



INTERNAL AUDIT DEPARTMENT
COUNTY OF ORANGE

*Integrity
Objectivity
Independence*

**Integrated
Internal Control Review
of the
Auditor-Controller Accounts Receivable
and Collection
Processes – IT Results

As of December 31, 2004**

AUDIT NO. 2428-B

REPORT DATE: AUGUST 11, 2005

Audit Director:	Peter Hughes, Ph.D., CPA, CITP
Deputy Director:	Eli Littner, CPA, CIA, CISA
Audit Manager:	Michael Goodwin, CPA, CIA
IT Audit Manager:	Autumn McKinney, CPA, CIA
In-Charge Auditor:	Nancy Ishida, CPA, CIA
In-Charge IT Auditor:	Scott Suzuki, CPA, CIA, CISA
Senior Internal Auditor:	Ken Wong, CPA, CIA

**Integrated Internal Control Review
of the Auditor-Controller
Accounts Receivable and Collection Processes – IT Results**

As of December 31, 2004

TABLE OF CONTENTS

Transmittal Letter	i
INTERNAL AUDITOR’S REPORT	1
EXECUTIVE SUMMARY	3
OBJECTIVES	3
BACKGROUND	3
SCOPE	4
CONCLUSION	5
DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES	6
Logical Access	6
Security Monitoring	8
Security Related Personnel Practices and User Account Management	8
Business Continuity Management – IT Division	9
Physical Security	11
Business Continuity Plan – Accounts Receivable and Collections	12
Security Program Planning & Management	13
Information Resource Classification	14
Software Development Methodology	15
Application Security	16
Data Validation Features	16
ATTACHMENT A: Report Item Classifications	18
ATTACHMENT B: Auditor-Controller Management Responses	19
ATTACHMENT C: Internal Audit Comment	30



COUNTY OF ORANGE
INTERNAL AUDIT DEPARTMENT

Integrity ♦ Objectivity ♦ Independence

ELI LITTNER
CPA, CIA, CFE, CFS CISA
DEPUTY DIRECTOR

MICHAEL GOODWIN
CPA, CIA
AUDIT MANAGER

ALAN MARCUM
MBA, CPA, CIA, CFE
AUDIT MANAGER

AUTUMN MCKINNEY
CPA, CIA, CGFM
AUDIT MANAGER

Office of the Director
PETER HUGHES
Ph.D., MBA, CPA, CIA, CFE, CITP

MAILING ADDRESS:
400 CIVIC CENTER DRIVE WEST
BUILDING 12, ROOM 232
SANTA ANA, CALIFORNIA 92701

TELEPHONE: (714) 834-5475
FAX: (714) 834-2880

EMAIL: peter.hughes@ocgov.com
WEBSITE: www.ocgov.com/audit/

Transmittal Letter

Audit No. 2428-B

August 11, 2005

TO: David E. Sundstrom
Auditor-Controller

FROM: Peter Hughes, Ph.D., CPA, Director
Internal Audit Department

SUBJECT: Integrated Internal Control Review of Auditor-Controller Accounts
Receivable and Collection Processes – IT Results

We have completed an Integrated Internal Control Review of the Auditor-Controller Accounts Receivable and Collection processes as of December 31, 2004. The final **Internal Auditor's Report** is attached along with your responses to our recommendations. This report contains the Information Technology results. We issued a separate report (#2428-A) for the manual processes and controls.

Please note, beginning in January 2005, we implemented a more structured and rigorous follow-up audit process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). As a matter of policy, our first Follow-Up Audit will now begin no later than six months upon the official release of the report. The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our second Follow-Up Audit will now begin at 12 months from the release of the original report, by which time all audit recommendations are expected to be addressed and implemented.

At the request of the AOC, we are to bring to their attention any audit recommendations we find still not addressed, resolved, or implemented after the second Follow-up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for discussion.

We have attached a Follow-Up Audit Report Form. Your department should complete this template as our audit recommendations are implemented. When we perform our Follow-Up Audit approximately six months from the date of this report, we will need to obtain the completed document to facilitate our review.

As the Director of the Internal Audit Department, effective December 14, 2004, I now make a monthly audit status presentation to the BOS where I detail any material and significant audit findings released in reports during the prior month, the implementation status of audit recommendations as disclosed by our follow-up audits, any pressing audit or resource issues; as well as, respond to inquiries from the BOS. Therefore, the results of this audit will be included in a future summary to the BOS.

As always, the Internal Audit Department is available to partner with you so that you can successfully implement or mitigate difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report or recommendations.

Additionally, we have attached a Customer Survey of Audit Services. Please complete the survey and return it to Renee Aragon, Executive Secretary, Internal Audit Department.

Attachment

Other recipients of this report:

- Members, Board of Supervisors
- Members, Audit Oversight Committee
- Thomas G. Mauk, County Executive Officer
- Shaun M. Skelly, Chief Assistant Auditor-Controller
- Mahesh Patel, Assistant Auditor-Controller, Information Technology
- Jan Grimes, Assistant Auditor-Controller, Central Operations
- Colin Hoffmaster, Senior Manager, A-C/General Accounting
- Win Swe, Manager, A-C, Accounts Receivable & Collections
- Tom Megara, Manager, A-C, Accounts Receivable
- Foreman, Grand Jury
- Darlene J. Bloom, Clerk of the Board of Supervisors



COUNTY OF ORANGE INTERNAL AUDIT DEPARTMENT

Integrity ♦ Objectivity ♦ Independence

ELI LITNER
CPA, CIA, CFE, CFS CISA
DEPUTY DIRECTOR

MICHAEL GOODWIN
CPA, CIA
AUDIT MANAGER

ALAN MARCUM
MBA, CPA, CIA, CFE
AUDIT MANAGER

AUTUMN MCKINNEY
CPA, CIA, CGFM
AUDIT MANAGER

Office of the Director
PETER HUGHES
Ph.D., MBA, CPA, CIA, CFE, CITP

MAILING ADDRESS:
400 CIVIC CENTER DRIVE WEST
BUILDING 12, ROOM 232
SANTA ANA, CALIFORNIA 92701

TELEPHONE: (714) 834-5475
FAX: (714) 834-2880
EMAIL: peter.hughes@ocgov.com
WEBSITE: www.ocgov.com/audit/

INTERNAL AUDITOR'S REPORT

Audit No. 2428-B

August 11, 2005

David E. Sundstrom
Auditor-Controller
12 Civic Center Plaza, Room 202
Santa Ana, CA 92702

We have completed an integrated internal control review of the Auditor-Controller Accounts Receivable and Collection processes as of December 31, 2004. Our audit was performed in accordance with professional standards established by the Institute of Internal Auditors. This report contains the Information Technology results of our audit. We issued a separate report (#2428-A) for the manual processes and controls.

