Reznick Group

SAN DIEGO HOUSING COMMISSION

INTERNAL CONTROL RELATED MATTERS

JUNE 30, 2007

Reznick Group

Reznick Group, P.C.
400 Capitol Mall
Suite 900
Sacramento, CA 95814-4424

Tel: (916) 442-9100
Fax: (916) 442-9103
www.reznickgroup.com

To the Board of Commissioners
San Diego Housing Commission

In planning and performing our audit of the financial statements of San Diego Housing Commission (the Commission) as of and for the year ended June 30, 2007, in accordance with auditing standards generally accepted in the United States of America, we considered the Commission's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Commission's internal control. Accordingly, we do not express an opinion on the effectiveness of the Commission's internal control.

Our consideration of internal control was for the limited purpose described in the first paragraph and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal controls that we consider to be control deficiencies.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

During our audit no material weaknesses were detected.

The following deficiencies were noted during the course of our audit and constitute control deficiencies:

1. It was noted during our audit that the Commission does not book all bank transfers and reconciling items listed on the bank reconciliations in the proper period. It was noted that all adjustments are posted by June 30th in order to reconcile all bank accounts for the year-end audit.

2. It was noted during our audit that partly due to the change in the payroll processing vendor there is a lack of oversight of the processed payroll and a lack of necessary documentation in the employee files. It was noted that the salary pay rate changes are not checked and approved by a supervisor once they are entered into the payroll system. In addition to a lack of review, there was also a lack of documentation or evaluation indicating the eligibility of an increase in the pay step. There was also a lack of documentation in the files of the employee authorized W-4 and direct deposit forms.

3. It was noted during our audit that significant payments were made to vendors that were not selected through a competitive bidding process in accordance with the procurement policy and procedures of the Commission. Even though a single transaction with each of these vendors is significantly below the threshold under which such bidding process is required, the cumulative payments to each vendor during the year exceeded the limits set under the Procurement Policy. It was also noted that vendors where procurement processes were followed the files did not contain history of the procurement process such as, information as to the bids received or an indication of how the selection of the vendor was determined.

4. It was noted during our audit that the Commission has made significant improvements to the information systems. There are still some remaining items regarding the appropriate information security and controls that the Commission did not implement; as result there were some deficiencies in the computer and information system functions surrounding the access controls and segregation of duties, the physical access controls, the contingency planning controls, and the change control methodology. A detail report on the findings and recommendations is attached.

Reznick Group, P.C.

Sacramento, California
March 5, 2008

San Diego Housing Commission FY 2007
Information Technology General Control Deficiencies

Access Controls

1. Access to application data are restricted to authorized personnel, but changes are not monitored and approved by management **(Refer to 2.f)**.

Effect

Without periodic review of changes to data, unauthorized changes could go undetected.

Recommendation

Periodic reviews and approvals of any changes to data should be performed and documented by management.

Management Response

We will implement a formal change approval process in FY 2008. Currently, all changes must be approved by the IT Officer but approval records are not maintained.

2. Notification of requests for new hire access and requests to disable access for termination of personnel is by email from management to the IT department. This email notification does not indicate which systems the users should be granted access to, and once the notice of termination is received in IT, the process does not indicate acknowledgment that the individual's access to the respective systems was revoked **(Refer to 2.h.i)**.

Effect

Lack of proper documentation of approved access granted or disabled access of users increases the risk that unauthorized access to SDHC applications/systems could go undetected.

Recommendation

Requests for new hire access should indicate all applications and systems that the user should be granted access to. Procedures should be implemented to ensure access for terminated individuals is revoked timely.

Management Response

We have implemented 2 additional steps to the access request process. We now require an IT System Access Request form to be filled out prior to granting access to application software. The form identifies the application and security role that the user requires. In addition, we are now creating a confirmation e-mail that access has been revoked for terminated employees.

3. User listings from PeopleSoft, ECS, and LSSI are reviewed by management on an annual basis to confirm that the user's access is still appropriate **(Refer to 2.h.ii)**. However, we observed several user IDs on ECS that had not been used in more than a year. Further, the user listings to critical financial folders stored on the network are not reviewed **(Refer to 2.o)**. This control deficiency was noted in prior year comments, See SDHC FY 2006 Findings and Recommendations, SDHC SYS - 01 #2.

    <u>Effect</u>

    Failure to perform more frequent review of access rights listings to PeopleSoft, ECS, LSSI, and critical financial folders stored on the network increases the risk that unauthorized access to SDHC applications/systems could be compromised and go undetected.

    <u>Recommendation</u>

    Quarterly reviews of current access listings to PeopleSoft, ECS, LSSI, and critical financial folders stored on the network should be performed and signed off by management.

    <u>Management Response</u>

    Based on discussions during and in response to the FY 2006 audit, we implemented the annual review of system access in FY 2007. We will begin quarterly review of access listings in FY 2008.

4. Password change intervals are set to 180 days on all SDHC applications and network, Network passwords are set to 10 login attempts before account lockout, and various ECS users have minimum password settings set to five characters in length although SDHC's policy requires a minimum length of six characters **(Refer to 2.i.ii)**.

