

AUDIT COMMITTEE

Thursday, September 2, 2010
4:00 PM

Conference Room 157
County Government Center
70 West Hedding Street
San Jose, CA

AGENDA

CALL TO ORDER

1. ROLL CALL

2. PUBLIC PRESENTATIONS:

This portion of the agenda is reserved for persons desiring to address the Committee on any matter not on the agenda. Speakers are limited to 2 minutes. The law does not permit Committee action or extended discussion on any item not on the agenda except under special circumstances. If Committee action is requested, the matter can be placed on a subsequent agenda. All statements that require a response will be referred to staff for reply in writing.

3. ORDERS OF THE DAY

CONSENT AGENDA

- 4. Approve the Regular Meeting Minutes of June 3, 2010.**

REGULAR AGENDA

- 5. ACTION ITEM - Approve exercising the first one-year option to extend the task order contract with Deloitte & Touche, LLP for Auditor General services, for amount not to exceed \$175,000 as specified in the contract. Exercising this option will extend the contract term to January 8, 2012 and increase the maximum contract value to \$525,000.**
- 6. INFORMATION ITEM - Receive the Auditor General's report on the SAP Governance Risk & Compliance (GRC) Segregation of Duties and Sensitive Access Controls Internal Audit.**
- 7. INFORMATION ITEM - Review Scope of Work for Annual Financial Audit Services.**

8. ACTION ITEM - Authorize the General Manager to execute a contract with Vavrinek, Trine, Day and Co. to provide financial and compliance audit services to Santa Clara Valley Transportation Authority (VTA) for three years starting July 1, 2011 at a cost of \$375,000 and two additional one-year extensions at a cost of \$125,000 for each year. The total value of the contract for the five year period ending June 30, 2016 is \$625,000.
9. INFORMATION ITEM - Receive an update from Auditor General staff on the status of the audits in the current Internal Audit Work Plan. (Verbal Report)

OTHER ITEMS

10. Items of Concern and Referral to Administration.
11. Review Committee Work Plan. (Burns)
12. Committee Staff Report. (Burns)
13. Chairperson's Report. (Gage)
14. Determine Consent Agenda for the October 7, 2010 Board of Directors Meeting.
15. ANNOUNCEMENTS
16. ADJOURN

NOTE COMMITTEE MEMBERS: In order to establish a quorum for this meeting, members are asked to call the Board Secretary's Office at (408) 321-5680 or E-mail: bd.sec.polling@vta.org before 5:00 p.m. on the day prior to the meeting. Thank you for your cooperation.

In compliance with the Americans with Disabilities Act (ADA), those requiring accommodations or accessible media for this meeting should notify the Board Secretary's Office 48 hours prior to the meeting at (408) 321-5680 or e-mail: board.secretary@vta.org, TDD (408) 321-2330. VTA's Homepage is located on the Web at: <http://www.vta.org/> or visit us on Facebook <http://www.facebook.org/scvta>.

Disclosure of Campaign Contributions to Board Members (Government Code Section 84308) In accordance with Government Code Section 84308, no VTA Board Member shall accept, solicit, or direct a contribution of more than \$250 from any party, or his or her agent, or from any participant, or his or her agent, while a proceeding involving a license, permit, or other entitlement for use is pending before the agency. Any Board Member who has received a contribution within the preceding 12 months in an amount of more than \$250 from a party or from any agent or participant shall disclose that fact on the record of the proceeding and shall not make, participate in making, or in any way

attempt to use his or her official position to influence the decision. A party to a proceeding before VTA shall disclose on the record of the proceeding any contribution in an amount of more than \$250 made within the preceding 12 months by the party, or his or her agent, to any Board Member. No party, or his or her agent, shall make a contribution of more than \$250 to any Board Member during the proceeding and for three months following the date a final decision is rendered by the agency in the proceeding. The foregoing statements are limited in their entirety by the provisions of Section 84308 and parties are urged to consult with their own legal counsel regarding the requirements of the law.

All reports for items on the open meeting agenda are available for review in the Board Secretary's Office, 3331 North First Street, San Jose, California, (408) 321-5680, the Monday, Tuesday, and Wednesday prior to the meeting. This information is available on VTA's website at <http://www.vta.org> and also at the meeting.

