpractice, vehicle damage, general liability and other claims filed against the County. In Fiscal Year (FY) 2009-2010, the CEO, County Counsel and TPAs authorized over $93 million in liability claim payments through RMIS.

As joint program directors, the CEO and County Counsel are both responsible for RMIS maintenance and upgrades, and for approving and executing work orders for changes to the System. However, because each department handles unique claims, administers its own System access, and applies separate System procedures and processes, this report includes independent findings and recommendations for each department. CEO and County Counsel management generally agree with our findings and recommendations. Their response is attached.

Results of Review

The CEO and County Counsel have appropriately established certain system controls such as system timeouts, and restricting users from entering and approving the same payments. However, the CEO and County Counsel need to strengthen controls over other areas of RMIS payment processing. Specifically:

- CEO and County Counsel need to restrict System access, as required by County Fiscal Manual (CFM) Section 8.6.4, to ensure the integrity of the System data. We noted instances where contract (non-County) employees and County staff have inappropriate access to System information or lack separation of duties, which increases the risk of error, fraud or other inappropriate activity. For example:

    - Contract employees responsible for program design and System maintenance are also responsible for assigning and changing users' System access, and can modify the payment file sent to eCAPS, create claims, add payees, and enter, approve and cancel payments.

    - County employees have the ability to process payments and establish vendors in the System, which should be separated, or have RMIS payment approval capabilities for which they do not qualify or need for their work.

    - All RMIS users, including contract, County and TPA staff can view confidential information (e.g., social security numbers), but their responsibilities have not been reviewed to ensure this access is required for their assigned tasks.

  CEO and County Counsel Response – The attached response indicates that they have removed the contractor's responsibility for assigning and changing user access and resolved the County employees' access conflicts.

  CEO and County Counsel also indicated that restricting RMIS access to confidential information would require a System enhancement and will weigh the costs and benefits of enhancing the System. They indicated that as a compensating control, all RMIS users agree to abide by the terms of their confidentiality policy by clicking "I Agree" when logging into RMIS.

- CEO and County Counsel need to ensure all RMIS user IDs are assigned to specific individuals to establish an audit trail and maintain user accountability. We noted 14 generic System user IDs, including ten IDs that have administrative capabilities described above, that are not assigned to specific employees. As a

result, there is no record of who used these IDs. Contract employees use one of these IDs to assign and change System access.

CEO and County Counsel Response – The attached response indicates that all generic accounts have been deactivated.

- CEO needs to establish policies defining the staff levels and duties for each System access role and create separate System roles for each approval level. We noted managers assign access to staff by copying other users' access profiles and do not always ensure the access requested is necessary or appropriate, which can lead to inappropriate access of information and increases the risk of errors. Also, the CEO's lower-level and higher-level RMIS approval capabilities are grouped into one System access role, which resulted in lower-level System approvers having more access than they need.

  CEO response – The attached response indicates that the CEO is updating the Internal Control Plan to strengthen System access roles.

- CEO needs to develop written procedures for adding, changing and disabling RMIS access, and ensure staff obtain proper documentation and approvals for access role assignments and changes. Thirteen (65%) of the 20 users we reviewed had access that either was not authorized by the appropriate manager or did not have written authorization for their access.

  CEO Response – The attached response indicates that procedures have been updated to ensure user access approvals are documented in the RMIS Help Desk System.

- CEO needs to remind staff not to share System access and ensure System access is cancelled when employees leave. We observed a CEO payment approver give their user ID and password to a data entry clerk, and noted two other instances where County staff used former employees' System access. We also noted that 30 County and TPA employees who left the department or TPA up to seven years ago, still have RMIS access.

  CEO Response – The attached response indicates that the CEO will remind users not to share System IDs and passwords and has already disabled terminated employees' and inactive users' System access.

- CEO needs to change their RMIS payment approval limits to ensure TPAs do not exceed their delegated payment authority. We noted that RMIS allows the two TPAs to issue payments without CEO approval for up to $50,000 and $25,000 respectively, instead of the $20,000 and $10,000 limits in the claims and management services contracts between the TPAs and the CEO. From July

2008 through September 2009, TPAs did not obtain CEO approval for approximately half the payments they issued over their delegated authority, totaling $5.8 million.

