INFORMATION TECHNOLOGY AUDIT
AUDITOR-CONTROLLER DEPARTMENT
LASER CHECK PRINTING

AS OF MARCH 31, 2003

REPORT DATE:
September 23, 2003

Audit Number #2326

Audit Director:	**Dr. Peter Hughes, CPA, CIA, CFE, CITP**
Deputy Director:	**Eli Littner, CPA, CIA, CISA**
Audit Manager:	**Autumn McKinney, CPA, CIA, CGFM**
In-Charge Auditor:	**Scott Suzuki, CPA, CIA, CISA**

INTERNAL AUDIT DEPARTMENT
COUNTY OF ORANGE

TABLE OF CONTENTS

TRANSMITTAL LETTER i

INTERNAL AUDITOR'S REPORT 1
Objectives 3
Background 3
Scope 3
Conclusion 4

OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES 5
1. Application Server Security 5
2. Duties Segregation 5
3. Supervisory Reviews and Reconciliation 6
4. Data Encryption and Logical Access to Security Files 8
5. User Account Administration 9
6. Data Back-Up 10
7. Data Retention 11
8. Safeguarding Blank Check Stock 12
9. Password Administration 12
10. Operating System Account Policies 13
11. Server Administrator 14
12. Application Controls 14
13. Change Controls 15
14. Audit Trails 16
15. Policies and Procedures 16
16. Vendor Contractual Compliance 17

ATTACHMENT: Auditor-Controller Response 19

PETER HUGHES, Ph.D., CPA, CIA, CFE, CITP
Director
INTERNAL AUDIT DEPARTMENT
400 Civic Center Drive West
Building 12, Room 232
Santa Ana, California 92701-4521
(714) 834-5475 Fax: (714) 834-2880

TRANSMITTAL LETTER

Audit No. 2326

September 23, 2003

TO: David E. Sundstrom
Auditor-Controller

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

SUBJECT: Information Technology Audit of Auditor-Controller's Laser Check Printing

We have completed our audit of the Auditor-Controller's laser check printing process for the period ending March 31, 2003. The final report is attached along with your responses to our recommendations. We have also attached a Customer Survey of Audit Services. Please complete the survey and return it to Eli Littner, Deputy Director of Internal Audit.

We appreciate the courtesy and cooperation of your staff during our review.

Other recipients of this audit report:
Members, Board of Supervisors
Members, Audit Oversight Committee
James D. Ruth, Interim County Executive Officer
Daniel K. Hatton, Chief Information Officer, CEO/Information & Technology
John Nakane, Chief Assistant, Auditor-Controller
Jim McConnell, Assistant Auditor-Controller, A-C/Central Operations
Mahesh Patel, Assistant Auditor-Controller, A-C/Information Technology
Robert Leblow, Manager, A-C/Claims & Disbursing Unit
Jim Berch, Manager, A-C/IT/Accounting, Payroll, and Property Tax Systems
Reza Khayyami, Chief Technology Officer, CEO/Information & Technology
John Wheeler, Information Systems Manager, CEO/Information & Technology
Robert Connal, Manager, CEO/IT/Network Services Division
KC Roestenberg, Program Director, ACS
Phil Paker, Manager, ACS/Applications Systems & Programming/CAPS
Phil Daignau, Team Lead, ACS/Applications Systems & Programming/CAPS
Foreman, Grand Jury
Macias, Gini & Company
Darlene J. Bloom, Clerk of the Board of Supervisors

PETER HUGHES, Ph.D., CPA, CIA, CFE, CITP
Director
INTERNAL AUDIT DEPARTMENT
400 Civic Center Drive West
Building 12, Room 232
Santa Ana, California 92701-4521
(714) 834-5475 Fax: (714) 834-2880

INTERNAL AUDITOR'S REPORT

Audit No. 2326

September 23, 2003

David E. Sundstrom
Auditor-Controller
12 Civic Center Plaza
P.O. Box 567
Santa Ana, California 92702-0567

We have performed an audit of the Auditor-Controller's laser check printing process as of March 31, 2003. Our review was made in accordance with professional standards, established by the Institute or Internal Auditors (IIA) and the Information Systems Audit and Control Association (ISACA) for the purpose of evaluating the design and operating effectiveness of internal controls for the laser check printing process. We believe our audit provides a reasonable basis for our opinion.

Management of the Auditor-Controller 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 Accounting Procedure (CAP) - *Internal Control Systems* (formerly No. 33) - prescribes the policies and standards to be followed by departments/agencies in establishing and maintaining internal control systems. Our audit enhances 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. Additionally, 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 audit was 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, it is our opinion that internal controls over critical aspects of the laser check printing process are not effective and need immediate attention. We also noted several opportunities where internal controls over this process could be introduced or further enhanced. Our recommendations are detailed in the Observations, Recommendations, and Management Responses section of this report. Responses from the Auditor-Controller's Department have been included for each recommendation and the complete text of responses has been appended to the report.

We appreciate the courtesy and cooperation extended to us by the personnel of the Auditor-Controller, CEO/Office of Information & Technology, and ACS during our review. If we can be of further assistance, please contact me directly, or Eli Littner, Deputy Director, at (714) 834-5899, or Autumn McKinney, Audit Manager, at (714) 834-6106.

Respectfully submitted,

Dr. Peter Hughes, CPA
Director, Internal Audit

Attachment

Distribution: Pursuant to Audit Oversight Committee Procedure No. 1
Members, Board of Supervisors
Members, Audit Oversight Committee
James D. Ruth, Interim County Executive Officer
Daniel K. Hatton, Chief Information Officer, CEO/Information & Technology
John Nakane, Chief Assistant, Auditor-Controller
Jim McConnell, Assistant Auditor-Controller, A-C/Central Operations
Mahesh Patel, Assistant Auditor-Controller, A-C/Information Technology
Robert Leblow, Manager, A-C/Claims & Disbursing Unit
Jim Berch, Manager, A-C/IT/Accounting, Payroll, and Property Tax Systems
Reza Khayyami, Chief Technology Officer, CEO/Information & Technology
John Wheeler, Information Systems Manager, CEO/Information & Technology
Robert Connal, Manager, CEO/IT/Network Services Division
KC Roestenberg, Program Director, ACS
Phil Paker, Manager, ACS/Applications Systems & Programming/CAPS
Phil Daignau, Team Lead, ACS/Applications Systems & Programming/CAPS
Foreman, Grand Jury
Macias, Gini & Company
Darlene J. Bloom, Clerk of the Board of Supervisors

OVERVIEW

Objectives

The Internal Audit Department conducted an audit of the Auditor-Controller's laser check printing process for the purpose of evaluating internal and system controls and determining whether such controls were functioning adequately to ensure:

- Checks are properly processed and result in complete output.
- Application and check data is protected from unauthorized users.
- Data is adequately protected from disasters.
- Only valid changes to the application are deployed.
- Check printing duties are adequately segregated.