Management of the Auditor-Controller's Office is responsible for establishing and maintaining a system of internal controls. The objectives of an internal control system are to provide management with reasonable, but not absolute assurance that assets are safeguarded against loss from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and recorded properly. County of Orange Accounting Manual (AM) No. S-2 – *Internal Control Systems* prescribes the policies and standards the departments/agencies should follow in establishing and maintaining internal control systems. Our review enhances and complements, but does not substitute for, the Auditor-Controller's continuing emphasis on control activities and self-assessment of control risks.

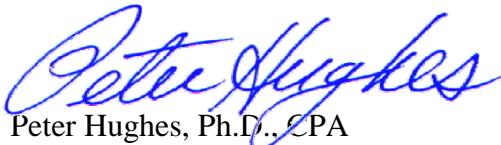
Because of inherent limitations in any system of internal controls, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or that the degree of compliance with the procedures may deteriorate. Accordingly, our review performed for the limited purpose described above would not necessarily disclose all weaknesses in the Auditor-Controller's operating procedures, accounting practices, and compliance with County policy.

Based upon our audit of the information technology controls related to the accounts receivable recording and collections processes, **no material weaknesses or significant issues were identified.** However, we did identify 37 control findings to improve controls and processes as noted in the Detailed Observations, Recommendations and Management Responses section of this report. Ten of the 37 are related to creating written policies and procedures, and 27 of the 37 are related to best practices/controls. See Attachment A for a description of report item classifications.

While in our report we indicate the specific processes, application, and general controls reviewed, **the Auditor-Controller should implement the recommendations in other processes, applications, and networks as they find them applicable.** An expectation of the Board of Supervisors is that departments and agencies will view this report as a “lessons learned” opportunity to guide them in proactively self-assessing other similar operations.

We appreciate the courtesy and cooperation extended to us by the personnel of the Auditor-Controller’s Information Technology and Accounts Receivable and Collections Sections during our review. If you have any questions regarding our review, please call contact me directly, Eli Littner, Deputy Director at 834-5899, Michael Goodwin, Audit Manager at 834-6066, or Autumn McKinney, IT Audit Manager at 834-6106.

Respectfully submitted,



Peter Hughes, Ph.D., CPA
Director, Internal Audit

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

- Members, Board of Supervisors
- Members, Audit Oversight Committee
- Thomas G. Mauk, County Executive Officer
- Shaun M. Skelly, Chief Assistant Auditor-Controller
- Mahesh Patel, Assistant Auditor-Controller, Information Technology
- Jan Grimes, Assistant Auditor-Controller, Central Operations
- Colin Hoffmaster, Senior Manager, A-C/General Accounting
- Win Swe, Manager, A-C, Accounts Receivable & Collections
- Tom Megara, Manager, A-C, Accounts Receivable
- Foreman, Grand Jury
- Darlene J. Bloom, Clerk of the Board of Supervisors

EXECUTIVE SUMMARY

OBJECTIVES

The Internal Audit Department conducted an integrated internal control review of the Auditor-Controller accounts receivable and collection processes. The objectives of our review were to determine if:

1. Invoices/claims submitted to the Auditor-Controller are recorded accurately, completely, and timely as accounts receivable on the Auditor-Controller's records.
2. Recorded accounts receivable are adequately monitored using reconciliations and aging reports.
3. Collection efforts on delinquent accounts are performed in accordance with established procedures and statutory requirements, including the process for writing off uncollectible debts.
4. Information Technology (IT) controls related to the above three objectives are adequate.
5. Any ineffective or inefficient processes existing that come to our attention during the audit.

BACKGROUND

The Auditor-Controller (A-C) is the Chief Accounting Officer for the County and oversees its central accounting systems, including the Accounts Receivable and Collections Section. The Section is comprised of the Accounts Receivable and Collections Units, each unit having their own distinct duties and responsibilities:

- Accounts Receivable Unit: This Unit receives copies of the invoices/claims issued by selected County departments to individuals, businesses, governments, and other entities for monies owed to the County. They record each invoice/claim as a receivable on the Auditor-Controller's records, set-up individual accounts on the accounts receivable system (CUBS), and process payments received. The general ledger balance for these receivables was approximately **\$36.7 million** as of 12/31/04. The accounts receivable balance fluctuates through the year as paid receivables are removed and new receivables are added. The Accounts Receivable Unit processes approximately \$200 million in receivables annually.
- Collections Unit: This Unit performs the collection services for delinquent receivables once the required series of collection letters have been issued. They perform collections for all County departments except for John Wayne Airport, the Social Services Agency, the Probation Department, the Public Defender, and the Treasurer-Tax Collector as these departments either use the collection services of other County departments or have their own collection units staffed by collection officers. The Collection Unit's major clients are the Sheriff-Coroner, the Health Care Agency, and the Resources and Development Management Department.



CUBS: The Auditor-Controller utilizes Columbia Ultimate Business Systems' Revenue Plus Collector System. This system, known as CUBS, serves as the subsidiary accounts receivable ledger. As such, the initial recording and subsequent collection of receivables are recorded in CUBS. Data in CUBS typically includes names, addresses, social security numbers, and occasionally electronic protected health information (ePHI) as described in the Health Insurance Portability and Accountability Act (HIPAA). CUBS is also used to generate collection notices, maintain collector activity, and produce aging and other management reports. CUBS resides on the Auditor-Controller's local area network (LAN) and is maintained by the Auditor-Controller's Information Technology Division.

SCOPE

Our integrated audit scope covered the initial recording of accounts receivable into CUBS; the reconciliations and aging reports used to monitor accounts receivable; and the collection and write-off of delinquent accounts. Additionally, selected information technology (IT) controls (general and application controls) supporting these processes were included in the audit scope.

Exclusions:

Our scope excluded cash receipting and processing of payments received for the accounts receivable activity. Our scope also excluded the trial court funding functions (reporting and distribution of fees, fines, and penalty assessments) performed by the Accounts Receivable Unit. We did not perform an application review of the CUBS system in its entirety and we did not review or test the integrity of the data (other than described) contained therein. While the CUBS system contains electronic protected health information (ePHI), we did not specifically test the requirements of the Health Insurance Portability & Accountability Act (HIPAA) Security Rule. We also did not perform a detailed security audit of the CUBS system or a vulnerability scan and penetration test of the local area network (LAN) on which it resides.

Detailed Scope for Information Technology (IT) Controls:

Our methodology included inquiry, observation, and examination of documentation for the IT controls. We reviewed selected application controls for the CUBS system and the general controls for the local area network (LAN) on which CUBS resides.