**NOTE: THE BOARD OF DIRECTORS MAY ACCEPT, REJECT OR MODIFY
ANY ACTION RECOMMENDED ON THIS AGENDA.**



Date: August 18, 2010
 Current Meeting: September 2, 2010
 Board Meeting: N/A

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
 Audit Committee

THROUGH: N/A

FROM: General Manager, Michael T. Burns

SUBJECT: Exercise First Option Year on Contract with Deloitte & Touche LLP for Auditor General Services

Policy-Related Action: No

Government Code Section 84308 Applies: Yes

ACTION ITEM

RECOMMENDATION:

Approve exercising the first one-year option to extend the task order contract with Deloitte & Touche, LLP for Auditor General services, for amount not to exceed \$175,000 as specified in the contract. Exercising this option will extend the contract term to January 8, 2012 and increase the maximum contract value to \$525,000.

BACKGROUND:

VTA's Auditor General is responsible for developing and recommending the Annual Internal Audit Plan, assigning and managing the audit resources required to conduct each internal audit, and providing audit results and progress reports to the Audit Committee. The Auditor General has a direct reporting relationship to the Audit Committee and an administrative reporting relationship to the General Manager.

In January 2009, the VTA Board of Directors awarded a task order contract to Deloitte & Touche, LLP to provide Auditor General services. The contract was for a two-year term at a maximum value of \$350,000 for the period. The contract also included three additional one-year options at a maximum amount of \$175,000 per year, to be exercised at the sole discretion of VTA. The Board action awarding the contract to Deloitte & Touche, LLP authorized the General Manager to exercise the option years, subject to Audit Committee approval.

DISCUSSION:

The two-year base period of the contract will be completed on January 8, 2011. At this time, the Audit Committee will need to decide whether to exercise one or more of the three available one-year options to extend the contract, or initiate a competitive procurement process to solicit proposals from additional qualified independent certified public accounting (CPA) firms to provide auditor general services and internal auditing services.

Staff recommends that the Audit Committee approve exercising the first one-year option, due to Deloitte & Touche's demonstrated high-quality work and responsiveness to Board and VTA administration concerns. Examples of its high quality work include: (1) developing and recommending goals and objectives for the internal audit program; (2) developing and recommending an annual internal audit plan, which included conducting a risk assessment of potential financial and business risks; and (3) completing four internal audits to date, with a fifth underway:

Internal Audits Completed

1. Security Guard Qualifications & Training
2. Silicon Valley Rapid Transit (SVRT) Project Soft Costs
3. Investment Controls
4. SAP Access Control

Internal Audits Underway

5. SVRT Contract Compliance

The Audit Committee concurred with the risk prioritization and internal audit focus areas, and the both the Audit Committee and the Board approved Deloitte & Touche's recommended FY10 and FY11 Internal Audit Plans. Deloitte & Touche's performance in providing these services has been very good, and all projects have been completed on schedule and within budget.

If the Committee chooses to not to extend the contract with Deloitte & Touche, LLP, government contracting code requires that a competitive procurement process be conducted to select a new vendor for Auditor General services, which would take approximately two to three months to complete. Given that the current contract expires in early January 2011, the competitive procurement process would have to be initiated in September 2010 to ensure that a new CPA firm would be under contract by year end in order to provide uninterrupted Auditor General services to the Board.

ALTERNATIVES:

The Audit Committee could choose to exercise two or all three remaining option years at this time, or it could initiate a competitive procurement process to solicit proposals from additional qualified independent certified public accounting (CPA) firms for auditor general services. It should be noted that this last option does not guarantee that overall costs for a replacement firm would be similar to or less than for the current vendor.

FISCAL IMPACT:

This action would result in approximately \$175,000 of expenditures for the first option year. Funds required for the work performed from January 2011 to June 2011 are available in the FY11 Adopted VTA Transit Enterprise Fund Budget approved by the Board on June 4, 2009. Appropriation for the remainder of the one-year extension will be included in the Recommended FY12 & FY13 Biennial Operating Budget.

Prepared by: Stephen Flynn, Sr. Management Analyst
Memo No. 2736

VTA Auditor General Services
One-Year Contract Extension with Deloitte & Touche, LLP
Effective January 9, 2011

Firm & Location	Contact Name	Role
Deloitte & Touche 50 Fremont Street San Francisco, CA 94105	Greg Thomas	Principal – Auditor General
Deloitte & Touche 225 West Santa Clara St., Suite 600 San Jose, CA 95113	Farah Faruqui, CPA Emily Kwan Sandra Koning	Partner – Project Co-Leader Manager Manager



Date: August 19, 2010
Current Meeting: September 2, 2010
Board Meeting: October 7, 2010

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
Audit Committee

THROUGH: General Manager, Michael T. Burns

FROM: Auditor General, Greg Thomas

SUBJECT: SAP GRC Segregation of Duties and Sensitive Access Controls Internal Audit

FOR INFORMATION ONLY

BACKGROUND:

The VTA Board of Directors in January 2009 approved the contract with Deloitte & Touche, LLP (D&T) to provide Auditor General and internal audit services to VTA.