CEO Response – The attached response indicates that on January 25, 2010, the CEO modified RMIS so that all payments, regardless of dollar amount, require a final County approval in eCAPS.

- CEO should work with the TPAs to evaluate scanning and electronically attaching source documents to payments in RMIS. We noted that TPAs photocopy payment source documents and mail the hard copy documents to the CEO for processing. To make the process more efficient, TPAs can expedite the payment process and reduce paper and postage costs by scanning and electronically attaching these documents to payments in the System for the CEO to process.

  CEO Response – The attached response indicates that the CEO is currently reviewing this recommendation.

- CEO and County Counsel need to increase payment efficiency and establish separation of duties by having the Auditor-Controller Disbursements Division (Disbursements) mail RMIS warrants. We noted that Disbursements generates the RMIS warrants. At the request of the CEO and County Counsel, Disbursements staff would pull and hold the warrants for the CEO and County Counsel to pick up, instead of Disbursements mailing the warrants directly to the payees. CEO staff then log and overnight mail the warrants to the TPAs, and County Counsel staff distribute their warrants to the lead attorney for each case. We also noted that staff handling these warrants have conflicting payment processing responsibilities, such as reviewing and approving payments and entering payments in RMIS.

  Although some payments require hand delivery as ordered by the courts, for all other payments the lengthy warrant handling and distribution process described above results in payment delays and increases the risk of lost and/or inappropriately cashed payments.

  CEO Response – The attached response indicates that the CEO is currently reviewing restricting warrant access to staff with no payment processing capabilities. CEO also indicated that they are discussing various options to have payments mailed by the Auditor-Controller Disbursements Division.

  County Counsel Response – The attached response indicates that County Counsel has restricted warrant access to staff who do not have payment processing capabilities. County Counsel also indicated that most of their

payments are already mailed by the Auditor-Controller Disbursements Division and that, when special handling is not required, all other payments will also be mailed by the Auditor-Controller Disbursements Division.

We also noted CEO and County Counsel need to formally monitor administrative user activity and strengthen System password controls by discontinuing the practice of allowing the use of expired passwords to access the System. In addition, the CEO and County Counsel need to accurately complete their annual Internal Control Certification Program. Further, the CEO needs to ensure TPA staff obtain all documentation before entering payments in RMIS and that payment requests agree with the documentation before applying System approvals.

While our review of a sample of payments did not disclose any invalid payments, the weaknesses noted in this report are serious and, if not corrected, could allow inappropriate payments to occur without being detected. Details of our findings and recommendations are attached.

Acknowledgement

We discussed our report with CEO and County Counsel management who generally agree with our findings and recommendations. Both departments' responses are attached.

We thank CEO and County Counsel management and staff for their cooperation and assistance during our review. Please call me if you have any questions, or your staff may contact Jim Schneiderman at (213) 253-0101.

WLW:MMO:JLS:MP

Attachments

c: William T Fujioka, Chief Executive Officer
Andrea Sheridan Ordin, County Counsel
Public Information Office
Audit Committee

CHIEF EXECUTIVE OFFICE AND COUNTY COUNSEL REVIEW OF RISK MANAGEMENT AND CLAIMS ADMINISTRATION INFORMATION SYSTEM

Background

The Chief Executive Office (CEO), County Counsel and two contracted Third-Party Administrators (TPAs) use the Risk Management and Claims Administration Information System (RMIS or System) to manage and pay medical malpractice, vehicle damage, general liability and other claims filed against the County. County and TPA personnel record claim information in RMIS and, once approved, payment requests are sent electronically to the County's eCAPS enterprise accounting system (eCAPS) to pay the claims. In fiscal year (FY) 2009-10, the CEO, County Counsel and TPAs authorized over $93 million in liability claim payments through RMIS.

As joint program directors, the CEO and County Counsel are both responsible for all RMIS maintenance and upgrades, and for approving and executing work orders for changes to the System. However, because each department handles unique claims, administers its own System access, and applies separate System procedures, this report includes independent findings and recommendations for each department.