- Application Controls: These are system controls directly related to the application. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. We reviewed and tested the application controls in CUBS for accurate and complete input of key data. We also reviewed evidence to test whether application access controls were in place and functioning as intended to adequately restrict access to data within the system.
- General Controls: These are policies, procedures, and controls that apply to the overall computer operations. They control the environment in which the application operates and are not application specific. General control categories include: 1) security planning and management, 2) access controls (physical and logical controls that limit or detect access to computer resources), 3) software development and change controls, 4) system software (such as operating systems, file maintenance software, and database management systems), 5) segregation of duties, and 6) service continuity. We utilized internal control questionnaires and observed evidence to review the general controls in these six areas.



CONCLUSION

This report and conclusion is only for the Information Technology (IT) component of the integrated review. We issued a separate report (#2428-A) for the manual processes and controls.

Based upon our review, **no material weaknesses or significant issues** were identified. However, we did identify 37 control findings to improve their processes as noted in the Detailed Observations, Recommendations, and Management Responses section of this report. Ten of the 37 are related to creating written policies and procedures, and 27 of the 37 are related to best practices/controls. See Attachment A for a description of report item classifications.

While our audit was not performed for HIPAA security compliance, we communicated to Auditor-Controller management that several of the control findings identified are required by the HIPAA Security Rule effective April 21, 2005.



DETAILED OBSERVATIONS, RECOMMENDATIONS MANAGEMENT RESPONSES

AND

Logical Access

The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication, and authorization mechanisms, linking users and resources with access rules. These control practices help to ensure systems and information are protected from unauthorized access or use.

Finding No. 1: Network share permissions were configured to allow any user on the local area network to map to and access a sensitive folder. Another permission was granted to a transferred employee who no longer required access.

Recommendation No. 1: We recommend that the Auditor-Controller periodically review permission settings for local area network shares to ensure employees/groups only have access to authorized shares.

Auditor-Controller Response: Concur. Permissions have been modified to restrict access to sensitive folders. A procedure will be developed for a periodic review of network shares to ensure appropriate access. Estimated completion by August 31, 2005.

Finding No. 2: On the local area network, two administrator accounts and two user accounts were not specifically assigned to an individual end user and the guest account was enabled.

Recommendation No. 2: We recommend that the Auditor-Controller remove the unassigned local area network administrator accounts, discontinue the practice of allowing one user account to be used by more than one user, and disable the guest account.

Auditor-Controller Response: Concur. Unassigned administrator accounts have been removed and the guest account has been disabled. We will research and implement a system rule to limit use of one user account to a single user. Estimated completion by August 31, 2005.

Finding No. 3: Security settings for the local area network operating system did not require passwords that met complexity requirements.

Recommendation No. 3: We recommend that the Auditor-Controller enable the local area network operating system's password complexity requirements.

Auditor-Controller Response: Concur. Complexity rules for all logins to the network have been implemented. System rules have been established as follows:

- Set minimum password length to 7 characters
- Enable complex passwords
- Enable 60 day password expiration
- Enable maximum setting for reuse of passwords



- Enable setting such that after three unsuccessful attempts at logging in, the user's account will be disabled.
- Enable the capability to lock a user's workstation after 15 minutes of inactivity and require the user to enter their password to unlock the workstation.

These rules apply to all workstations in the Auditor-Controller's central office and can only be modified by a System Administrator.

Finding No. 4: The Auditor-Controller does not have a written policy governing user account passwords.

Recommendation No. 4: We recommend that the Auditor-Controller create a written policy for user account passwords including syntax requirements, change frequency, and reuse.

Auditor-Controller Response: Concur. A written policy has been developed and will be published by August 31, 2005. Per response to Recommendation 3 above, the system password rules have been implemented.

Finding No. 5: The Auditor-Controller's end user workstations are not configured to log off after a period of inactivity.

Recommendation No. 5: We recommend that the Auditor-Controller require its IT Division to configure workstations to automatically log off after a period of inactivity and to create a written policy requiring such.

Auditor-Controller Response: Concur. A System Rule has been implemented which locks out access to the desktop after 15 minutes of inactivity. The user's password is required to activate the workstation. A written policy regarding this rule has been developed and will be published by August 31, 2005.

Finding No. 6: The Auditor-Controller has no written policies for administering remote access to its local area network and does not change the modem password.

Recommendation No. 6: We recommend that the Auditor-Controller create written policies for administering remote access including periodic password changes for the modem.

Auditor-Controller Response: Concur. A written policy will be developed for administering remote access and periodic password changes for the modem. Estimated completion by August 31, 2005.

Finding No. 7: The Auditor-Controller has not documented its authorization for dial-up access granted to the CUBS vendor.

Recommendation No. 7: We recommend that the Auditor-Controller document authorization for any remote access granted to its local area network.



Auditor-Controller Response: Concur. Authorization for remote access will be documented. Estimated completion by August 31, 2005.

Finding No. 8: CUBS's application security settings require passwords to be only four characters in length.

Recommendation No. 8: We recommend that the Auditor-Controller increase CUBS's security setting for minimum password length to a minimum of eight characters.

Auditor-Controller Response: Concur. A request to change the minimum password setting for the CUBS application has been submitted to the vendor. Additionally, since access to the CUBS system is controlled at the network level, we believe changes already implemented to address Recommendation No. 3, above, further mitigate the problem. Estimated completion by August 31, 2005.

Security Monitoring

IT security administration should ensure that violation and security activity is logged, reported, reviewed, and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity.

Finding No. 9: The Auditor-Controller did not configure its network operating system auditing policies according to security best practices.

Recommendation No. 9: We recommend that the Auditor-Controller reconfigure its network operating system audit policies to record key security event activity, such as system events, policy changes, account management, and account logons.

Auditor-Controller Response: Concur. A system group policy has been created for both domain and domain controllers to audit specific events.

Finding No. 10: The Auditor-Controller does not have any written procedures for performing security audit log reviews.

Recommendation No. 10: We recommend that the Auditor-Controller establish written procedures for reviewing the network operating system's audit log, including IT Manager review of changes to policy settings and security event activity.

Auditor-Controller Response: Concur. IT staff will be trained in reviewing audit logs and written procedures will be developed accordingly. Estimated completion by August 31, 2005.

Security Related Personnel Practices and User Account Management

Management should ensure that appropriate and timely actions are taken regarding employee transfers and terminations so that internal controls and security are not impaired.



Finding No. 11: The Auditor-Controller does not have a consistent methodology for notifying its IT Division of new, transferring or terminating users. Subsequently, the IT Division does not receive timely notification of such events so that user accounts can be changed accordingly.

Recommendation No. 11: We recommend that the Auditor-Controller develop written procedures for notifying the IT Division of employee status changes.