Background

In 2002, RxLaser received a contract from the County to provide a new check printing application, printing hardware and supplies, and related support. This new laser check printing process prints the entire check on special stock including bank information, logos, and signatures and replaces the previous impact printing on pre-printed check stock. The laser check printing process generates approximately 120,000 checks per month for the Auditor-Controller's accounts payable, trust, and payroll disbursements and the Social Services Agency's welfare disbursements. ACS (Affiliated Computer Solutions) manages the RxLaser servers under contract with the CEO/Office of Information & Technology (CEO/IT). The laser check printing application and database reside at the County EDC (Enterprise Data Center) on two servers, a primary and a secondary/back-up. Additional installations of the check printing application reside in the Auditor-Controller's Disbursing Unit for manual check runs and in the ACS development area for development and testing purposes only (no check printing takes place at this location).

Scope

Our audit scope covered the laser check printing process from the point at which check data was received by the check printing application from CAPS (County Accounting & Payroll System), CDS (Case Data System), and GIS (GAIN Information System) to the point where checks were physically printed. Our detailed testing covered only check data received from CAPS and not CDS or GIS. As related to the audit scope, we also reviewed access controls, disaster recovery plans, supplies safeguarding, and change control practices.

We did not review procedures for distributing checks once they were printed, authorization of checks, recording of expenditures in the general ledger, or other general computer and application controls not related to the check printing process. Additionally, we did not perform an application review of the laser check printing application in its entirety and we did not review or test the integrity of the data contained therein.

Conclusion

Based upon our audit, it is our opinion that internal controls over critical aspects of the laser check printing process are not currently effective and need immediate attention. We also noted several opportunities where internal controls over the following areas could be either introduced or further enhanced because these areas could result in significant errors or irregularities if uncorrected:

- Access Controls: Network access control lists for the County's routers were not defined to prevent access to the laser check printing subnet from unauthorized intranet hosts. Critical application database and data files were not encrypted. Administration over passwords, user accounts, and operating system policies was not adequate.

- Duties Segregation: Duties amid the Disbursing Unit staff were not adequately segregated as four non-supervisory employees have complete control of the manual check creation process.

- Supervisory Reviews and Reconciliations: We noted several areas where supervisory reviews and reconciliations can and should be improved.

- Service Continuity: The replication process for the RxLaser server needs formalization. There were no written policies and procedures for laser check printing operations or disaster recovery.

- Data Retention: Data to reprint checks was archived for six months.

- Check Stock Safeguarding: Check stock was not appropriately accounted for and an excessive number of employees were permitted access to the cage containing blank check stock at the EDC.

- Duties Assignment: There was no system administrator assigned to the RxLaser servers.

- Application controls: Application controls for the laser check printing application require improvement so that the authorized signature is not printed on test pages and checks payable to cash are not printed.

- Change Controls: Certain development and change procedures were not adequate and were not consistently followed.

- Audit Trail: A log of checks printed from the laser check printing application (*Daily Report)* was not generated and retained.

Additionally, we noted vendor contractual non-compliance.

Our findings and recommendations are detailed in the Observations, Recommendations, and Management Responses section of this report.

We appreciate the courtesy and cooperation extended to us by the personnel of the Auditor-Controller, CEO/Office of Information & Technology, and ACS during our review.

OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

1. Application Server Security

The RxLaser servers and printers reside on a subnet of the County network. Original security plans called for limiting access to this subnet to a select number of hosts.

Our audit revealed that network ACLs (access control lists) for the County's routers were not defined to prevent access to the laser check printing subnet. We were informed that the CEO/IT's Network Services Division did not receive instructions to define the ACLs when the subnet was deployed.

Without defined ACLs and with proper knowledge, it is possible for unauthorized intranet hosts to access the laser check printing subnet. The logical access to and use of I/T computing resources should be restricted by the implementation of authorization mechanisms that link users and resources with access rules.

Failure to properly limit access to the laser check printing subnet increases the risk of:

- Incurring data loss from malicious attacks.
- Disruption to the laser check printing process.
- Irregularities in the laser check printing database and possible improper check creation.

Moreover, these risks are magnified because the application database was not encrypted (discussed in item No. 4 below).

Recommendation No. 1: We recommend that the Auditor-Controller immediately direct the CEO/IT to properly define router ACLs to ensure only authorized network hosts have access to the laser check printing subnet.

Auditor-Controller Response: Concur. Network Services Division has restricted the RXLaser environment to: Auditor Controller network; AS&P network; Enterprise Data Center network; St Andrews Network; IBM Mainframe; Insight Manager for monitoring, and a Enterprise Data Center backup server per the list provided by the RXLaser administration team. NSD has further tested these ACL's and have confirmed operation.

2. Duties Segregation

The A-C's Disbursing Unit staff has the capability to create "manual" accounts payable, trust, and payroll checks on demand.

Manual check printing duties of the Disbursing Unit staff are not adequately segregated. Seven employees, three of whom are supervisors, have complete control of the manual check creation process. These Disbursing Unit staff can obtain blank check stock, create a manual check (warrant) transaction in CAPS, approve the manual check (warrant) in CAPS, and access the laser check printing application to print a manual check. Currently, CAPS security profile settings allow the same user to create and approve a manual check (warrant).

Improper segregation of employee duties increases the risk where a single employee could fraudulently create, approve, and cash a check. A-C management agreed the duties are not segregated; however, they indicated that staffing constraints might not allow them to achieve adequate segregation, especially for the supervisory personnel who may, as a function of their position, be able to override certain controls nonetheless.

When actual duties segregation is not practical or otherwise achievable under existing circumstances, mitigating detective controls should be established. These detective controls are typically enhanced supervisory reviews and reconciliations. Item No. 3 below addresses the need for improved supervisory review and reconciliation.

Recommendation No. 2: We recommend the Auditor-Controller evaluate separating duties within the manual check process to the extent possible. If separation is not possible, the Auditor-Controller should ensure its supervisory reviews and reconciliations (discussed further in item No. 3. below) are sufficient.