    <u>Effect</u>

    Weak password settings increase the risk that unauthorized access to SDHC applications/systems may occur.

    <u>Recommendation</u>

    Strong passwords should include change intervals set to a maximum of 90 days, no more than 3 login attempts before account lockout, and a minimum of 6 characters in length.

    <u>Management Response</u>

    We will make the recommended changes in FY 2008.

Application Development and System Software Controls

5. SDHC does not maintain documented System Development Life Cycle procedures **(Refer to 3.a, 4.a.iii, 5.k)**.

   Effect

   Lack of documented SDLC procedures to guide the implementation of new applications or system software, and/ or changes to existing applications and system software increases the risk of improper design and implementation of applications and system software.

   Recommendation

   Formal documented System Development Life Cycle procedures should be in place and maintained for implementing new SDHC applications and system software, and changes to existing SDHC applications and system software.

   Management Response

   We are developing a System Development Life Cycle procedure in FY 2008.

6. Key system software parameters are not periodically reviewed **(Refer to 4.a.vi)**.

   Effect

   Without periodic reviews of key system software parameters, unauthorized changes, inappropriate use, and unsuitable governance of system resources and processing may go undetected.

   Recommendation

   Management should ensure reviews are periodically performed on key system software parameters.

   Management Response

   Documented periodic management review of parameters will be implemented in FY 2008.

Operational Controls

7. Logs of system administrator activities are not created and maintained for subsequent review and approval by management **(Refer to 5.c)**.

   Effect

   Without record of system administrator’s activities on SDHC systems, unauthorized activity could go undetected.

Recommendation

Automated or manual logs of system administrator activities on SDHC systems should be maintained and reviewed by management.

Management Response

Logs are maintained and reviewed daily but documentation of the review is not maintained. A documented review and approval process will be implemented in FY 2008.

8. Reports are not created and reviewed by management of system failures, restart and recovery, or other unusual activity. Further, SDHC does not have Incident Response polices and procedures documented and in place. This control deficiency was noted in prior year comments, See SDHC FY 2006 Findings and Recommendations, SDHC SYS - 01 #6 **(Refer to 5.d)**.

   Effect

   Without Incident Response administrative regulations and procedures to periodically monitor and report access violations, such as, failed logon attempts, attempts to gain access to sensitive functions, individuals who make numerous attempts to access these critical systems, system failures, restart and recovery, and/or other unusual activity reports increase the risk these system activities could go undetected.

   Recommendation

   Incident Response policies and procedures should be implemented to help track and monitor incidents and document how they were corrected. Management should also perform periodic reviews of system failures, restarts and recoveries, and/or other unusual activities.

   Management Response

   We have begun development of documented Incident Response policies and procedures and will document review by management in FY 2008. Many of the procedures were in place and implemented and are being consolidated in our response matrix. Also, a daily documented review of activity and logs for each server was implemented in FY 2007.

9. Procedures are not in place to monitor system administrator compliance with prescribed operating procedures **(Refer to 5.g)**.

   Effect

   Without review of the system administrators activities, unauthorized use and changes performed by system administrators may go undetected.

Recommendation

Implement procedures to monitor system administrator compliance with prescribed operating procedures.

Management Response

Procedures to document compliance with prescribed operating procedures will be implemented in FY 2008.

10. We noted excessive failures in backing up SDHC data, and no record of the remediation steps taken to correct failed back-ups was maintained **(Refer to 5.h)**.

    Effect

    Without record and review of remediation steps taken to correct failed back-up, these failures to backing up the data could go unnoticed.

    Recommendation

    A log of data back-ups should be maintained noting remediation actions taken, and subsequently reviewed by management.

    Management Response

    Failures noted were for servers no longer in service but not removed from our scheduled back-up jobs. We have corrected this issue and, in addition, will log the remediation action for future errors in our maintenance log.

11. We were informed that periodic security briefings are given to IT personnel on an as needed basis, but no documentation is maintained to support the content of security briefings or provide evidence that these briefings are held **(Refer to 5.j)**.

    Effect

    Without documentation, it is difficult to provide evidence the security briefings take place.

    Recommendation

    Management should implement a process to document that security briefings are given to IT personnel.

    Management Response

    We will document date, time, agenda and attendees of future security briefings beginning in FY 2008.

12. SDHC does not maintain a log of vendor access to their applications **(Refer to 5.m)**.

Effect

Lack of documentation for granting and disabling vendor access to systems increases the risk of unauthorized access to SDHC applications/systems going undetected.

Recommendation

A log documenting when vendor access to SDHC systems was granted and disabled, along with evidence of approval, should be maintained and periodically reviewed by management.

Management Response

A logging process has been created and implemented.

Disaster Recovery/Contingency Planning

13. The SDHC Disaster Recovery Plan is not tested regularly **(Refer to 6.c)**.

Effect

Without periodic testing of the Disaster Recovery Plan to identify potential risks of losing the capability to process, retrieve, and protect information maintained electronically there is an increased risk that the plan may not be sufficient for use in the event of a disaster.