Auditor-Controller Response: Concur. Auditor-Controller IT staff will work with A/C Human Resources staff to develop written procedures for notification of employee status changes. Estimated completion by August 31, 2005.

Finding No. 12: Resource owners (e.g., department section managers) do not periodically review who has access to their data.

Recommendation No. 12: We recommend that the Auditor-Controller require resource owners to periodically review who has access to their data to ensure they remain appropriate. This review should be documented.

Auditor-Controller Response: Concur. Auditor-Controller IT staff will work with resource owners to develop reporting to allow for such a review. Estimated completion by November 30, 2005.

Finding No. 13: The Auditor-Controller has no written policies and procedures for administering temporary or emergency access to its IT resources.

Recommendation No. 13: We recommend that the Auditor-Controller develop written policies and procedures for administering temporary or emergency access to its IT resources.

Auditor-Controller Response: Concur. Written policies and procedures will be developed for administering temporary or emergency access to IT resources. Estimated completion by November 30, 2005.

Business Continuity Management – IT Division

Organizations should have a documented and tested IT continuity plan that is in line with the overall business continuity plan to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption.

Finding No. 14: The Auditor-Controller has not documented a contingency plan for restoring IT operations following a disaster.

Recommendation No. 14: We recommend that the Auditor-Controller develop a documented contingency plan for restoring IT operations that includes an assessment of the criticality and sensitivity of IT operations, identification of supporting resources, and



establishment of emergency processing priorities. The plan should be agreed upon by both end-users and the IT Division, communicated to affected parties, and periodically tested.

Auditor-Controller Response: Concur. The Auditor-Controller will develop a documented contingency plan for restoring IT operations. Estimate completion by April 30, 2006.

Finding Nos. 15 and 16: The Auditor-Controller's LAN back-up tapes were stored in the server room in an unanchored fireproof safe. Additionally, the safe keys were located next to the safe.

Recommendation No. 15: We recommend that the Auditor-Controller store back-up tapes at an off-site location.

Auditor-Controller Response: Concur. We have contracted with an offsite storage vendor and have developed a schedule and process for our daily, monthly and annual backup cycles.

Recommendation No. 16: We recommend that the Auditor-Controller store any tapes located on-site in a secure manner.

Auditor-Controller Response: Concur. Only tapes required for the current week are being kept onsite in a fireproof vault. Once the daily backups have been completed, the tapes are stored at the Enterprise Data Center until they are sent to the offsite vendor at the end of the week.

Finding No. 17: The Auditor-Controller's backup procedures do not include testing of backup tapes or restoration procedures.

Recommendation No. 17: We recommend that the Auditor-Controller create written procedures for testing and restoration of back-up tapes.

Auditor-Controller Response: Concur. Written procedures for testing and restoration of back-up tapes will be created. Estimated completion by September 30, 2005.

Finding No. 18: In the Auditor-Controller's LAN server room, there are no fire detection devices present, the only fire suppression device is a hand extinguisher (that was inspected over five years ago), the humidity monitor is not functioning correctly, and there is no system to notify Auditor-Controller IT staff of problems with environmental controls (temperature, humidity).

Recommendation No. 18: We recommend the Auditor-Controller evaluate installing fire detection devices, periodically inspect the fire extinguisher, evaluate repairing the humidity monitor, and evaluate implementing an environmental control problem notification system.

Auditor-Controller Response: Concur. The Auditor-Controller will evaluate the above recommendations along with other options such as relocating the servers to achieve the same outcome in an economical way. Estimated completion of evaluation by October 31, 2005.



Finding No. 19: The Auditor-Controller's local area network utilizes the Hall of Finance and Records' (Building 12) uninterrupted power supply and emergency generator. The Auditor-Controller has no documentation and IT staff have limited knowledge (e.g., maintenance, performance, etc.) of the uninterrupted power supply and emergency generator that are relied upon.

Recommendation No. 19: We recommend that the Auditor-Controller obtain a better understanding of the local area network's uninterrupted power supply and emergency generator.

Auditor-Controller Response: Concur. The Auditor-Controller will request documentation on the uninterrupted power supply and emergency generator from RDMD. Estimated completion by October 31, 2005.

Finding No. 20: The Auditor-Controller does not have a formal hardware preventative maintenance program.

Recommendation No. 20: We recommend that the Auditor-Controller implement a periodic preventative maintenance procedure for hardware.

Auditor-Controller Response: Concur. The Auditor-Controller will implement a periodic preventative maintenance procedure for hardware. Estimated completion by October 31, 2005.

Physical Security

Appropriate physical security and access control measures should be established for IT facilities to reduce the risk of unauthorized personnel gaining access to facilities or access being inappropriately granted.

Finding No. 21: Certain employees of the Clerk-Recorder operate surveillance equipment in the same room as the Auditor-Controller's server room and accordingly know the numeric key code to enter the room.

Recommendation No. 21: We recommend that the Auditor-Controller evaluate segregating their servers so that only authorized Auditor-Controller personnel have access to them.

Auditor-Controller Response: Concur. However, this is not practical as this is shared space with the Clerk-Recorder. We will work with the Clerk-Recorder to develop a process that restricts access to the server area and which requires logging of entry to the servers. Other options such as locking down the server racks will also be evaluated. Estimated completion by August 31, 2005.



Finding No. 22: The Auditor-Controller has no documented physical security policies governing access to its server room and closets containing communications hardware, including access by visitors, contractors, and maintenance personnel.

Recommendation No. 22: We recommend that the Auditor-Controller develop written policies governing access to IT areas, namely the server room and any communication closets.

Auditor-Controller Response: Concur. We will develop written policies governing access to IT areas. Estimated completion by September 30, 2005.

Finding No. 23: Visitors are not formally signed in to the Auditor-Controller's server room or communications closets.

Recommendation No. 23: We recommend that the Auditor-Controller require IT staff to ensure visitors to sensitive IT areas sign in and out.

Auditor-Controller Response: Concur. We rarely, if ever, have visitors to the server room. However, a visitor sign in / sign out form will be developed and implemented. Estimated completion by August 31, 2005.

Finding No. 24: The numeric key code for the server room is not changed with regular frequency and there are no written policies governing changes to the code.

Recommendation No. 24: We recommend that the Auditor-Controller develop written policies governing the server room's combination lock including periodic changes.

Auditor-Controller Response: Concur. Written policies governing the server room's combination lock including periodic changes will be developed. Estimated completion by August 31, 2005.

Finding No. 25: The Auditor-Controller has no documented policies for the disposal of computer hardware.

Recommendation No. 25: We recommend that the Auditor-Controller develop written procedures for the disposal of computer hardware, including sanitation of equipment and/or media prior to disposal or reuse.