Auditor-Controller Response: Concur. The Auditor-Controller will evaluate options to ensure its supervisory reviews and reconciliations are sufficient.

3. Supervisory Reviews and Reconciliation

The laser check printing application offers basic reporting capability. Manual logs supplement the application reports by documenting input and associated supervisory approval. These reports and logs should be reviewed by management and reconciled to output.

We noted the following areas where supervisory reviews and reconciliations can and should be improved:

a) Manual Check Logs: The Disbursing Unit utilizes a manual log to account for the manual check numbers used each month and to document supervisory approval for manual checks. We found that:

- For manual accounts payable and trust checks, supervisory approval was not consistently documented on the manual log and in some cases the documented approval was by non-supervisory personnel.
- For manual payroll checks, there was no documentation on the log of the preparer or supervisory approval because the logs did not include columns for such information.

b) Comparison of Manual Check Report vs. Manual Check Log: To ensure only approved manual checks are actually printed by the check printing application, a system report of the output should be reviewed and compared to the manual check log by the Disbursing Unit. This comparison is not being performed.

c) Reconciliation of Manual Check Report (Payroll) vs. CAPS: Creating a manual payroll check does not automatically record the transaction in CAPS; therefore, it is possible to print a manual payroll check without it being recorded in CAPS. The Disbursing Unit does not perform a reconciliation between the manual payroll check reports and CAPS reports to ensure all manual payroll checks created have been entered into CAPS.

d) Queue Report: There is no "traditional" system activity log for the application (see item No. 16 below). In lieu of this, the *Queue Report* is available (shows limited check printing activity for both automated runs and manual checks), but the Disbursing Unit Manager is not reviewing it. Currently, the *Queue Report* can only be run at the EDC. Adding this functionality to the Disbursing Unit workstation requires a system change (see item No. 16 below). However, the *Queue Report* could and should be forwarded by the EDC to the Disbursing Unit.

e) Reconciliation of Automated Check Runs: The ACS production operator performs a three-way reconciliation of the batch count and beginning/ending check numbers between: 1) check data submitted from CAPS (documented on the *Warrant Verification Log)*, 2) actual checks prints, and 3) a check printing application report (*Batch Control Record*) summarizing the automated check run. The ACS production supervisor reviews this reconciliation; however, this review is currently not documented.

   Also, this three-way reconciliation of the automated check run does not compare the total dollar value of the check run. Total dollar value of the run is an important reconciling item to ensure the accuracy and completeness of checks printed.

Failure to review summary reports and document supervisory reviews increases the risk checks could be issued fraudulently or in error and decreases accountability during the check printing process. The supervisory reviews and reconciliations related to manual checks are even more important because of the segregation of duties issues discussed in item No. 2. above.

Recommendation No. 3A: We recommend the Auditor-Controller Disbursing Unit perform the following:

a) Ensure supervisory personnel document their approval of manual checks on the manual check logs and ensure preparers also initial the manual logs.
b) Print and retain manual check reports and compare them to the manual check logs on a periodic basis.
c) Print and retain manual payroll check reports and reconcile them to CAPS on a periodic basis.
d) Ensure supervisory personnel periodically review and document their review of the *Queue Report* for unusual activity.

Auditor-Controller Response: Concur. Auditor-Controller Disbursing Unit will perform the tasks as recommended above.

Recommendation No. 3B: We recommend the Auditor-Controller require CEO/IT to document their supervisory review of the three-way reconciliation for automated check runs on the *Warrant Verification Log.*

Auditor-Controller Response: Concur. EDC will provide Disbursing a report daily for signoff.

Recommendation No. 3C: We also recommend the Auditor-Controller require CEO/IT to balance check batch amounts, along with the check batch quantities, during the three-way reconciliation of automated check runs.

Auditor-Controller Response: Concur. We will request CEO/IT staff to include dollar amounts in the three way reconciliation of automated check runs.

4. Data Encryption and Logical Access to Security Files

A. Data Encryption:

Contemporary check printing applications encrypt check image data, signatures, and bank account information so that only authorized users (key holders) can read the encrypted data. We noted critical database and data files are not encrypted as follows:

- Application database tables containing check archive data and the system activity log.
- Data File: The data file containing bank account information and security data.
- Security Database: The laser check printing application (Disbursing Unit version only) does not contain commonly found access control features such as multiple user I/Ds (see item No. 16 below). As a work around, the vendor created a database that allows multiple user I/Ds and the ability to create security profiles for each user I/D. This database is not encrypted.

B. Logical Access to Files:

- Data File: Logical access controls for the data file containing bank account information and security data are not established to prevent unauthorized access. Therefore, any user with logical access to the check printing server could access the file. Additionally, because unauthorized intranet hosts could potentially access the laser check printing subnet (as discussed in item 1.above), with proper knowledge these unauthorized intranet hosts would be able to access this file.
- Security Database: Logical access controls for the security database are not established to prevent unauthorized access. However, even if these logical access controls had been established, they could have been overridden because all of the Disbursing Unit staff were given operating system administrator access privileges (see item No. 5. below).

Without encryption, the risk of alteration to these files is increased. Additionally, weak access controls to unencrypted files magnify this risk.

Recommendation No. 4A: We recommend the Auditor-Controller encrypt database tables and data files that contain sensitive information.

Auditor-Controller Response: Concur, but Unable to Implement. We concur with the recommendation. However, currently we would not be able to support this direction as the County of Orange does not have access to all source code for this application. To comply with this request would require Vendor involvement or obtaining all the source code to support this direction. We are pursuing avenues to obtain the source code.

Recommendation No. 4B: We recommend the Auditor-Controller enable operating system security on the Disbursing Unit workstation to restrict access to folders containing critical data files.

Auditor-Controller Response: Concur. Auditor-Controller will establish security at the folder level on the remote workstation.

Recommendation No. 4C: We recommend the Auditor-Controller require CEO/IT to enable operating system security on the RxLaser servers at the EDC and to restrict access to folders containing critical data files.

Auditor-Controller Response: Concur. We will direct CEO/IT to establish security at the folder level on the server.

5. User Account Administration

Access to an application should be limited based on the user's demonstrated need to view, add, change, or delete data. To access the laser check printing application, users should be assigned user accounts and passwords for the operating system and the laser check printing application.