Access Controls

County Fiscal Manual (CFM) Section 8.6.4 requires departments to limit system access based on each user's responsibilities. Administrative access, such as the ability to setup or change a user's access, should be limited to key individuals and closely monitored. Departments should also periodically review user access to ensure it is authorized and appropriate. These controls ensure the integrity of the System data.

We noted instances where contract (non-County) employees and County staff have inappropriate access to System information or lack separation of duties, which increases the risk of error, fraud or other inappropriate activity. For example:

- Four contract employees, who are responsible for program design and system maintenance also have the ability to give and change CEO and TPA users' System access, create claims, add payees, and enter, approve and cancel payments. They and other staff in the contractor's headquarters can also modify information in the payment file sent to eCAPS.

- A total of 14 CEO and County Counsel staff have the ability to process payments and establish vendors in the System which should be separated, or have RMIS payment approval capabilities for which do they do not qualify or need for their work.

- Thirty County and TPA employees, who left the department or TPA up to seven years ago, still have RMIS access and should be removed to prevent

unauthorized activity. In two cases, current County staff continue to use the terminated employees' access to monitor claims and adjust the amount to be paid on claims.

- Eleven County employees have active RMIS access that they do not use. Seven of the employees have had access for over five years and have never used it, and the other four employees were assigned new user IDs, but the old IDs were not cancelled.

We also noted that all 479 RMIS users, including 195 users with inquiry only access, can view confidential claimant information, such as social security numbers and other personally identifiable information. To protect claimant information and reduce the risk of identity theft, CEO and County Counsel should review all System user responsibilities to ensure staff need this information for their assigned tasks.

We noted the following issues that contribute to the lack of access controls:

- CEO does not have policies defining the staff levels and duties for each System access role to limit access, including access to confidential information, based on each user's responsibility. We noted managers assign access to staff by copying other users' access profiles, and do not always ensure the access is appropriate. Also, the CEO's lower-level and higher-level RMIS approval capabilities are grouped into one System access role, which resulted in lower-lever System approvers having more approval capability than they need.

- CEO does not have written procedures for adding, changing and disabling RMIS access, and staff do not always obtain proper documentation or approval for access role assignments and changes. We noted 13 (65%) of the 20 users we reviewed had access that either was not authorized by the appropriate manager, or did not have written authorization for their access.

- CEO and County Counsel do not formally monitor administrative user activity, such as setting up or changing a user's System access, as required by CFM Section 8.6.4. We noted the CEO and County Counsel could not document that they monitor the 17 user identifications (IDs) with administrative capabilities, to ensure user activity is appropriate.

- CEO and County Counsel do not ensure RMIS user IDs are specific to each individual. We noted 14 generic System user IDs, including ten with administrative capabilities as described above, that are not assigned to specific employees. As a result, there is no record of who used these IDs. Contract employees use one of these IDs to assign and change System access.

- CEO, TPA and County Counsel management do not review System access regularly to ensure assignments and changes are appropriate and authorized.

- RMIS users share System credentials. We observed a CEO payment approver give their user ID and password to a data entry clerk, and, as previously mentioned, County staff use terminated users' access.

- RMIS prompts users to change their passwords every 90 days, but it does not prevent staff from using the expired password.

While our review of a sample of payments did not disclose any invalid payments, the weaknesses noted in the System could allow inappropriate payments to occur without being detected. To strengthen access controls and limit System access based on each user's responsibilities, CEO and County Counsel management should implement the following recommendations.

Recommendations

CEO and County Counsel management:

1. **Limit System access by:**

   a. **Restricting administrative access, including the ability to assign and change users' access, to a few key individuals who are independent of program design and System maintenance and support, and regularly monitor their activity.**

   b. **Removing conflicting payment and vendor processing access or payment approval capabilities that they do not qualify for or need for their work.**

   c. **Reviewing System user responsibilities to ensure staff with access to confidential information need it for their work.**

2. **Ensure RMIS user identifications are assigned to specific individuals to establish accountability and provide an audit trail over user activity.**

3. **Review System access regularly to ensure access assignments and changes are appropriate and authorized.**

4. **Ensure RMIS prevents staff from using expired passwords.**

CEO management:

5. **Establish policies defining the staff levels and duties for each System access role and create separate System roles for each approval level.**

6. **Document procedures for adding, changing and disabling user access, and ensure staff obtain proper documentation and approval for access role assignments and changes.**

7. **Remind users not to share System credentials.**

8. **Cancel terminated employees' and inactive users' System access and, in the future, ensure System access is cancelled when employees leave.**

9. **Ensure staff using the terminated employee's access are assigned proper access, if needed, and evaluate the appropriateness of the activity performed using the terminated employee's access.**

Payment Review and Approval

CFM Section 4.5.5 requires payments to be reviewed and approved by people independent of the data entry function. The CEO must also review and approve all payments in excess of the TPAs' delegated payment authority.

We reviewed payment procedures at CEO, County Counsel and both TPAs, and noted the following TPA control weaknesses:

- TPA staff who approve payments in RMIS do not always review source documents to ensure the payments are valid and properly supported. Although other TPA personnel manually review and approve claims outside of the System, RMIS payment approvers do not always review this documentation.

- TPA personnel who manually review and approve claims also enter the claims in RMIS in violation of their payment internal control policy.

- RMIS allows TPAs to issue payments without CEO approval for up to $50,000 and $25,000, instead of the $20,000 and $10,000 limits as in the claims and management services contracts between TPAs and the CEO. From July 2008 through September 2009, TPAs did not obtain CEO approval for approximately half the payments they issued over their delegated authority, totaling $5.8 million.

- TPA staff do not consistently obtain Release and Settlement Agreements confirming that claimants agree with judgments and settlements before processing payments in RMIS. Although some payments require special handling as ordered by the courts, TPA staff should obtain claimant Release and Settlement Agreements for all other judgments and settlements to ensure they are correct and agreed upon before processing payments in RMIS.

We also noted that TPAs copy payment source documents and mail them to the CEO. However, TPAs can expedite the payment process, and reduce paper and postage costs by scanning and electronically attaching these documents to payments in RMIS.

While our review of a sample of payments did not disclose any invalid payments, the weaknesses noted above could allow inappropriate payments to occur without being detected. CEO should implement the following recommendations.

Recommendations

CEO management:

10. **Ensure TPA staff verify payments are valid and properly supported with source documents before applying System approvals.**

11. **Ensure TPA staff that manually review and approve payments are independent of the RMIS data entry function.**

12. **Change the RMIS payment approval limits to ensure TPAs do not exceed their delegated payment authority.**

13. **Work with TPAs to evaluate scanning and electronically attaching source documents to RMIS payments.**

14. **Ensure TPA staff obtain claimant Release and Settlement Agreements for judgments and settlements that do not require special handling before processing payments in RMIS.**

Warrant Processing

The Auditor-Controller Disbursements Division generates RMIS warrants. At the request of the CEO and County Counsel, Disbursements staff then pull and hold the warrants for the CEO and County Counsel to pick up, instead of Disbursements mailing the warrants directly to the payees. CEO staff then log and overnight mail the warrants to the TPAs, and County Counsel staff distribute their warrants to the lead attorney for each case. This process is inefficient, lacks proper separation of duties and increases the risk for inappropriate payments. For example:

- CEO, County Counsel and TPA staff responsible for handling warrants have conflicting payment processing responsibilities and capabilities, such as reviewing and approving payments and entering payments in RMIS.

- TPA staff use physical warrants to record the warrant information on case documents, but RMIS already has the warrant information they need.

- TPA staff sometimes hold warrants until claimants sign Release and Settlement Agreements, indicating they agree with the settlement. As mentioned in the Payment Review section above, staff should obtain Release and Settlement Agreements for judgments and settlements that do not require special handling, before processing payments in RMIS.

CEO management also indicated that they have claimants pick-up warrants to avoid mailing high-dollar TPA warrants. However, 80% of RMIS payments are under $10,000 and only 5% are over $50,000. To avoid mailing high-dollar warrants, CEO and County Counsel management should establish dollar-thresholds for payments that must be picked up.