Auditor-Controller Response: Concur. Written procedures will be developed for the disposal of computer hardware, including sanitation of equipment and/or media prior to disposal or reuse. Estimated completion by August 31, 2005.

Business Continuity Plan – Accounts Receivable and Collections

The purpose of business continuity planning is to assist entities in continuing critical functions and recovering from disruptions to business operations.



Finding No. 26: The Auditor-Controller's business continuity plan for the Accounts Receivable and Collections Section does not include the following elements:

- **Prioritization of Business Processes** – The business continuity plan does not prioritize key business processes as ranging from mission critical to non-critical.
- **Disaster Scenarios** – The business continuity plan does not distinguish between or identify procedures for varying disaster scenarios.
- **Equipment and Forms** – The business continuity plan does not specifically identify the equipment and the manual forms needed to perform work in the event of a disaster.
- **Vendor Contacts** – The business continuity plan does not include contact information for key vendors.

Recommendation No. 26: We recommend that the Auditor-Controller's business continuity plan for the Accounts Receivable and Collections Section be enhanced to include identification and prioritization of key business processes, descriptions of procedures for varying types of disaster scenarios, identification of equipment and documents to be used, and emergency contact information for key vendors.

Auditor-Controller Response: Concur. Auditor-Controller Accounts Receivable and Collections will work in coordination with the Auditor-Controller Information Technology Division to complete the Unit's business continuity plan and also incorporate Collections-Accounts Receivable information into their continuity plan. Completion date will be the same as provided in the above finding number fourteen.

Finding No. 27: The Auditor-Controller's Accounts Receivable and Collections Section has not formally tested its business continuity plan.

Recommendation No. 27: We recommend that the Auditor-Controller formally test the business continuity plan for the Accounts Receivable and Collections Section on a periodic basis.

Auditor-Controller Response: Concur. Testing will be performed semi-annually, beginning fiscal year 2005-06.

Security Program Planning & Management

An organization wide program for security planning and management is the foundation of a security control structure. Without a well-designed program, security controls may be inadequate, responsibilities may be unclear, and controls may be inconsistently applied.

Finding No. 28: The Auditor-Controller has not performed a comprehensive high-level IT risk assessment.

Recommendation No. 28: We recommend that the Auditor-Controller develop a risk assessment that identifies and considers threats and vulnerabilities to both physical and



logical security, identifies the greatest risks, and dispositions which risks to accept and which to mitigate through security controls.

Auditor-Controller Response: Concur. The Auditor-Controller will contract for a risk assessment. The timing for this will depend on the availability of a budget to do so as well as implementation of an upgrade to a Windows 2003 server. Estimated completion by December 31, 2005.

Finding No. 29: The Auditor-Controller does not have a written plan that clearly describes a security program including who is responsible for managing access to resources.

Recommendation No. 29: We recommend that the Auditor-Controller develop a security program plan that covers all major systems and facilities and outlines the duties of IT management responsible for overseeing security as well as end users of the department's computer resources.

Auditor-Controller Response: Concur. A security program plan will be developed. Estimated completion by February 28, 2006.

Finding No. 30: The Auditor-Controller does not provide ongoing security awareness training or communications to its user community.

Recommendation No. 30: We recommend that the Auditor-Controller provide periodic computer security awareness training or communications to its employees.

Auditor-Controller Response: Concur. Periodic communications on computer security awareness will be issued. Estimated completion by October 31, 2005.

Finding No. 31: The Auditor-Controller does not have documented policies and procedures for responding to incidents caused by viruses, hackers, or software bugs.

Recommendation No. 31: We recommend that the Auditor-Controller develop written policies and procedures for responding to incidents that disrupt IT services.

Auditor-Controller Response: Concur. The Auditor-Controller will develop written policies and procedures for responding to incidents that disrupt IT services. Estimated completion by October 31, 2005.

Information Resource Classification

To protect IT resources (such as hardware, software, and data) with the most cost-effective means, resource owners should determine the level of protection needed by classifying information resources according to their criticality and sensitivity.

Finding Nos. 32, 33, and 34: The Auditor-Controller has not classified IT resources based upon established criticality and sensitivity criteria.



Recommendation No. 32: We recommend that the Auditor-Controller develop IT resource classification categories that meet their legal and business requirements for confidentiality, integrity, and availability.

Auditor-Controller Response: Concur. IT resources will be classified according to categories that meet legal and business requirements. To be cost-effective, broad categories will be used to reduce ongoing administration. Estimated completion by April 30, 2006.

Recommendation No. 33: We recommend that the Auditor-Controller formally identify its IT resource owners.

Auditor-Controller Response: Concur. IT resource owners will be formally identified. Estimated completion by April 30, 2006.

Recommendation No. 34: Once the classification categories and resources owners are identified, we recommend that the Auditor-Controller classify its IT resources based upon criticality and sensitivity.

Auditor-Controller Response: Concur. IT resources will be appropriately classified. Estimated completion by April 30, 2006.

Software Development Methodology

Organizations should have a documented system development methodology that includes requirements for testing, documentation, and approval. Following a documented system development methodology will help ensure systems meet user requirements, systems are adequately tested for performance and accuracy, and the possibility for unauthorized installation of software is minimized.

Finding No. 35: The Auditor-Controller does not have a documented system development methodology.

Recommendation No. 35: We recommend that the Auditor-Controller create a written system development methodology that addresses at a minimum:

- Selecting, installing, and modifying software.
- Authorizations for software modifications.
- Software test plan standards and required test plan approvals.
- Emergency changes.

Auditor-Controller Response: Partially Concur. The Auditor-Controller uses the SEI-CMM model for support of the CAPS application and has acquired the Rational toolset along with its development methodology for the re-engineering of the Assessment Tax System.

Since the CUBS application is not developed in-house, the particular development methodology used is not within our control. That said, written procedures for requesting modifications, testing and implementing code changes in CUBS will be developed.



Procedures for emergency changes will also be developed. Estimated completion by November 30, 2005.

Internal Audit Department Comment: The Auditor-Controller agrees to develop written procedures for modifying, testing, and implementing code changes to CUBS which substantially addresses the intent of the recommendation. The Internal Audit Department accepts the agreed upon action as full concurrence.

Application Security

The logical access to and use of IT computing resources should be restricted by the implementation of adequate application security mechanisms including procedures to keep such authentication and access mechanisms effective.

Finding No. 36: CUBS does not have commonly found security features that:

- Lock a user account out after a preset number of incorrect passwords have been entered (unsuccessful log-on lock-out).
- Prevent users from selecting the same password after a password change is required (password reuse prevention).
- Automatically log-off the application after a period of user inactivity (inactivity automatic time-out).