We noted the following security issues related to user accounts and passwords:

Disbursing Unit:

- All Disbursing Unit staff logged on to the application workstation operating system using the local administrator account.
- One user account was for an employee that no longer needed access to the check printing application.
- The Claims & Disbursing Unit Manager was granted administrator privileges to the laser check printing application.

EDC:

- Three non-administrator operating system user accounts are assigned administrator privileges. All ACS production operators shared one of these accounts.
- Two operating system user accounts are for unknown employees.
- Two operating system user accounts are for employees no longer requiring access.
- The two backup ACS database administrators logged on to the operating system under the primary ACS database administrator's user account and password
- All ACS production operators logged on under a shared user account and password for the application and operating system.

Failure to properly monitor user accounts for appropriateness and granting excessive administrator privileges increases the risk of:

- Incurring data loss from malicious attacks or disgruntled employees.
- Disruption to the laser check printing process.
- Irregularities in the laser check printing database and subsequent improper check creation.

Sharing user accounts and passwords defeats accountability and increases risk.

Recommendation No. 5A: We recommend the Auditor-Controller review Disbursing Unit user privileges for the application and adjust their profiles accordingly, including removing administrator privileges for users not requiring such access. We also recommend that the Auditor-Controller have Disbursing Unit staff log on to the check printing workstation using their respective user accounts.

Auditor-Controller Response: Concur. The remote workstation has been re-configured as follows:

1) Unique Ids have been established at the operating system level for all staff who is authorized to use the application. Specific user groups have been established for user and administrators.
2) Complex passwords have been established.
3) Automated Password Expiration policy of 60 days has been established.
4) Automatic workstation lockout after 5 tries.
5) System will lock out after 5 minutes of non-use. A password will be required to reactivate.

Recommendation No. 5B: We recommend the Auditor-Controller require CEO/IT to review the application server operating system user accounts for appropriateness and adjust account rights accordingly, including removing administrator privileges for users not requiring such access. We also recommend the Auditor-Controller require CEO/IT to create operating system user accounts for each production operator and remove the shared user accounts.

Auditor-Controller Response: Concur. The Auditor-Controller will direct CEO/IT to make changes to the server per the recommendations stated above

Recommendation No. 5C: We recommend the Auditor-Controller require CEO/IT to apply application security features (similar to the Disbursing Unit's version) to the EDC's version so that all ACS production operators are assigned individual user accounts and passwords for the laser check printing application.

Auditor-Controller Response: Concur. EDC production operators have been assigned individual user accounts and passwords for the laser check printing application. Each operator has a unique log on ID and password.

6. Data Back-Up

Part of the back-up strategy for the RxLaser servers includes RAID technology that replicates the database from the primary to the secondary/back-up server each morning following a check run. To ensure the replication occurs and is successful, the ACS database administrator reviews the replication monitor.

On the date of our test work (May 6, 2003), we determined that the RxLaser server replication monitor had not been checked as of 4 p.m. When it was subsequently checked, it was identified that the replication had failed because the secondary/backup server was at capacity (see item No 7. below, data retention). As such, a period of time had passed when there was no back up for the prior evening's check runs.

Discussions with employees responsible for supervising the database replication process indicated there is no formal procedure for ensuring the replication monitor was checked in a timely manner.

In addition, we observed that the replication history log was not enabled. This log should be enabled to provide an audit trail of replications.

Recommendation No. 6A: We recommend the Auditor-Controller require CEO/IT to create a formal procedure that ensures the replication monitor is reviewed at the start of every business day following a check run.

Auditor-Controller Response: Concur. The Auditor–Controller will direct CEO/IT to create a formal procedure to review the replication monitor at the start of every business day following a check run.

Recommendation No. 6B: We also recommend the Auditor-Controller require CEO/IT to enable the replication monitor history log.

Auditor-Controller Response: Concur. The Auditor–Controller will direct CEO/IT to enable the replication history log during check runs.

7. Data Retention

A check reprint is usually performed when a check is destroyed during the printing or envelope "stuffing" process and generally occurs shortly after the original check was printed (within 24 to 48 hours).

We were informed that data to reprint checks was archived for six months, to coincide with the six-month stale dating of a check. The amount of data being retained subsequently caused disk capacity issues during data backup routines on the RxLaser servers.

Retention periods for sensitive data should be set for a minimum period that balances risk with business need. The longer check archive data is retained, the longer it is subject to check reprints and/or alteration. Retaining data to perform check reprints beyond what is necessary increases the risk a check maybe reprinted for improper purposes.

Recommendation No. 7: We recommend the Auditor-Controller evaluate reducing the check archive retention to a shorter period that still meets business needs.

Auditor-Controller Response: Concur. With most of the security controls recommended in this Audit already in place, there are compensating controls to reduce the risk of improper printing of checks. There is also a real business need to have the ability to reprint checks that have not expired. We have had checks presented to us in the past that have been close to the expiration date. To have to cancel the check and re-issue is a lengthy process and would cause clients unnecessary delays and increase the current staff workload. Part of the reason for using laser checks was to be able to provide same day service and eliminate any delays. Additionally, the check file is sent to the bank for Perfect Presentment Positive Pay. If the bank receives a check that has already been cashed, the check is rejected and not paid. Both checks in question are then investigated to see if they are fraudulent. Thus, the risk is balanced with the business need.

8. Safeguarding Blank Check Stock

We noted the following issues pertaining to safeguarding blank check stock:

- Manual Check Stock: At the Disbursing Unit, serial numbers on blank check stock are not recorded when received from the vendor, blank check stock is not logged out when removed from the vault, and there is no periodic inventory of blank check stock.
- Automated Check Stock: Weekly, the EDC Warehouse Manager inventories blank check stock on-hand in the secured cage. Daily, the EDC Shift Operations Manager prepares a calculation of how much check stock should be on-hand based upon received, spoiled, and used quantities. This information is forwarded to the Disbursing Unit; however, the Disbursing Unit was not reconciling this information.
- Access to EDC Check Stock Cage: Check stock at the EDC is located in a locked cage controlled by keycards. During our audit, we noted 24 of 36 access cards with rights to the EDC check stock cage assigned to employees with no business need to access the cage.

Failure to provide proper asset safeguarding practices for blank check stock increases the risk a fraudulent check could be produced.

Recommendation No. 8A: We recommend the Auditor-Controller record blank check stock on hand at the Disbursing Unit, log check stock out when removing it from the secured area, and periodically inventory check stock on hand.

Auditor-Controller Response: Concur. The disbursing unit will log all blank stock on hand and periodically inventory the stock.