We believe CEO and County Counsel management can increase payment efficiency and strengthen controls over warrant handling and mailing by allowing Disbursements to mail warrants. CEO and County Counsel should establish dollar-threshold for payments that must be picked up, and have Disbursements mail warrants that do not require special handling. CEO and County Counsel management should also restrict warrant access to CEO, TPA and County Counsel individuals with no payment processing capabilities.

Recommendations

CEO and County Counsel management:

15. **Establish dollar-thresholds for payments that must be picked-up and have the Auditor-Controller Disbursements Division mail warrants that do not require special handling.**

16. **Restrict warrant access to CEO, TPA and County Counsel individuals with no payment processing capabilities.**

Internal Control Certification Program

The Auditor-Controller developed the Internal Control Certification Program (ICCP) to assist County departmental managers in evaluating and improving internal controls in all fiscal areas, to reduce the risk of error, fraud and other improper activities. Under the ICCP, County departments are required to annually (or biennially) review and evaluate controls in key areas and certify that the proper controls are in place or note that action is being taken to correct any deficiencies or weaknesses noted.

The non-compliances noted in our review of the RMIS payment process should have been detected when completing the ICCP. However, CEO's and County Counsel's most recent certification indicates that the appropriate controls were in place.

To help CEO and County Counsel managers evaluate and improve internal controls, management should ensure that qualified staff independent of the function for all applicable assessable units, accurately complete the ICCP questionnaires.

Recommendation

17. **CEO and County Counsel management ensure that qualified staff independent of the function for all applicable assessable units, accurately complete the Internal Control Certification Program.**

ATTACHMENT

County of Los Angeles
CHIEF EXECUTIVE OFFICE
Kenneth Hahn Hall of Administration
500 West Temple Street, Room 713, Los Angeles, California 90012
(213) 974-1101
http://ceo.lacounty.gov

WILLIAM T FUJIOKA
Chief Executive Officer

Board of Supervisors
GLORIA MOLINA
First District

MARK RIDLEY-THOMAS
Second District

ZEV YAROSLAVSKY
Third District

DON KNABE
Fourth District

MICHAEL D. ANTONOVICH
Fifth District

November 3, 2010

To: Wendy L. Watanabe
Auditor-Controller

From: William T Fujioka
Chief Executive Officer

Andrea Sheridan Ordin
County Counsel

REVIEW OF THE RISK MANAGEMENT AND CLAIMS ADMINISTRATION INFORMATION SYSTEM

Attached is our response to the recommendations made in your review of the Risk Management and Claims Administration Information System. We appreciate the cooperation extended to us by your department through the review process. As a result of the interaction between Auditor-Controller and departmental staff, CEO and County Counsel have been able to implement resolutions to deficiencies identified during the course of the review.

If you have any questions or require additional information, please let me know or you may contact Laurie Milhiser, County Risk Manager, at (213) 351-5346, or John Krattli, Senior Assistant County Counsel, at (213) 974-1838.

WTF:ASO:ES
LM:SN:RM:sg

Attachment

"To Enrich Lives Through Effective And Caring Service"

Please Conserve Paper – This Document and Copies are Two-Sided
Intra-County Correspondence Sent Electronically Only

Chief Executive Office and County Counsel Response to

Auditor-Controller's Review of Risk Management and Claims Administration Information System

Auditor-Controller Recommendation #1

CEO and County Counsel Management limit System access by:

a. **Restricting administrative access, including the ability to assign/change user's access, to a few key individuals who are independent of program design and System maintenance/support, and regularly monitor their activity.**

b. **Removing conflicting payment and vendor processing access or payment approval capabilities that they do not qualify for or need for their work.**

c. **Reviewing System user responsibilities to ensure staff with access to confidential information need it for their work.**

CEO and County Counsel Management's Response:

a. The CEO and County Counsel have each restricted administrative access to three security administrators on their respective staffs who assign/change user access. To further restrict administrative access, effective August 25, 2010, all generic user accounts with administrative access were de-activated.

   Risk Technologies Inc. (RTI), as the developers of RMIS, will continue to have system administrator access solely for the purposes of troubleshooting and fixing issues found in the production environment.