In June 2009, the Board approved the FY10 Internal Audit Work Plan recommended by the Auditor General. In May 2010, Deloitte & Touche, LLP, in its capacity as VTA's Internal Audit, initiated the fourth item identified in this plan: SAP Access Control (SAP is VTA's enterprise resource planning software). The audit was performed in accordance with the Standards for Consulting Services issued by the American Institute for Certified Public Accountants.

DISCUSSION:

Segregation of duties is an internal control mechanism used in financial and other operations that, via checks and balances, prevents one person from having overall control from initiation to settlement of a transaction or process, in order to reduce the potential for error, misuse or fraud.

The purpose of this internal audit was to conduct a design review of VTA's SAP access controls related to segregation of duties and sensitive or critical access controls. It included assessing the design and configuration of the SAP's Governance Risk & Compliance (GRC) tool recently installed by VTA that reports on segregation of duties conflicts.

Internal Audit completed its review and the results of this audit are presented in Auditor General Report No. 2010-01 (see Attachment A). This report describes the objectives established for this audit, its scope, and the approach used by the internal audit team. The report presents the internal audit team's observations, the risk rating associated with each observation, and the Auditor General's recommendation for addressing each observation. The report also includes

VTA management's response to each observation, and steps that have been or will be taken to address the Auditor General's recommendations.

Overall, the assessment did not identify any significant risk issues. Observations or recommendations were issued on several low-risk items. VTA agreed with these findings, and all recommendations will be implemented by September 15, 2010 except for one, which will be done by November 2011.

Recommendations for improvement contained in this report are presented for the consideration of VTA management, which is solely responsible for the effective implementation of any corrective action plans.

Prepared By: Greg Thomas, Auditor General
Memo No. 2378

AUDITOR GENERAL REPORT No. 2010-01

TO: Chair Audit Committee, Don Gage
Santa Clara Valley Transportation Authority

THROUGH: General Manager, Michael T. Burns

FROM: Greg Thomas, Principal, Deloitte & Touche LLP
Auditor General's Office

DATE: July 27, 2010

**SUBJECT: SAP GRC Segregation of Duties and Sensitive Access Controls
Internal Audit**

Enclosed is our report for the SAP GRC Segregation of Duties and Sensitive Access Controls Design Assessment Audit.

Our internal audit was performed in accordance with the terms of our engagement letter between Santa Clara Valley Transportation Authority (VTA) and Deloitte & Touche LLP for Auditor General Services, Contract No. SO9022 dated January 9, 2009, and in accordance with the Standards for Consulting Services issued by the American Institute of Certified Public Accountants. This report is intended solely for the information and use of VTA's Audit Committee and Management and is not intended to be used by anyone other than these specified parties. Recommendations for improvement are presented for Management's consideration. Management is responsible for the effective implementation of corrective action plans.

Please contact Greg Thomas in the VTA Auditor General's office if you have any questions.

This report is intended solely for the information and internal use of Santa Clara Valley Transportation Authority, and should not be used or relied upon by any other person or entity.

AUDITOR GENERAL REPORT No. 2010-01

SAP GRC Segregation of Duties and Sensitive Access Controls Internal Audit

July 27, 2010

Table of Contents

I. EXECUTIVE SUMMARY	3
II. BACKGROUND	4
III. OBJECTIVE, SCOPE & APPROACH	5
A. Objective	5
B. Scope.....	6
C. Approach	6
IV. RATINGS:	7
V. RESULTS:.....	8
A. Risk Rulesets.....	8
B. Segregation of Duties within the GRC RAR Tool.....	9
C. Policies and Procedures.....	10
VI. GENERAL RECOMENDATIONS:	11
VII. APPENDIX: Abbreviations	11

I. EXECUTIVE SUMMARY

The Santa Clara Valley Transportation Authority (“VTA”) implemented SAP ERP Central Component (ECC) 6.0 and Governance Risk and Compliance (GRC) Access Control 5.3 Suite in July 2009. SAP is an enterprise resource planning (ERP) application designed to coordinate all the resources, information, and activities needed to complete each business processes. GRC Access Control suite within SAP is a tool to control SAP access and authorizations across the enterprise as well as to ensure segregation of duties (SOD) compliance.