Recommendation No. 8B: We recommend the Auditor-Controller reconcile the EDC's reports of physical counts of check stock on-hand to calculated on-hand quantities, investigating any differences when necessary.

Auditor-Controller Response: Concur. The Auditor-Controller will reconcile the check stock inventory and check usage to the calculated amounts of checks used per the daily checks printed report from CAPS.

Recommendation No. 8C: We recommend the Auditor-Controller require CEO/IT to remove all rights from the EDC's access control system for persons that do not require access to the check stock cage.

Auditor-Controller Response: Concur. The EDC has reviewed the access levels and has made the changes necessary to secure the cage. A restricted access zone has been established for the access control system allowing only those with need to enter the check stock cage.

9. Password Administration

A password is required to reprint a check in the check printing database. Production operators and daytime control room staff at the EDC, as well as four non-supervisory Disbursing Unit personnel knew the password for check reprinting.

We were informed the check reprint password was shared amid non-supervisory personnel to expedite the check reprint process.

The sharing of the check reprint password circumvents proper security administration and allows non-supervisory personnel to reprint checks without supervisory oversight. Sharing of the check reprint password increases the risk a check could be reprinted for improper purposes.

Recommendation No. 9: We recommend that Auditor-Controller request the check reprint password be changed and ensure that it is only shared amid supervisory personnel.

Auditor-Controller Response: Concur. The EDC will change the reprint password and allow only the supervisors to manage reprints. In addition, a process to record all reprint activity will be implemented.

Since the workstation at the Auditor-Controller's office is used almost exclusively for reprints, the reprint password will be known to staff authorized to perform reprints. The reprint password can be changed upon request either by 2 CEO/IT support staff or the by the Auditor-Controller LSA and backup.

10. Operating System Account Policies

When operating system account policies are left at default settings, logical access controls are not adequate and audit trails are not established.

Operating system account polices for the RxLaser server at the EDC were left at default settings and therefore, are not adequately set. Additionally, certain operating system account policies at the domain controller for the check printing application workstation in the Disbursing Unit are not enabled. We observed:

- EDC: On the RxLaser server, security policies are at default settings for password policies (no requirements), account lockout (disabled), and auditing (no auditing).
- EDC and Disbursing Unit: All user account log on passwords are set to never expire.
- Disbursing Unit: On the local domain controller, password complexity requirements are disabled, auditing was not enabled, and valid log on hours are not established.
- Disbursing Unit: While not an operating system account policy, the local setting at the check printing application workstation was not set to automatically lockout after a period of user inactivity.

Recommendation No. 10: We recommend the Auditor-Controller and CEO/IT set operating system account policies and local security settings to appropriate parameters including password expiration and complexity, enabling security auditing for selected events, and automatic workstation lockout.

Auditor-Controller Response: Concur. The remote workstation has been re-configured as follows:

1) Unique Ids have been established at the operating system level for all staff who is authorized to use the application. Specific user groups have been established for user and administrators.
2) Complex passwords have been established.
3) Automated Password Expiration policy of 60 days has been established.
4) Automatic workstation lockout after 5 tries.
5) Screen saver lockout after 5 minutes. Password required for re-entry.

The Auditor-Controller will direct the CEO/IT to institute the same changes at the server.

11. Server Administrator

There was no system administrator assigned to the RxLaser servers. With no assigned administrator for the servers, the risk of inappropriate user privileges being granted is increased.

The lack of an assigned system administrator with responsibility for the RxLaser servers may have contributed to other issues identified in items No. 5 and 10 above relating to management of user accounts, passwords, and operating system account policies.

Recommendation No. 11: We recommend the Auditor-Controller require CEO/IT to assign a system administrator for the RxLaser servers.

Auditor-Controller Response: Concur. An administrator has been identified. A responsibility matrix is being developed and will be published to support staff.

12. Application Controls

We noted the following weaknesses in the laser check printing application controls:

- At the EDC, a test network printer function in the laser check printing application prints the authorizing signature on the test page.
- Application controls do not prevent issuing checks payable to cash.

In order to make these changes, the A-C and CEO/IT will either have to obtain the complete source code and have ACS make the changes or request the vendor to make the changes. This may be a difficult option considering the vendor contract compliance issues that exist as discussed in item No. 16 below.

Recommendation No. 12: We recommend the Auditor-Controller consider implementing changes to the laser check printing application that prevent the printing of the authorized signature on test pages and prevent issuing checks payable solely to cash.

Auditor-Controller Response: Concur. The development application already prints "Not Negotiable" in the signature block for test checks. This was implemented shortly after the production laser checks were implemented. Checks printed at the EDC as a final test will have the signature. This is required to ensure that the check print parameters in the production application are production parameters. It is not possible to change the EDC printer test pages without negatively impacting the production check print process.

All edits for payee names are controlled within AFNS. There is a permanent audit trail in AFNS for all payee names associated with checks.

We will explore the possibility of developing an audits report identifying any checks payable to "Cash" which could then be verified against both the Financial and Payroll Systems.

13. Change Controls

Certain development procedures are not adequate and were not consistently followed. We observed the following:

- When one of the RxLaser servers was replaced, the current version of the laser check printing application was not loaded.
- When changes are made to the printer flash memory module, the ACS production support department sends the new module to the ACS development area with the authorizing signature. The ACS production support department should remove the signature before sending the module.
- The A-C and ACS did not consistently approve changes to the laser check printing application in writing.

Properly developed change control procedures reduce the risk of installing incorrect software versions or software that has not been adequately tested. Reducing the locations that possess the authorizing signature increases the difficulty to improperly create a check.

Recommendation No. 13A: We recommend the Auditor-Controller require CEO/IT to implement procedures to ensure the correct version of the laser check application is used for all updates and re-loads.

Auditor-Controller Response: Concur. We will direct CEO/IT to develop the appropriate procedures.

Recommendation No. 13B: We also recommend the Auditor-Controller and CEO/IT approve all changes to the laser check printing application in writing.

Auditor-Controller Response: Concur. The recommendation is already being followed. Changes to the application are documented using the Requirements Definition Document (RDD) which is submitted to CSD for design and development. Approvals for all requirements and implementation are provided in writing. This is consistent with CMM methodology which has been adopted by the EDC. The Request for Technical Change (RTC) process is used for approval of implementation.

Recommendation No. 13C: We also recommend the Auditor-Controller require CEO/IT to ensure the ACS production support department removes the signatures on printer flash memory modules prior to submission to the ACS development area.