Recommendation

Management should perform periodic testing of the SDHC Disaster Recovery Plan to ensure all contingencies have been addressed and that the plan will work in the event of a disaster.

Management Response

We are planning an update to the SDHC Disaster Recovery Plan during FY 2008 and will include documented testing as part of the process.

14. Routine test restores are not performed of backed-up data **(Refer to 6.d)**.

Effect

Not performing routine test restores to back up data could increase the risk that software copies, master files, and transaction/transaction history files may not be available when needed.

Recommendation

Routine test restores of back up data should be performed and a log of the test restore results should be maintained for subsequent management review.

Management Response

We have begun monthly restore testing of application databases and will document the results. In the past, tests of backed-up data were done regularly as a step in the creation of our testing environment but not documented or maintained.

Prior Year Issues pending resolution

15. Access to the floor of the office building where the server room is located, and separately, the server room is restricted to authorized personnel by card key. However, a visitor log of individuals that access the SDHC server room is not maintained **(Refer to 2.b)**. This control deficiency was noted in prior year comments, See SDHC FY 2006 Findings and Recommendations, SDHC SYS - 02 #4.

Effect

Without a record of who enters the server room, when they entered and for what purpose increases the risk that management may not be aware of unauthorized access to the sever room.

Recommendation

A visitor log of the server room should be maintained that identifies the person, purpose, time in/out, and document that authorized the access.

Management Response

A visitor log exists for the building and access to both the 4th floor and server room are controlled by card key and require a swipe from IT staff. In addition, we are now maintaining a vendor log book in the server room.

SAN DIEGO HOUSING COMMISSIONS RESPONSES

Response to Item 1:

During their review of financial transactions, the auditors found instances of bank wires and reconciling items that were not posted in the proper periods. Although bank reconciliations were done in an accurate and timely manner, some of the adjustments in particular bank accounts carried over for several months before actually being posted to the general ledger. Staff agrees with the auditors' comment and has made changes to departmental work assignments, established written procedures, and communicated performance expectations to ensure consistent and timely entry to the general ledger. The department has implemented additional monitoring at the appropriate level to ensure compliance.

Response to Item 2:

During the course of the audit, the auditors noted a lack of oversight in the payroll area and a lack of required documentation in employee files and/or payroll processing files. At the time, the Financial Services Department was under-staffed and switched payroll contractors for performance issues. Staff agrees with the auditors' comment and has taken steps to address the issues in both the Human Resource and Payroll areas.

The Financial Services department has made changes in departmental work assignments, established written procedures and communicated performance expectations to ensure consistent review and complete documentation of payroll transactions. Specifically, the following changes have been made to ensure an appropriate level of oversight:

1. All changes to the payroll system are listed on a Change Report which is accompanied by supporting documentation. This report is reviewed and signed off by two levels of accounting review.
2. Payroll batch files, generated by the payroll system, as well as supporting documentation are reviewed by an Accounting Supervisor, who gives final authorization to submit the file to the third party payroll provider.

In addition, procedural changes have been implemented in the Human Resources department that address the issue of documentation for changes in pay rates. Previously, and in compliance with the Memorandum of Understanding with the union, step increases were granted automatically for employees receiving a "Meets or Exceeds" annual performance evaluation, and the evaluation was the supporting documentation for the increase. In order not to penalize employees for the supervisor's failure to complete timely evaluations, the MOU also provided for automatic step increases in the absence of a completed evaluation. This action was performed automatically in the previous payroll software system, without the need for human intervention or supporting documentation.

The current system software does not process automatic pay increases. All increases are keyed by Human Resources staff based on hard copy documentation.

Response to Item 3:

The auditors' comments regarding internal control matters involve vendors with aggregate expenditures in excess of levels that would typically require a competitive bidding process. It was also noted that files did not contain the necessary documentation in regards to the procurement process involved in securing the goods or services.

In March 2007 the Housing Commission requested General Counsel to revisit the issue of aggregation in relation to its procurement practices. Counsel's legal opinion dated July 2, 2007 stated that, as long as goods or services procured during a fiscal year from a vendor were varied in scope and or project, the policy for aggregate or cumulative payments was not applicable. Staff monitors all requests for vendor services to ensure that ethical standards, fairness, reasonable cost and accountability are included in the procurement process.

The Housing Commission believes that, based on the Legal Opinion provided that includes references to regulations and statutes supporting the current procurement practice, the Housing Commission has been complying with all requirements. However, in the future the Housing Commission staff will consider the auditors' comments when procuring services from vendors.

Without specifics as to which files did not include certain documentation, it is impossible to completely address the balance of this Item.

Additionally, a control recently instituted is a monthly procurement audit, put in place to ensure full compliance with the law, including the competitive bidding process, complete documentation, and payments to vendors. Also, a Procurement Manual will be completed by August 2008 to complement the newly revised Procurement Policy. This handbook will constitute a guide to ensure that the Housing Commission's purchasing and contracting functions promote administrative standardization and efficiency while at the same time maintain internal control and compliance with applicable statutes and regulations.

Response to Item 4:

Already included in draft.