Modules being used in the GRC Access Control Suite are as follows:

- Risk Analysis and Remediation (RAR) – utilized for capturing and monitoring SOD conflicts as well as critical access
- Superuser Privilege Management (SPM – was previously known as Firefighter) – utilized for elevated/emergency access

Internal Audit (IA) performed a design review of VTA’s SAP access controls related to SOD and sensitive/critical access. Our scope included assessing the design and configuration of the GRC RAR tool being used for reporting on SOD conflicts. The process included conducting interviews with key VTA personnel; evaluating policies, procedures, and project documents related to SODs and critical transactions; and conducting follow-up interviews and discussing observations with VTA Management prior to issuing a draft report.

Overall, the assessment did not identify any significant risk issues. Observations/recommendations were issued on several low-risk items. VTA agreed with these findings, and all recommendations will be implemented by September 15, 2010 with the exception of one, which will be implemented by November 2011.

Detailed observations and recommendations are provided in the main body of the report in the sections entitled “Risk Rulesets,” “Segregation of Duties within the GRC RAR tool Administration”, and “Policies and Procedures”. To assist the reader, an appendix of abbreviations used throughout the report has been included as the last page. Provided below is a summary of the observations and recommendations in these three areas:

- A. **Risk Rulesets:** The overall risk rulesets pertaining to the Funds Management (FM) and custom transaction codes (Z transaction codes) have not been included in the GRC RAR tool; therefore, SOD conflicts are not currently being reported completely for the VTA’s SAP environment. Management needs to analyze the risks for FM and Z transaction codes, update the GRC SOD risk ruleset, and maintain critical FM and Z transaction codes via the critical transactions table in GRC.

A mitigating factor to the risk was noted; management has considered the FM and Z transaction codes for the built of SAP ECC roles. The built was following SAP best

practices with the approval of the business owners (BPO). Therefore, although the risk rulesets do not currently include FM or Z transaction codes, these transaction codes were built and assigned into the appropriate SAP ECC roles.

- B. Segregation of Duties within the GRC RAR tool Administration:** SOD amongst the owners and approvers of the rulesets within the RAR tool have not been considered. Management should implement SOD of the administration access within the GRC RAR tool.

A mitigating factor to the risk was noted; the Technology team monitors SOD rules and implements changes per approval received from the Division Chief. A report of changes made to GRC-RAR is published and distributed to the BPO for review on a periodic basis, thus mitigating the risk that the Technology team can make changes without approval.

- C. Policies and Procedures:** The VTA Security and GRC policies and procedures were reviewed and appeared to be deficient in describing GRC system change management procedures for risks, rulesets, mitigations and configuration settings. A lack of documented procedures and policies was also found around the SOD process. Management should consider the recommendations to develop a formal set of policies and procedures for the GRC tool as well as for the SOD process (e.g., running jobs, sending SOD reports, reviewing reports, and assessing if actions have been performed). Existing policies and procedures should be reviewed and amended as appropriate.

II. BACKGROUND

The Santa Clara Valley Transportation Authority (“VTA”) implemented SAP ECC 6.0 and GRC Access Control 5.3 Suite in July 2009.

Business processes being used in the SAP ECC system for Finance (FI) and Controlling (CO) areas are as follows:

- Controlling
- Asset Accounting
- Accounts Payable
- Accounts Receivables
- Cash Management
- General Ledger
- Funds Management

This report is intended solely for the information and internal use of Santa Clara Valley Transportation Authority, and should not be used or relied upon by any other person or entity.

Business processes being used in the SAP ECC system for Human Resources (HR) areas are as follows:

- Benefits
- Organizational Management
- Personnel Administration
- Training and Events
- Time Management
- Payroll

The GRC Access Control suite is an integrated set of modules that work across the enterprise. Modules within the suite provide information to document and manage risks and controls in real time. They can help automate controls and thereby minimize the likelihood and impact of risks. The real time overview can give management a point in time snapshot of their SAP security access environment.

Out of the four available modules within the GRC suite – only Risk Analysis and Remediation (RAR) and Superuser Privilege Management (SPM) have been installed and configured at VTA. RAR is used for capturing risks and mitigations as well as for SOD monitoring; SPM is used for elevated or emergency access with proper audit trails.