Auditor-Controller Response: Concur. The recommendation is already being followed. Procedures have been developed, documented and implemented to remove the signature from memory modules prior to submission to Development. The development application prints "Not Negotiable" in the signature block for test checks. This was implemented shortly after the production laser checks were implemented. Checks printed at the EDC as a final test will have the signature. This is required to ensure that the check print parameters in the production application are production parameters.

14. Audit Trails

A log of checks printed from the laser check printing application *(Daily Report)* is not being generated. In lieu of this, the A-C relies on a CAPS report of checks submitted to the application for printing.

Without a check log from the application, there is no audit trail showing proof of what checks were actually printed. The check log can be compared to the accounting system (CAPS) to ensure no alterations were made to check data after submission to the laser check printing application.

Recommendation No. 14: We recommend the Auditor-Controller print or electronically archive the *Daily Report* for all checks printed and retain it in accordance with County record retention policies.

Auditor-Controller Response: Concur. We will add verifying the Daily Report from the laser print application to the Check Register but will not print out the report due to the length of the report. We will verify this on-line and initial on the Check Register that it has been agreed to the Daily Report.

15. Policies and Procedures

Policies and procedures for the laser check printing process are not documented as follows:

- Normal Check Processing: There are no documented policies and procedures for the printing and reprinting of checks (circumstances, approvals required), supervisory review of reports, and storing and accounting for blank check stock.
- Disaster Recovery: There are no documented policies and procedures for disaster recovery including how to print checks, and recovering the database and check printing application in the event of a disaster.

Undocumented procedures for normal check processing could result in differing check printing methodologies between production staff. Failure to properly document business continuity procedures could result in unacceptable delays in operations during a disaster.

Recommendation No. 15: We recommend the Auditor-Controller and CEO/IT prepare written policies and procedures for normal and emergency check processing.

Auditor-Controller Response: Concur. The EDC is in the process of developing a Standard Operating Procedure for the Laser check system. Auditor-Controller is in process of preparing an operating procedure as well as a disaster recovery procedure.

Our audit scope did not cover compliance with the vendor contract; however, during our audit we became aware of the following contractual issues:

16. Vendor Contractual Compliance

The County has had a number of vendor support issues and contractual non-compliance since the laser check printing application and process was deployed:

- Access Control Features: Attachment B – Scope of Services, Item K. of the contract states "Contractor provides a full range of security options." While not explicitly stated in the contract, we noted the laser check printing application does not contain commonly found security options that would be expected for an application of this nature such as: multiple user I/D's (EDC employees share one user account), forced password changes (passwords never expire), minimum password length parameters (no minimum), controls over manual check printing (not password controlled), and unsuccessful log on lockout (unsuccessful log on attempts never lockout). Additionally, the application does not utilize any form of data encryption.

- Report Capabilities: Attachment B – Scope of Services, Item P, of the contract states the "Contractor shall provide an ad-hoc reporting facility for all checks stored in the Contractor database repository.... Contractor shall also produce security profile reports as well as user usage tracking, user logins, time logged on and logouts." The laser check printing application's reports did not include the below capabilities as required:

  a) Reports did not establish accountability by identifying users with associated transactions,
  b) There is no system activity log that shows audit information such as users logging on and off of the application and reprint jobs run.

  Also, while not explicitly stated in the contract, the laser check printing application's reports did not include the below report capability that would be expected:

  c) The check *Reprint Register* can only summarize checks reprinted based upon the original check issuance date, and not the date the check was reprinted. Having the *Reprint Register* summarized by the date of check reprint is needed for appropriate supervisory oversight.

- Source Script: Attachment F – Software Licensing & Support, Item B, of the contract states the "Contractor shall provide County the source script and all documentation necessary to program in this script language." As of our audit, the vendor has not provided all of the source script to the County.

- Dual Signature Capability: Attachment B – Scope of Services, Item L, of the contract states "The SYSTEM shall provide for dual signatures on specified classes of checks...Additionally, the SYSTEM must have the ability to sort/special handle those checks requiring two signatures." We noted the laser check printing application does not provide such functionality as Disbursing Unit staff must manually run a report of checks that require a second signature and then manually remove these checks from the check batch.

- Vendor Support: Attachment E - Hardware Maintenance Services, of the contract states the vendor is to provide for problem resolution and escalation, a "Minimum of 2-hour service response, 24-hours per day, 7-days a week, 365-days per year" and a "...toll free contact for hardware maintenance." We were informed the vendor was not consistently responsive to the County's service requests and was available only during normal business hours.

Recommendation No. 16: We recommend the A-C and the CEO/IT pursue contractual remedies against the vendor for specific performance in the areas of access control features, report capabilities, access to application source script, dual signature capability, and vendor support.

Auditor-Controller Response: Concur. CEO/IT is pursuing contractual remedies with the assistance of CEO Purchasing and County Counsel.

ATTACHMENT: Auditor-Controller Response

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.oc.ca.gov/ac

DAVID E. SUNDSTROM, CPA
AUDITOR-CONTROLLER

JOHN H. NAKANE
CHIEF ASSISTANT AUDITOR-CONTROLLER

JAMES M. McCONNELL
ASSISTANT AUDITOR-CONTROLLER
CENTRAL OPERATIONS

SHAUN M. SKELLY
ASSISTANT AUDITOR-CONTROLLER
AGENCY ACCOUNTING

MAHESH N. PATEL
ASSISTANT AUDITOR-CONTROLLER
INFORMATION TECHNOLOGY

RECEIVED
SEP 17 2003
INTERNAL AUDIT
DEPARTMENT

September 16, 2003

TO: Dr. Peter Hughes, Director, Internal Audit Department

SUBJECT: Information Technology Audit Report for Laser Check Printing

We have reviewed the report prepared by the Internal Audit Department covering their review of Auditor-Controller Laser Check Printing as of March 31, 2003, Audit No. 2326.

We concur with the recommendations made in the Internal Audit report. Our responses to the recommendations are contained in the attachment.