Recommendation No. 36: We recommend that the Auditor-Controller submit software change suggestions to the vendor to address the absent application security features.

Auditor-Controller Response: Concur. Suggested changes were submitted to Columbia Ultimate on July 5, 2005. The first and third security feature above will be available in the CUBS upgrade that is currently in process and should be implemented by August 31, 2005.

Additionally, since access to the CUBS system is controlled at the network level, we believe changes already implemented to address Recommendation No. 3, above, further mitigate the problem.

Data Validation Features

Transaction data entered for processing should be subject to a variety of edit controls to check for accuracy, completeness and validity. Performing accuracy, completeness and validity checks will facilitate early detection of data errors.

Finding No. 37: CUBS does not have data validation features for key input fields that ensure:

- Reference numbers are entered for each transaction (completeness check).
- Dates entered fall within valid ranges (reasonableness check).
- Only numbers are entered for telephone numbers (numeric check).
- Invoice amounts are not entered as credits (sign check).
- Only valid state address codes are entered (existence check).



Recommendation No. 37: We recommend that the Auditor-Controller submit software change suggestions to the vendor to address the absent data validation features.

Auditor-Controller Response: Concur. Suggested changes were submitted to Columbia Ultimate on July 5, 2005. The date for the completion of this change has not yet been provided by the vendor.



ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we have classified audit report items into three distinct categories:

Material Weaknesses:

Audit findings or a combination of Significant Issues that can result in financial liability and exposure to a department/agency and to the County as a whole. Management is expected to address “Material Weaknesses” brought to their attention immediately.

Significant Issues:

Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of processes or internal controls. Significant Issues do not present a material exposure throughout the County. They generally will require prompt corrective actions.

Control Findings:

Audit findings that require management’s corrective action to implement or enhance processes and internal controls. Control Findings are expected to be addressed within our follow-up process of six months, but no later than twelve months.



ATTACHMENT B: Auditor-Controller Management Responses



DAVID E. SUNDSTROM, CPA
AUDITOR-CONTROLLER

AUDITOR-CONTROLLER COUNTY OF ORANGE

HALL OF FINANCE AND RECORDS
12 CIVIC CENTER PLAZA, ROOM 202
POST OFFICE BOX 567
SANTA ANA, CALIFORNIA 92702-0567
(714) 834-2450 FAX: (714) 834-2569

www.ac.ocgov.com

SHAUN M. SKELLY
CHIEF ASSISTANT AUDITOR-CONTROLLER

JAN E. GRIMES
ASSISTANT AUDITOR-CONTROLLER
CENTRAL OPERATIONS

WILLIAM A. CASTRO
ASSISTANT AUDITOR-CONTROLLER
SATELLITE ACCOUNTING OPERATIONS

MAHESH N. PATEL
ASSISTANT AUDITOR-CONTROLLER
INFORMATION TECHNOLOGY

RECEIVED

AUG 09 2005

INTERNAL AUDIT
DEPARTMENT

TO: Peter Hughes, Director
Internal Audit Department

SUBJECT: Response to Internal Audit Revised Draft Report of Integrated Internal Control
Review of the Auditor-Controller Accounts Receivable and Collection Processes

The following are our responses to the recommendations contained in the Draft Report on Integrated Internal Control Review and Accounts Receivable and Collections Process IT Results (Audit No. 2428-B).

We appreciate that the scope of the audit included the general controls over our Local Area Network (LAN) and the physical and environmental controls of our server room. It should be noted that logical access to the CUBS system is restricted to those working in the Collections/Accounts Receivable units and is not directly affected by the noted control weaknesses concerning LAN security. Therefore, we considered the potential vulnerabilities of all of our automated systems operating on our LAN or housed in our server room when responding to the recommendations concerning LAN security. Of the five recommendations specific to the CUBS application, we have immediately addressed the three which were within our control and have requested that the vendor modify their off-the-shelf software for the remaining two.

However, I do not concur with your overall assessment that there are 37 reportable conditions surrounding the collections/accounts receivable function. This observation is misleading because Internal Audit's definition of a "reportable condition" is inconsistent with the generally accepted terminology used throughout the accounting and auditing industry.

Although the Internal Audit Department has developed its own definitions for commonly used control classifications, and publishes these as an appendix to the report, a knowledgeable reader would have no need to refer to those definitions. Internal Audit defines a reportable condition as "Audit findings that require management's corrective action to implement or enhance processes and internal" (sic). However, a reportable condition is defined in The American Institute of Certified Public Accounts Statement of Auditing Standards (SAS) 60 as matters that represent a significant deficiency in the design or operation of the internal control structure which could adversely affect the organization's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. Other documents



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 2

which include this definition are: "Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements," issued by the Public Company Accounting Oversight Board (PCAOB) and Office of Management and Budget (OMB) OMB Circular A-123, "Management's Responsibility for Internal Control." Based on this, none of the findings cited in the report remotely fall within the classification of a reportable condition.

Recommendation No. 1:

We recommend that the Auditor-Controller periodically review permission settings for local area network shares to ensure employees/groups only have access to authorized shares.

Auditor-Controller Response:

Concur. Permissions have been modified to restrict access to sensitive folders. A procedure will be developed for a periodic review of network shares to ensure appropriate access. Estimated completion by August 31, 2005.

Recommendation No. 2:

We recommend that the Auditor-Controller remove the unassigned local area network administrator accounts, discontinue the practice of allowing one user account to be used by more than one user, and disable the guest account.

Auditor-Controller Response:

Concur. Unassigned administrator accounts have been removed and the guest account has been disabled. We will research and implement a system rule to limit use of one user account to a single user. Estimated completion by August 31, 2005.

Recommendation No. 3:

We recommend that the Auditor-Controller enable the local area network operating system's password complexity requirements.

Auditor-Controller Response:

Concur. Complexity rules for all logins to the network have been implemented. System rules have been established as follows:

- Set minimum password length to 7 characters
- Enable complex passwords
- Enable 60 day password expiration
- Enable maximum setting for reuse of passwords
- Enable setting such that after three unsuccessful attempts at logging in, the user's account will be disabled.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 3

- Enable the capability to lock a user's workstation after 15 minutes of inactivity and require the user to enter their password to unlock the workstation.

These rules apply to all workstations in the Auditor-Controller's central office and can only be modified by a System Administrator.

Recommendation No. 4:

We recommend that the Auditor-Controller create a written policy for user account passwords including syntax requirements, change frequency, and reuse.

Auditor-Controller Response:

Concur. A written policy has been developed and will be published by August 31, 2005. Per response to Recommendation 3 above, the system password rules have been implemented.