Segregation of Duties: The SAP ECC system has a total of 984 dialog users spread across several business processes. The RAR tool is being used for maintaining the risk ruleset and for reporting SOD conflicts of these users. The RAR ruleset for business process areas Finance (FI00) and Human Resources (HR00) were in scope for this audit.

The focus of the internal audit was a design assessment of the SOD risk rulesets and the configuration of the RAR tool. The audit procedures included analyzing the SAP RAR tool configurations, assessing how the risks are managed and monitored as well as identifying areas for improvement in the ruleset design and overall SOD process.

III. OBJECTIVE, SCOPE & APPROACH

A. Objective

The objectives of this internal audit of SAP GRC Segregation of Duties and Sensitive Access Controls were to:

- ❖ Gain an understanding of VTA's Finance and HR business processes by reviewing VTA's FI and HR business blueprints and related documentation
- ❖ Evaluate SAP GRC Access Control RAR configuration settings for risk analysis, connectors and master user source per design and per industry leading practice
- ❖ Assess high risk categories of SODs and sensitive access controls design through the review of SAP GRC Access Control implementation documents

- ❖ Evaluate high risk SOD and sensitive access rules configuration against industry leading practices

B. Scope

The scope included a control design assessment in the following areas:

- ❖ RAR tool and risk rulesets between May 26, 2010 to June 11, 2010
- ❖ Design and configuration settings of the GRC RAR tool for SOD and sensitive access
- ❖ In-scope modules:
 - Finance (FI) & Controlling (CO)
 - Funds Management
 - HR-Organization Management
 - HR-Payroll
- ❖ Rules with high risk categorization in the SAP GRC RAR tool
- ❖ Rules at the SAP transaction code level only

The following activities were considered out of scope:

- ❖ Evaluate the effectiveness of SOD and sensitive access controls
- ❖ Review rule sets in the Material Management and Project System modules
- ❖ Assist with remediation activities
- ❖ Assess SOD and Sensitive Access rules that are categorized as medium or low risk

In performing our evaluation, our team reviewed and evaluated the following:

- ❖ VTA Security Setup Documentation
- ❖ VTA Security Administrator Handbook
- ❖ VTA GRC Administrator Handbook
- ❖ VTA Business Blueprints for Finance and HR Business Processes
- ❖ VTA Critical Business Process Matrix (includes critical transaction codes)
- ❖ VTA Customized transactions and reports file

C. Approach

Our team conducted interviews with key VTA personnel during the fieldwork between May 2010 and June 2010. Personnel interviewed were as follows:

- Security and Controls Team: Arun Ramanathan, Brian Fong and Igor Taratutin
- Finance and Controlling Team: Rinky Chopra
- Human Resources Team: Kenneth Mireles and Liusan Yip

Once these interviews were completed, our team evaluated policies and procedures and other project documents related to SODs and critical transactions in the GRC tool.

For the review of the RAR tool configuration settings, our team obtained information on the RAR tool's configuration setting and focused on benchmarking the settings against a set of leading practices.

For the review of the SOD risk rulesets assessment, our team obtained VTA's risk rulesets and focused on benchmarking the rulesets against leading practices to identify risk rulesets or critical transaction codes recommended for regular monitoring.

The team conducted follow-up interviews, as needed, to discuss and confirm observations with VTA Management prior to issuing the draft report.

IV. RATINGS:

Risk ratings have been assigned to each observation to provide VTA Management with a better understanding of the risk and potential impact of each observation. VTA's risk rating definitions are:

- ❖ High – Significant control weakness presents a high likelihood of the event occurring, potentially exposing VTA to significant financial loss, unauthorized access to key data, business or service interruption, and/or an impact to the VTA brand or public perception. This control weakness should be addressed immediately.
- ❖ Medium – Significant control weakness presents a possibility the event will occur potentially exposing VTA to moderate levels of financial loss, short term disruption to operations, short term impact to VTA brand or public perception and/or not making optimal use of human or system resources. This control weakness should be addressed in the near term.
- ❖ Low – Control weakness, if corrected or mitigated, will further strengthen the system of internal control. Likelihood of occurrence and impact if the event did occur are rated as low.
- ❖ Other Opportunities (No Rating) – Opportunity to improve efficiency or profitability of operations, but does not indicate an internal control weakness.

The risk ratings resulting from the work performed are provided in the following as an estimate to help Management understand the overall risk and impacts of all of the observations combined.