David E. Sundstrom
Auditor-Controller

/lr
Attachment

ATTACHMENT: Auditor-Controller Response (continued)

Distribution of copies:

Auditor-Controller
Mahesh Patel
John Nakane
Jim McConnell
Shaun Skelly
Bob Leblow
Jim Berch
Ray Stephens
Virginia Czarnecki

Internal Audit
Eli Littner
Scott Suzuki
Autumn McKinney

CEO-IT
Dan Hatton
Reza Khayyami
Ted Kerekes
Robert Connal

ACS
KC Roestenberg
Phil Paker
John Woolery
Phillip Daigneau
Scott Spafford
Mary Lou Wencloff

ATTACHMENT: Auditor-Controller Response (continued)

LASER CHECK PRINTING AUDIT

1. Application Server Security – EDC

Recommendation No. 1: We recommend that the Auditor-Controller immediately direct the CEO/IT to properly define router ACLs to ensure only authorized network hosts have access to the laser check printing subnet.

Auditor-Controller Response:

Concur:

Network Services Division has restricted the RXLaser environment to: Auditor Controller network; AS&P network; Enterprise Data Center network; St Andrews Network; IBM Mainframe; Insight Manager for monitoring, and a Enterprise Data Center backup server per the list provided by the RXLaser administration team. NSD has further tested these ACL's and have confirmed operation.

2. Duties Segregation – Disbursing Unit

Recommendation No. 2: We recommend the Auditor-Controller evaluate separating duties within the manual check process to the extent possible. If separation is not possible, the Auditor-Controller should ensure its supervisory reviews and reconciliations (discussed further in item No. 3. below) are sufficient.

Auditor-Controller Response:

Concur.

The Auditor-Controller will evaluate options to ensure its supervisory reviews and reconciliations are sufficient.

3. Supervisory Reviews and Reconciliation

Recommendation No. 3A: We recommend the Auditor-Controller Disbursing Unit perform the following:

a) Ensure supervisory personnel document their approval of manual checks on the manual check logs and ensure preparers also initial the manual logs.
b) Print and retain manual check reports and compare them to the manual check logs on a periodic basis.
c) Print and retain manual payroll check reports and reconcile them to CAPS on a periodic basis.
d) Ensure supervisory personnel periodically review and document their review of the *Queue Report* for unusual activity.

Auditor-Controller Response:

Concur.

Auditor-Controller Disbursing Unit will perform the tasks as recommended above.

ATTACHMENT: Auditor-Controller Response (continued)

Recommendation No. 3B: We recommend the Auditor-Controller require CEO/IT to document their supervisory review of the three-way reconciliation for automated check runs on the *Warrant Verification Log.*

Auditor-Controller Response:

Concur.

EDC will provide Disbursing a report daily for signoff.

Recommendation No. 3C: We also recommend the Auditor-Controller require CEO/IT to balance check batch amounts, along with the check batch quantities, during the three-way reconciliation of automated check runs.

Auditor-Controller Response:

Concur.

We will request CEO/IT staff to include dollar amounts in the three way reconciliation of automated check runs.

4. Data Encryption and Logical Access to Security Files

Recommendation No. 4A: We recommend the Auditor-Controller encrypt database tables and data files that contain sensitive information.

Auditor-Controller Response:

Concur, but Unable to Implement.

We concur with the recommendation. However, currently we would not be able to support this direction as the County of Orange does not have access to all source code for this application. To comply with this request would require Vendor involvement or obtaining all the source code to support this direction. We are pursuing avenues to obtain the source code.

Recommendation No. 4B: We recommend the Auditor-Controller enable operating system security on the Disbursing Unit workstation to restrict access to folders containing critical data files.

Auditor-Controller Response:

Concur.

Auditor-Controller will establish security at the folder level on the remote workstation.

Recommendation No. 4C: We recommend the Auditor-Controller require CEO/IT to enable operating system security on the RxLaser servers at the EDC and to restrict access to folders containing critical data files.

ATTACHMENT: Auditor-Controller Response (continued)

Auditor-Controller Response:

Concur.

We will direct CEO/IT to establish security at the folder level on the server.

5. User Account Administration

Recommendation No. 5A: We recommend the Auditor-Controller review Disbursing Unit user privileges for the application and adjust their profiles accordingly, including removing administrator privileges for users not requiring such access. We also recommend that the Auditor-Controller have Disbursing Unit staff log on to the check printing workstation using their respective user accounts.

Auditor-Controller Response:

Concur.

The remote workstation has been re-configured as follows:

1) Unique Ids have been established at the operating system level for all staff who is authorized to use the application. Specific user groups have been established for user and administrators.
2) Complex passwords have been established.
3) Automated Password Expiration policy of 60 days has been established.
4) Automatic workstation lockout after 5 tries.
5) System will lock out after 5 minutes of non-use. A password will be required to reactivate.

Recommendation No. 5B: We recommend the Auditor-Controller require CEO/IT to review the application server operating system user accounts for appropriateness and adjust account rights accordingly, including removing administrator privileges for users not requiring such access. We also recommend the Auditor-Controller require CEO/IT to create operating system user accounts for each production operator and remove the shared user accounts.

Auditor-Controller Response:

Concur.

The Auditor-Controller will direct CEO/IT to make changes to the server per the recommendations stated above

Recommendation No. 5C: We recommend the Auditor-Controller require CEO/IT to apply application security features (similar to the Disbursing Unit's version) to the EDC's version so that all production operators are assigned individual user accounts and passwords for the laser check printing application.

ATTACHMENT: Auditor-Controller Response (continued)

Auditor-Controller Response:

Concur.

EDC production operators have been assigned individual user accounts and passwords for the laser check printing application. Each operator has a unique log on ID and password.

6. Data Back-Up – EDC

Recommendation No. 6A: We recommend the Auditor-Controller require CEO/IT to create a formal procedure that ensures the replication monitor is reviewed at the start of every business day following a check run.

Auditor-Controller Response:

Concur.

The Auditor–Controller will direct CEO/IT to create a formal procedure to review the replication monitor at the start of every business day following a check run.

Recommendation No. 6B: We also recommend the Auditor-Controller require CEO/IT to enable the replication monitor history log.

Auditor-Controller Response:

Concur.

The Auditor–Controller will direct CEO/IT to enable the replication history log during check runs

7. Data Retention

Recommendation No. 7: We recommend the Auditor-Controller evaluate reducing the check archive retention to a shorter period that still meets business needs.

Auditor-Controller Response:

Concur.

With most of the security controls recommended in this Audit already in place, there are compensating controls to reduce the risk of improper printing of checks. There is also a real business need to have the ability to reprint checks that have not expired. We have had checks presented to us in the past that have been close to the expiration date. To have to cancel the check and re-issue is a lengthy process and would cause clients unnecessary delays and increase the current staff workload. Part of the reason for using laser checks was to be able to provide same day service and eliminate any delays. Additionally, the check file is sent to the bank for Perfect Presentment Positive Pay. If the bank receives a check that has already been cashed, the check is rejected and not paid. Both checks in question are then investigated to see if they are fraudulent. Thus, the risk is balanced with the business need.