Recommendation No. 5:

We recommend that the Auditor-Controller require its IT Division to configure workstations to automatically log off after a period of inactivity and to create a written policy requiring such.

Auditor-Controller Response:

Concur. A System Rule has been implemented which locks out access to the desktop after 15 minutes of inactivity. The user's password is required to activate the workstation. A written policy regarding this rule has been developed and will be published by August 31, 2005.

Recommendation No. 6:

We recommend that the Auditor-Controller create written policies for administering remote access including periodic password changes for the modem.

Auditor-Controller Response:

Concur. A written policy will be developed for administering remote access and periodic password changes for the modem. Estimated completion by August 31, 2005.

Recommendation No. 7:

We recommend that the Auditor-Controller document authorization for any remote access granted to its local area network.

Auditor-Controller Response:

Concur. Authorization for remote access will be documented. Estimated completion by August 31, 2005.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 4

Recommendation No. 8:

We recommend that the Auditor-Controller increase CUBS's security setting for minimum password length to a minimum of eight characters.

Auditor-Controller Response:

Concur. A request to change the minimum password setting for the CUBS application has been submitted to the vendor. Additionally, since access to the CUBS system is controlled at the network level, we believe changes already implemented to address Recommendation No. 3, above, further mitigate the problem. Estimated completion by August 31, 2005.

Recommendation No. 9:

We recommend that the Auditor-Controller reconfigure its network operating system audit policies to record key security event activity, such as system events, policy changes, account management, and account logons.

Auditor-Controller Response:

Concur. A system group policy has been created for both domain and domain controllers to audit specific events.

Recommendation No. 10:

We recommend that the Auditor-Controller establish written procedures for reviewing the network operating system's audit log, including IT Manager review of changes to policy settings and security event activity.

Auditor-Controller Response:

Concur. IT staff will be trained in reviewing audit logs and written procedures will be developed accordingly. Estimated completion by August 31, 2005.

Recommendation No. 11:

We recommend that the Auditor-Controller develop written procedures for notifying the IT Division of employee status changes.

Auditor-Controller Response:

Concur. Auditor-Controller IT staff will work with A/C Human Resources staff to develop written procedures for notification of employee status changes. Estimated completion by August 31, 2005.

Recommendation No. 12:

We recommend that the Auditor-Controller require resource owners to periodically review who has access to their data to ensure they remain appropriate. This review should be documented.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 5

Auditor-Controller Response:

Concur. Auditor-Controller IT staff will work with resource owners to develop reporting to allow for such a review. Estimated completion by November 30, 2005.

Recommendation No. 13:

We recommend that the Auditor-Controller develop written policies and procedures for administering temporary or emergency access to its IT resources.

Auditor-Controller Response:

Concur. Written policies and procedures will be developed for administering temporary or emergency access to IT resources. Estimated completion by November 30, 2005.

Recommendation No. 14:

We recommend that the Auditor-Controller develop a documented contingency plan for restoring IT operations that includes an assessment of the criticality and sensitivity of IT operations, identification of supporting resources, and establishment of emergency processing priorities. The plan should be agreed upon by both end-users and the IT Division, communicated to affected parties, and periodically tested.

Auditor-Controller Response:

Concur. The Auditor-Controller will develop a documented contingency plan for restoring IT operations. Estimate completion by April 30, 2006.

Recommendation No. 15:

We recommend that the Auditor-Controller store back-up tapes at an off-site location.

Auditor-Controller Response:

Concur. We have contracted with an offsite storage vendor and have developed a schedule and process for our daily, monthly and annual backup cycles.

Recommendation No. 16:

We recommend that the Auditor-Controller store any tapes located on-site in a secure manner.

Auditor-Controller Response:

Concur. Only tapes required for the current week are being kept onsite in a fireproof vault. Once the daily backups have been completed, the tapes are stored at the Enterprise Data Center until they are sent to the offsite vendor at the end of the week.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 6

Recommendation No. 17:

We recommend that the Auditor-Controller create written procedures for testing and restoration of back-up tapes.

Auditor-Controller Response:

Concur. Written procedures for testing and restoration of back-up tapes will be created. Estimated completion by September 30, 2005

Recommendation No. 18:

We recommend that the Auditor-Controller evaluate installing fire detection devices, periodically inspect the fire extinguisher, evaluate repairing the humidity monitor, and evaluate implementing a environment control problem notification system.

Auditor-Controller Response:

Concur. The Auditor-Controller will evaluate the above recommendations along with other options such as relocating the servers to achieve the same outcome in an economical way. Estimated completion of evaluation by October 31, 2005.

Recommendation No. 19:

We recommend that the Auditor-Controller obtain a better understanding of the local area network's uninterrupted power supply and emergency generator.

Auditor-Controller Response:

Concur. The Auditor-Controller will request documentation on the uninterrupted power supply and emergency generator from RDMD. Estimated completion by October 31, 2005.

Recommendation No. 20:

We recommend that the Auditor-Controller implement a periodic preventative maintenance procedure for hardware.

Auditor-Controller Response:

Concur. The Auditor-Controller will implement a periodic preventative maintenance procedure for hardware. Estimated completion by October 31, 2005.

Recommendation No. 21:

We recommend that the Auditor-Controller evaluate segregating their servers so that only authorized Auditor-Controller personnel have access to them.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 7

Auditor-Controller Response:

Concur. However, this is not practical as this is shared space with the Clerk-Recorder. We will work with the Clerk-Recorder to develop a process that restricts access to the server area and which requires logging of entry to the servers. Other options such as locking down the server racks will also be evaluated. Estimated completion by August 31, 2005.

Recommendation No. 22:

We recommend that the Auditor-Controller develop written policies governing access to IT areas, namely the server room and any communication closets.

Auditor-Controller Response:

Concur. We will develop written policies governing access to IT areas. Estimated completion by September 30, 2005.

Recommendation No. 23:

We recommend that the Auditor-Controller require IT staff to ensure visitors to sensitive IT areas sign in and out.

Auditor-Controller Response:

Concur. We rarely, if ever, have visitors to the server room. However, a visitor sign in / sign out form will be developed and implemented. Estimated completion by August 31, 2005.

Recommendation No. 24:

We recommend that the Auditor-Controller develop written policies governing the server room's combination lock including periodic changes.

Auditor-Controller Response:

Concur. Written policies governing the server room's combination lock including periodic changes will be developed. Estimated completion by August 31, 2005.

Recommendation No. 25:

We recommend that the Auditor-Controller develop written procedures for the disposal of computer hardware, including sanitation of equipment and/or media prior to disposal or reuse.