An Overall Risk Rating has been provided to help Management understand the overall risk and impacts of all of the observations combined:

Overall Risk Rating: Low

This report is intended solely for the information and internal use of Santa Clara Valley Transportation Authority, and should not be used or relied upon by any other person or entity.

V. RESULTS:

The following sections summarize the internal audit observations, each individual area's risk rating, recommendations from the Auditor General's office, and Management's Response. The results of our field work are delineated below in the sections entitled Risk Rulesets, Segregation of Duties within the GRC tool Administration, and Policies and Procedures.

A. Risk Rulesets

Funds Management (FM)

The FM module within the Finance and Controlling (FI and CO) business process is being used by the budget department at VTA to create master data for funds, cost centers and grants, for uploading, transferring and maintaining approved budgets as well as for performing year-end carry forward budget activities. The budget at VTA is approved by Board of Directors before it is uploaded in SAP in the CO module and then transferred to FM. The Budget Manager is responsible for review and coordination of the upload and transfer of the budget.

Custom (Z) Transaction codes

Transaction codes are command codes utilized by users to perform a task in SAP. There is a standard set of transaction codes derived from SAP; however the need to create custom transaction codes may arise due to the following reasons:

- The standard SAP transaction codes do not support a necessary task or function
- A transaction code needs to be customized to suit the business requirements

Custom transaction codes are typically assigned a naming convention which starts with the letter "Z". An analysis of the total number of custom (Z) transaction codes at VTA showed a total of 231 custom transaction codes which are a combination the following:

- Reports
- Interfaces
- Create/Change/Display type transaction codes

Observation

Based on an evaluation of the existing risk rulesets, we have noted FM and Z transaction codes have not been included in the GRC RAR rulesets as well as in the sensitive transaction code matrix; therefore, potential segregation of duties conflicts and sensitive access issues are not being considered.

A mitigating factor to the risk was noted; management has considered the FM and Z transaction codes for the built of SAP ECC roles. The built was following SAP best practices with the approval of the business owners (BPO). Therefore, although the risk rulesets do not currently include FM or Z transaction codes, these transaction codes were built and assigned into the appropriate SAP ECC roles.

Comments/Recommendations

Based upon our assessment of the risk rulesets, management should consider the following recommendations:

- Management should identify FM and Z transaction codes for the SOD risk rulesets and Sensitive Transaction Matrix.
- Owners, approvers and monitors should be indentified for the risks as well as risk mitigations, if any.
- Management should develop procedures for mitigating identified risk exposures for these transaction codes.
- Management should develop a review program that results in meaningful periodic reviews of custom transaction codes going forward.
- Management should develop procedures for the appropriate provisioning and maintenance of on-going FM or Z transaction codes in SAP.
- Management should develop procedures for mitigating identified risk exposures for the new transaction codes.

Risk Rating: Low

Management Response:

VTA concurs and will implement all of the above recommendations by September 15, 2010.

B. Segregation of Duties within the GRC RAR Tool Administration

The SAP GRC RAR tool provides two risk mitigations:

- It makes deliberate fraud more difficult because it requires the collusion of two or more persons
- It is intended to decrease unintentional errors as no single individual should have end-to-end access rights

Business process and access related SODs are maintained in the SAP system at VTA and the GRC RAR tool is being utilized for monitoring the SOD conflicts. The administration

associated with the SOD risk rulesets should be clearly segregated to help ensure the integrity and accurate maintenance of the RAR tool.

Observation

The design and configuration of the GRC RAR tool was analyzed and it was noted that the administration within the RAR tool was not setup to segregate owners and approvers of the rulesets.

A mitigating factor to the risk was noted; the Technology team monitors SOD rules and implements changes per approval received from the Division Chief. A report of changes made to GRC-RAR is published and distributed to the BPO for review on a periodic basis, thus mitigating the risk that the Technology team can make changes without approval.

Comments/ Recommendations

Management should consider these recommendations:

- Implement SOD rules for risks and mitigation owners, approvers and monitors
- Adopt an established approval process for continuous maintenance of the GRC rulesets.

Risk Rating: Low

Management Response:

VTA concurs and will implement all of the above recommendations by September 15, 2010.

C. Policies and Procedures

Policies and procedures should be established to document the preferred and authorized practice within the organization. Documented policies and procedures help ensure standardization in the business areas.

Observation

Although an informal process is in place, a formalized procedure of managing SAP GRC is lacking. The RAR system change management procedures for risks, rulesets, mitigations and configuration settings have not been formally developed. Also, the overall SOD process has not been formally developed which should include the protocols of identifying responsible parties to: (1) run reports for management on a periodic basis; (2) review SOD reports for appropriateness; (3) ensure mitigating controls are identified for conflicts; (4) provision accounts upon authorized SOD mitigations; and (4) provide continuous monitoring of the SOD conflicts status.