   As part of the CEO's and County Counsel's formal periodic review processes, user responsibility, activity, and appropriateness will be further monitored using additional System audit reports currently under development. Forms and approval processes are being developed. *Status: in progress*

b. In accordance with the CEO Internal Control Plan, all established users administered by CEO are now in compliance with this policy. All users do not have both conflicting payment and vendor processing rights. In addition, all CEO users, who were identified with payment approval capabilities that were not needed for their work, had the rights removed. *Status: implemented August 2010*

   In 2008, County Counsel established controls and procedures to separate the payment and vendor processing functions. To further enhance these controls, access to the payment and vendor entry functions has been restricted. The

user roles of staff identified as having conflicting access were modified on September 9, 2010, to remove the conflicting role. The role identified as causing the conflict, Role 402, was removed. *Status: implemented September 2010*

c. As part of the CEO's formal periodic review process, user responsibility, activity and appropriateness will be further monitored using additional system audit reports. *Status: in progress*

County Counsel users are regularly reviewed for status (e.g., terminated, retired, transferred, position/role change) and user responsibilities to ensure that access is commensurate with user responsibilities. User profiles are updated accordingly. Updates are also applied as a result of County Counsel's Annual RMIS user profile review process. *Status: implemented 2007*

RMIS is a confidential database with attorney-client work-product and other privileged information. CEO and County Counsel both agree that users approved for RMIS access need access to confidential information contained within the system. All users agree to abide by the terms of the confidentiality notice by logging into RMIS and clicking 'I AGREE'. *Status: implemented 2006*

Restricting access to personally identifiable information would require a work order to be issued to the contractor to modify the system. The benefits of such an enhancement would need to be weighed against the added cost for such work order. *Status: in progress*

Auditor-Controller Recommendation #2

CEO and County Counsel Management ensure RMIS user identifications are assigned to specific individuals to establish accountability and provide an audit trail over user activity:

CEO and County Counsel Management's Response:

All generic user accounts administered by CEO and County Counsel were deactivated on August 25, 2010. *Status: implemented August 2010*

Auditor-Controller Recommendation #3

CEO and County Counsel Management review System access regularly to ensure access assignments and changes are appropriate and authorized:

CEO and County Counsel Management's Response:

As part of CEO's formal periodic review process, user access and appropriateness will be reviewed and the completion of the signature page will be required. *Status: in progress*

County Counsel users are regularly reviewed for status (e.g., terminated, retired, transferred, position/role change) and user responsibilities to ensure that access is commensurate with user responsibilities. User profiles are updated accordingly. Updates are also applied as a result of County Counsel's Annual RMIS user profile review process. County Counsel will regularly review the status of all County Counsel staff to ensure that profiles are properly updated. *Status: implemented 2007*

Auditor-Controller Recommendation #4

CEO and County Counsel Management ensure RMIS prevents staff from using expired passwords:

CEO and County Counsel Management's Response:

The password expiration control was implemented system wide in February 2010. *Status: completed*

Auditor-Controller Recommendation #5

CEO Management establish policies defining the staff levels/duties for each System access role and create separate System roles for each approval level:

CEO Management's Response:

CEO Risk Management is updating the Internal Control Plan (ICP) to strengthen System access roles. *Status: in progress*

Auditor-Controller Recommendation #6

CEO Management document procedures for adding, changing and disabling user access, and ensure staff obtain proper documentation and approval for access role assignments/changes:

CEO Management's Response:

Existing procedures have been updated to ensure all user access approvals are documented in the RMIS Help Desk System (Altiris). All RMIS Help Desk System incidents shall be reviewed by the security administrators before closing the ticket. *Status: implemented March 2010*

Auditor-Controller Recommendation #7

CEO Management remind users not to share System credentials:

CEO Management's Response:

This practice violates department security policies. As part of the CEO formal periodic review process, users will be reminded not to share System credentials and department administrators will be required to certify that their users have been educated not to share System credentials. *Status: in progress*

Auditor-Controller Recommendation #8

CEO Management cancel terminated employees' and inactive users' System access and, in the future, ensure System access is cancelled when employees leave:

CEO Management's Response:

All users administered by CEO have been reviewed for status (e.g., terminated, retired, transferred, position/role change) and disabled accordingly. *Status: implemented March 2010*