Auditor-Controller Response:

Concur. Written procedures will be developed for the disposal of computer hardware, including sanitation of equipment and/or media prior to disposal or reuse. Estimated completion by August 31, 2005.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 8

Recommendation No. 26:

We recommend that the Auditor-Controller's business continuity plan for the Accounts Receivable and Collections Section be enhanced to include identification and prioritization of key business processes, descriptions of procedures for varying types of disaster scenarios, identification of equipment and documents to be used, and emergency contact information for key vendors.

Auditor-Controller Response:

Concur. Auditor-Controller Accounts Receivable and Collections will work in coordination with the Auditor-Controller Information Technology Division to complete the Unit's business continuity plan and also incorporate Collections-Accounts Receivable information into their continuity plan. Completion date will be the same as provided in the above finding number fourteen.

Recommendation No. 27:

We recommend that the Auditor-Controller formally test the business continuity plan for the Accounts Receivable and Collections Section on a periodic basis.

Auditor-Controller Response:

Concur. Testing will be performed semi-annually, beginning fiscal year 2005-06.

Recommendation No. 28:

We recommend that the Auditor-Controller develop a risk assessment that identifies and considers threats and vulnerabilities to both physical and logical security, identifies the greatest risks, and dispositions which risks to accept and which to mitigate through security controls.

Auditor-Controller Response:

Concur. The Auditor-Controller will contract for a risk assessment. The timing for this will depend on the availability of a budget to do so as well as implementation of an upgrade to a Windows 2003 server. Estimated completion by December 31, 2005.

Recommendation No. 29:

We recommend that the Auditor-Controller develop a security program plan that covers all major systems and facilities and outlines the duties of IT management responsible for overseeing security as well as end users of the department's computer resources.

Auditor-Controller Response:

Concur. A security program plan will be developed. Estimated completion by February 28, 2006.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 9

Recommendation No. 30:

We recommend that the Auditor-Controller provide periodic computer security awareness training or communications to employees.

Auditor-Controller Response:

Concur. Periodic communications on computer security awareness will be issued. Estimated completion by October 31, 2005

Recommendation No. 31:

We recommend that the Auditor-Controller develop written policies and procedures for responding to incidents that disrupt IT services.

Auditor-Controller Response:

Concur. The Auditor-Controller will develop written policies and procedures for responding to incidents that disrupt IT services. Estimated completion by October 31, 2005.

Recommendation No. 32:

We recommend that the Auditor-Controller develop IT resource classification categories that meet their legal and business requirements for confidentiality, integrity, and availability.

Auditor-Controller Response:

Concur. IT resources will be classified according to categories that meet legal and business requirements. To be cost-effective, broad categories will be used to reduce ongoing administration. Estimated completion by April 30, 2006.

Recommendation No. 33:

We also recommend that the Auditor-Controller formally identify IT resource owners.

Auditor-Controller Response:

Concur. IT resource owners will be formally identified. Estimated completion by April 30, 2006.

Recommendation No. 34: Once the classification categories and resources owners are identified, we recommend that the Auditor-Controller classify its IT resources based on criticality and sensitivity.

Auditor-Controller Response:

Concur. IT resources will be appropriately classified. Estimated completion by April 30, 2006.



Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 10

Recommendation No. 35:

We recommend that the Auditor-Controller create a written system development methodology that addresses at a minimum:

- Selecting, installing, and modifying software.
- Authorizations for software modifications.
- Software test plan standards and required test plan approvals.
- Emergency changes.

Auditor-Controller Response:

Partially Concur. The Auditor-Controller uses the SEI-CMM model for support of the CAPS application and has acquired the Rational toolset along with its development methodology for the re-engineering of the Assessment Tax System

Since the CUBS application is not developed in-house, the particular development methodology used is not within our control. That said, written procedures for requesting modifications, testing and implementing code changes in CUBS will be developed. Procedures for emergency changes will also be developed. Estimated completion by November 30, 2005.

Recommendation No. 36:

We recommend that the Auditor-Controller submit software change suggestions to the vendor to address the absent application security features.

Auditor-Controller Response:

Concur. Suggested changes were submitted to Columbia Ultimate on July 5, 2005. The first and third security feature above will be available in the CUBS upgrade that is currently in process and should be implemented by August 31, 2005.

Additionally, since access to the CUBS system is controlled at the network level, we believe changes already implemented to address Recommendation No. 3, above, further mitigate the problem.

Recommendation No. 37:

We recommend that the Auditor-Controller submit software change suggestions to the vendor to address the absent data validation features.

Auditor-Controller Response:


Concur. Suggested changes were submitted to Columbia Ultimate on July 5, 2005. The date for the completion of this change has not yet been provided by the vendor.



ATTACHMENT B: Auditor-Controller Management Responses (con't)

Peter Hughes, Director, Internal Audit Department
Revised Audit Report No. 2428-B
August 4, 2005
Page 11

Thank you for the opportunity to respond to the draft report. Please contact Mahesh Patel at 834-3895, if you have any questions on our response.


David E. Sundstrom
Auditor-Controller

MP:lr (Response to Audit Report No. 2428-B)
Attachment

cc: Shaun Skelly, Auditor-Controller
Jan Grimes, Auditor-Controller
Mahesh Patel, Auditor-Controller
Win Swe, Auditor-Controller
Tom Megara, Auditor-Controller
Colin Hoffmaster, Auditor-Controller
Mahesh Patel, Auditor-Controller





**COUNTY OF ORANGE
INTERNAL AUDIT DEPARTMENT**

Integrity • Objectivity • Independence

ELI LITTNER
CPA, CIA, CFE, CFS, CISA
DEPUTY DIRECTOR

MICHAEL J. GOODWIN
CPA, CIA
AUDIT MANAGER

ALAN MARCUM
MBA, CPA, CIA, CFE
AUDIT MANAGER

AUTUMN MCKINNEY
CPA, CIA, CGFM
AUDIT MANAGER

Office of the Director
PETER HUGHES
Ph.D., MBA, CPA, CIA, CFE, CITP

MAILING ADDRESS:
400 CIVIC CENTER DRIVE WEST
BUILDING 12, ROOM 232
SANTA ANA, CALIFORNIA 92701

TELEPHONE: (714) 834-5475
FAX: (714) 834-2880
EMAIL: peter.hughes@ocgov.com
WEBSITE: www.ocgov.com/audit/

REJOINDER

We thank the Auditor-Controller for their August 4, 2005 response to the audit findings and their concurrence with the 37 recommendations.

While we do not agree with the Auditor-Controller's interpretation of how the authoritative accounting literature defines a "reportable condition" for internal auditing purposes, we can agree to a nomenclature change from "reportable condition" to "control finding" for the sake of clarity.

The Internal Audit Department is an independent audit function reporting directly to the Orange County Board of Supervisors.