Comments/Recommendations

As a result, management should consider these recommendations:

- Formalize policies related to the GRC process (i.e., identify potential SOD risks and sensitive transaction codes, assign duties, identify change management process, evaluate SOD analysis procedures, etc.)
- Develop formal policies to monitor and manage changes to the SOD process (i.e., monitor and detect changes with SOD functions, actions, permissions, and overall continuous monitoring of SOD analysis). Currently, there is an informal monitoring process in place, but if one person in the process fails to perform a review or approve an activity, then the SOD violations would not be reviewed or corrected in a timely manner.

Risk Rating: Low

Management Response:

VTA concurs and will implement all of the above recommendations by September 15, 2010.

VI. GENERAL RECOMENDATIONS:

- Utilize the critical transaction code table within the GRC RAR tool for more efficient monitoring of sensitive access. Currently the critical transaction code matrix is a manual process dependent on the business process owners and it is not being periodically reviewed for accuracy.
- Migrate the emergency/additional access from Firecall IDs to the GRC SPM tool; (was previously known as GRC Firefighter). This will help ensure an automated process with relevant audit trails.
- Adopt a formalized process to utilize Form G (user creation/modification form) to capture relevant approvals for requesting and granting SAP access.

Management Response:

VTA concurs and will implement the first two recommendations by September 15, 2010. The formalized electronic Form G approval and archiving will be completed by November 2011.

VII. APPENDIX

Listing of Abbreviations Used

BPO	Business process owner
CO	SAP Controlling business process area
ECC	ERP central component
ERP	Enterprise resource planning
FI	SAP Finance business process area
FM	SAP Funds Management business process area
GRC	Governance risk and compliance
HR	SAP Human Resources business process area
IA	Internal Audit
RAR	Risk Analysis and Remediation
SOD	Segregation of duties
SPM	Superuser Privilege Management



Date: August 19, 2010
Current Meeting: September 2, 2010
Board Meeting: N/A

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
Audit Committee

THROUGH: General Manager, Michael T. Burns

FROM: Chief Financial Officer, Joseph T. Smith

SUBJECT: External Financial Auditor Review FY2010 Audit Plan

FOR INFORMATION ONLY

BACKGROUND:

Pursuant to state law and administrative code of the Santa Clara Valley Transportation Authority (VTA), Vavrinek, Trine, Day & Company, LLP was hired as the independent Certified Public Accountant, to conduct the audit of VTA financial statements.

The scope of their services includes the following:

- Conduct the financial statement audit and render an opinion on the:
 - ü VTA General-Purpose Financial Statements
 - ü VTA-Amalgamated Transit Union (ATU) Pension Plan
 - ü VTA's Federal Financial Assistance Program (Single Audit)
 - ü Other Post Employment Benefit Report
- Perform internal control assessment over financial reporting based on the audit of the financial statements
- Perform compliance audit with requirement of the Transportation Development Act
- Perform agreed-upon procedures with regard to the data reported in the VTA's Annual National Transit Database.
- Perform grant-required audits

DISCUSSION:

Vavrinek, Trine, Day and Co. has been VTA's independent external auditor since June 2006. For Fiscal Years 2006, through 2009, they have conducted their audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in the Government Auditing Standards, issued by the Comptroller General of the United States.

Presently, Vavrinek, Trine, Day and Co. is conducting interim work relative to the audit of VTA's financial statements for Fiscal Year 2010. Presented below is their timeline and deliverables relating to this engagement.

April-July 2010

- Tested internal controls in relation to Measure A and Single Audit
- Cash disbursements in relation to Measure A and Single Audit
- Cash receipt sample testing
- Cash disbursement sample testing
- Payroll disbursement sample testing
- Documented procedures in relation to development of VTA's indirect cost allocation

August-October 2010

- Complete Audit field work

November 2010

- Present the 2010 Comprehensive Annual Financial Report along with the VTA-ATU Pension Plan Report, and the Other Post Employment Benefit Report to the Audit Committee on November 4, 2010

Reviewed and verified by: Ali Hudda, Deputy Director of Accounting

Prepared By: Tony Sandhu, Financial Accounting Manager
Memo No. 2380



Date: August 24, 2010
 Current Meeting: September 2, 2010
 Board Meeting: October 7, 2010