Auditor-Controller Recommendation #9

CEO Management ensure staff using the terminated employees' access are assigned proper access, if needed, and evaluate the appropriateness of the activity performed using the terminated employees' access:

CEO Management's Response:

All users administered by CEO have been reviewed for status and appropriateness. Users that were found violating department security policies by using a terminated employee's access have been required to go through the entire registration and approval process to establish access to the System. *Status: implemented March 2010*

Auditor-Controller Recommendation #10

CEO Management ensure TPA staff verify payments are valid and properly supported with source/originating documents before applying System approvals:

CEO Management's Response:

CEO Risk Management is working with TPA management to develop procedures to ensure payments are verified and supported with the necessary documentation before applying System approvals. *Status: in progress*

Auditor-Controller Recommendation #11

CEO Management ensure TPA staff that manually review/approve payments are independent of the RMIS data entry function:

CEO Management's Response:

CEO Risk Management is currently working with TPA management to develop procedures to ensure separation of duties. *Status: in progress*

Auditor-Controller Recommendation #12

CEO Management change the RMIS payment approval limits to ensure TPAs do not exceed their delegated payment authority:

CEO Management's Response:

Effective January 25, 2010, RMIS was modified so that Final Approvals of all payments (regardless of dollar amounts) must be applied in eCAPS by the County. *Status: implemented January 2010*

Auditor-Controller Recommendation #13

CEO Management work with TPA's to evaluate scanning and electronically attaching source/originating documents to RMIS payments:

CEO Management's Response:

CEO Risk Management is currently reviewing this recommendation.

Auditor-Controller Recommendation #14

CEO Management ensure TPA staff obtain claimant Release and Settlement Agreements for judgments/settlements that do not require special handling, before processing payments in RMIS:

CEO and County Counsel Management's Response:

CEO Risk Management is working with the TPAs to develop procedures to ensure claimant release forms are being obtained before processing payments in RMIS.

Auditor-Controller Recommendation #15

CEO and County Counsel Management establish dollar-thresholds for payments that must be picked-up and have the Auditor-Controller Disbursements Division mail warrants that do not require special handling:

CEO and County Counsel Management's Response:

CEO Risk Management is in the process of identifying payments and discussing the various options to mail the payments through the Auditor-Controller Disbursements Division. *Status: in progress*

A significant number, approximately 75 percent, of County Counsel's payments are mailed by the Auditor-Controller Disbursements Division. Over the past three years, the County Counsel's Office has made a concerted effort to ensure that payments, which can be mailed, are mailed.

Some payments are very time sensitive and cannot be mailed. Some payments need to be hand-delivered by the attorney. The need for special handling is not based on the dollar amount of a payment. The attorney and the attorney's Division Chief requesting the payment are the persons best equipped to determine when a particular payment requires special handling. When special handling is not required, County Counsel will mail the payments through the Auditor-Controller Disbursements Division.

Auditor-Controller Recommendation #16

CEO and County Counsel Management restrict warrant access to CEO, TPA and County Counsel individuals with no payment processing capabilities:

CEO and County Counsel Management's Response:

CEO Risk Management is currently reviewing this recommendation.

County Counsel agrees with this recommendation and has restricted warrant access to individuals who do not have payment processing capabilities. On September 9, 2010, the user profile of the County Counsel staff member who had physical access to warrants was modified to remove Role 402. Role 402 was identified by Audit staff as having a conflict with warrant handling functions. *Status: implemented September 2010*

Auditor-Controller Recommendation #17

CEO and County Counsel Management ensure that qualified staff independent of the function for all applicable assessable units, accurately complete the Internal Control Certification Program:

CEO and County Counsel Management's Response:

CEO has completed its FY 2009-2010 ICCP review for RMIS and will continue the ICCP review of RMIS on an annual basis. CEO Management will ensure that qualified staff independent of the function for all applicable assessable units, accurately completes the department's ICCP review. *Status: in progress*

County Counsel agrees with this recommendation and County Counsel Management will ensure that qualified staff independent of the function for all applicable assessable units, accurately completes the department's next ICCP review. *Status: in progress*