ATTACHMENT: Auditor-Controller Response (continued)

8. Safeguarding Blank Check Stock

Recommendation No. 8A: We recommend the Auditor-Controller record blank check stock on hand at the Disbursing Unit, log check stock out when removing it from the the secured area, and periodically inventory check stock on hand.

Auditor-Controller Response:

Concur.

The disbursing unit will log all blank stock on hand and periodically inventory the stock.

Recommendation No. 8B: We recommend the Auditor-Controller reconcile the EDC's reports of physical counts of check stock on-hand to calculated on-hand quantities, investigating any differences when necessary.

Auditor-Controller Response:

Concur.

The Auditor-Controller will reconcile the check stock inventory and check usage to the calculated amounts of checks used per the daily checks printed report from CAPS.

Recommendation No. 8C: We recommend the Auditor-Controller require CEO/IT to remove all rights from the EDC's access control system for persons that do not require access to the check stock cage.

Auditor-Controller Response:

Concur.

The EDC has reviewed the access levels and has made the changes necessary to secure the cage. A restricted access zone has been established for the access control system allowing only those with need to enter the check stock cage.

9. Password Administration

Recommendation No. 9: We recommend that Auditor-Controller request the check reprint password be changed and ensure that it is only shared amid supervisory personnel.

Auditor-Controller Response:

Concur.

The EDC will change the reprint password and allow only the supervisors to manage reprints. In addition, a process to record all reprint activity will be implemented.

Since the workstation at the Auditor-Controller's office is used almost exclusively for reprints, the reprint password will be known to staff authorized to perform reprints. The reprint password can be changed upon request either by 2 CEO/IT support staff or the by the Auditor-Controller LSA and backup.

ATTACHMENT: Auditor-Controller Response (continued)

10. Operating System Account Policies

Recommendation No. 10: We recommend the Auditor-Controller and CEO/IT set operating system account policies and local security settings to appropriate parameters including password expiration and complexity, enabling security auditing for selected events, and automatic workstation lockout.

Auditor-Controller Response:

Concur.

The remote workstation has been re-configured as follows:

1) Unique Ids have been established at the operating system level for all staff who is authorized to use the application. Specific user groups have been established for user and administrators.
2) Complex passwords have been established.
3) Automated Password Expiration policy of 60 days has been established.
4) Automatic workstation lockout after 5 tries .
5) Screen saver lockout after 5 minutes. Password required for re-entry.

The Auditor-Controller will direct the CEO/IT to institute the same changes at the server.

11. Server Administrator – EDC

Recommendation No. 11: We recommend the Auditor-Controller require CEO/IT to assign a system administrator for the RxLaser servers.

Auditor-Controller Response:

Concur.

An administrator has been identified. A responsibility matrix is being developed and will be published to support staff.

12. Application Controls

Recommendation No. 12: We recommend the Auditor-Controller consider implementing changes to the laser check printing application that prevent the printing of the authorized signature on test pages and prevent issuing checks payable solely to cash.

Auditor-Controller Response:

Concur.

The development application already prints "Not Negotiable" in the signature block for test checks. This was implemented shortly after the production laser checks were implemented. Checks printed at the EDC as a final test will have the signature. This is required to ensure that the check print parameters in the production application are production parameters. It is not possible to change the EDC printer test pages without negatively impacting the production check print process.

ATTACHMENT: Auditor-Controller Response (continued)

All edits for payee names are controlled within AFNS. There is a permanent audit trail in AFNS for all payee names associated with checks.

We will explore the possibility of developing an audits report identifying any checks payable to "Cash" which could then be verified against both the Financial and Payroll Systems.

13. Change Controls – EDC

Recommendation No. 13A: We recommend the Auditor-Controller require CEO/IT to implement procedures to ensure the correct version of the laser check application is used for all updates and re-loads.

Auditor-Controller Response:

Concur:

We will direct CEO/IT to develop the appropriate procedures.

Recommendation No. 13B: We also recommend the Auditor-Controller and CEO/IT approve all changes to the laser check printing application in writing.

Auditor-Controller Response:

Concur.

The recommendation is already being followed. Changes to the application are documented using the Requirements Definition Document (RDD) which is submitted to CSD for design and development. Approvals for all requirements and implementation are provided in writing. This is consistent with CMM methodology which has been adopted by the EDC. The Request for Technical Change (RTC) process is used for approval of implementation.

Recommendation No. 13C: We also recommend the Auditor-Controller require CEO/IT to ensure the CEO/IT production support department removes the signatures on printer flash memory modules prior to submission to the CEO/IT development area.

Auditor-Controller Response:

Concur.

The recommendation is already being followed. Procedures have been developed, documented and implemented to remove the signature from memory modules prior to submission to Development. The development application prints "Not Negotiable" in the signature block for test checks. This was implemented shortly after the production laser checks were implemented. Checks printed at the EDC as a final test will have the signature. This is required to ensure that the check print parameters in the production application are production parameters.

ATTACHMENT: Auditor-Controller Response (continued)

14. Audit Trails – Disbursing Unit

Recommendation No. 14: We recommend the Auditor-Controller print or electronically archive the *Daily Report* for all checks printed and retain it in accordance with County record retention policies.

Auditor-Controller Response:

Concur.

We will add verifying the Daily Report from the laser print application to the Check Register but will not print out the report due to the length of the report. We will verify this on-line and initial on the Check Register that it has been agreed to the Daily Report.

15. Policies and Procedures

Recommendation No. 15: We recommend the Auditor-Controller and CEO/IT prepare written policies and procedures for normal and emergency check processing.

Auditor-Controller Response:

Concur.

The EDC is in the process of developing a Standard Operating Procedure for the Laser check system. Auditor-Controller is in process of preparing an operating procedure as well as a disaster recovery procedure.

16. Vendor Contractual Compliance

Recommendation No. 16: We recommend the A-C and the CEO/IT pursue contractual remedies against the vendor for specific performance in the areas of access control features, report capabilities, access to application source script, dual signature capability, and vendor support.

Auditor-Controller Response:

Concur.

CEO/IT is pursuing contractual remedies with the assistance of CEO Purchasing and County Counsel.