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
 Audit Committee

THROUGH: General Manager, Michael T. Burns

FROM: Chief Financial Officer, Joseph T. Smith

SUBJECT: External Audit Services Contract

Policy-Related Action: No

Government Code Section 84308 Applies: Yes

ACTION ITEM

RECOMMENDATION:

Authorize the General Manager to execute a contract with Vavrinek, Trine, Day and Co. to provide financial and compliance audit services to Santa Clara Valley Transportation Authority (VTA) for three years starting July 1, 2011 at a cost of \$375,000 and two additional one-year extensions at a cost of \$125,000 for each year. The total value of the contract for the five year period ending June 30, 2016 is \$625,000.

BACKGROUND:

Section 11-7 of the Administrative Code requires an independent audit of VTA's finances at the close of each fiscal year by a certified public accountant. In addition, VTA's external regulatory agencies such as the Federal Transit Administration (FTA) and the State Controller, as well other entities such as bond counsel require independent audit reports. The following is a list of the reports that are needed to meet these requirements:

- VTA General Purpose Financial Statements
- VTA/ATU Pension Plan Report
- VTA Single Audit Report
- Other Post Employment Benefit Report
- Transportation Development Act Compliance Report
- Federal Transportation Administration Agreed-upon Procedures related to Nation Transit Database

- Grant-required audits

Auditing and reporting services have been performed by Vavrinek, Trine, Day and Co. since May 2006. Their current five-year contract concludes with the audit of fiscal year 2010.

DISCUSSION:

On May 20, 2010, a Request for Proposal (RFP) was issued for Financial External Audit Services. The RFP was sent to eight firms and advertised in the San Jose Post Record and VTA Website. A Pre-proposal conference was held on June 3, 2010. Proposals were received from ten firms.

A selection committee comprised of the Chief Financial Officer, Deputy Director of Accounting, Contracts Administrator, Fiscal Resources Manager and Accounting Manager reviewed the proposals. Review criteria were:

- Qualifications of the firm
- Qualifications of the staff
- Understanding of project requirements
- Local firm preference
- Cost and price

After evaluating the proposals, the selection committee interviewed four firms. The interview with the firms resulted in the following ranking, with number one being the selected vendor:

1. Vavrinek, Trine, Day and Co.
2. Mayer Hoffman McCann
3. Caporicci & Larson
4. Brown Armstrong

Given the complexities inherent in VTA's General Purpose Financial Statements, Vavrinek, Trine, Day and Co.'s professional experience was considered to be a close match to VTA's requirements. Furthermore, their proposal was the lowest cost of the four firms and did not involve any fee contingencies.

The new contract price with Vavrinek, Trine, Day and Co. will result in cost reduction of \$65,000 for the five year period.

ALTERNATIVES:

The Committee could direct staff to issue a new RFP for these services. However, this is not recommended because it is not believed that a new solicitation would result in additional proposers or a lower price.

FISCAL IMPACT:

This action will authorize up to \$625,000 for external financial audit services over the next five years. Funds for the first two years will be included in the FY 2012 & FY 2013 VTA Transit Enterprise Fund Operating Budget. Appropriation for the remaining years will be included in subsequent budgets.

Reviewed and verified by: Ali Hudda, Deputy Director of Accounting

Prepared by: Grace S. Ragni, Fiscal Resources Manager
Memo No. 2613

ATTACHMENT AListing of Consultants
External Audit Services

FIRM	ADDRESS	CONTACT	TITLE
Vavrinek, Trine, Day & Company, LLP	260 Sheridan Avenue, Suite 440, Palo Alto, CA 94306- 2011	Leonard Danna	Engagement Partner



Date: August 24, 2010
Current Meeting: September 2, 2010
Board Meeting: N/A

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
Audit Committee

THROUGH: General Manager, Michael T. Burns

FROM: Auditor General, Greg Thomas

SUBJECT: Review Status of Internal Audit Work Plan

FOR INFORMATION ONLY

VTA's Auditor General is responsible for developing and recommending the Annual Internal Audit Plan, assigning and managing the audit resources required to conduct each internal audit, and providing audit results and progress reports to the Audit Committee.

To keep the members informed, staff from Deloitte & Touche, LLP, the independent auditing firm providing Auditor General services to VTA, will provide reports at each Audit Committee meeting on the current status of the internal audit work plan and its component audits.

Prepared By: Greg Thomas, Auditor General
Memo No. 1896