

AUDIT COMMITTEE

Thursday, May 5, 2011
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 February 3, 2011.**

REGULAR AGENDA

- 5. ACTION ITEM - Review and receive the Auditor General's internal audit report on Information Technology Network Security.**
- 6. ACTION ITEM - Review and receive the Auditor General's follow-up report on the implementation status of management's action plans contained in the SAP Governance Risk and Compliance (GRC) Segregation of Duties (SOD) and Sensitive Access Internal Audit Report.**
- 7. INFORMATION ITEM - Receive an update from Auditor General staff on the status of the audits in the current Internal Audit Work Plan.**

OTHER ITEMS

8. Items of Concern and Referral to Administration.
9. Review Committee Work Plan. (Burns)
10. Committee Staff Report. (Burns)
11. Chairperson's Report. (Herrera)
12. Determine Items for the Consent Agenda for the August 4, 2011 Board of Directors' meeting.
13. **ANNOUNCEMENTS**
14. **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.com/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.**

AUDIT COMMITTEE

Thursday, February 3, 2011

MINUTES

CALL TO ORDER

The Regular Meeting of the Audit Committee was called to order at 4:01 p.m. by Chairperson Herrera in Room 157, County Government Center, 70 West Hedding Street, San Jose, California.

1. ROLL CALL

Attendee Name	Title	Status
Rose Herrera	Chairperson	Present
Sam Liccardo	Member	Present
Chuck Page	Member	Present
Ken Yeager	Vice Chairperson	Absent

A quorum was present.

2. PUBLIC PRESENTATIONS

There were no public presentations.

3. ORDERS OF THE DAY

Chairperson Herrera stated the Chairperson's report would follow Orders of the Day.

M/S/C (Page/Liccardo) to approve the Orders of the Day.

The Agenda was taken out of order.

15. Chairperson's Report

Chairperson Herrera welcomed the members of the public, staff, auditors and her fellow Audit Committee members.

Chairperson Herrera noted her commitment to fiscal responsibility. She stated VTA provides a quality service and it is the responsibility of the Board to ensure that the service is provided in a way that uses the public tax dollars responsibly. Chairperson Herrera reported that she is looking forward to working with both the staff and her colleagues. She stressed the importance of having productive conversations and recognizing individual contributions and roles at VTA.

NOTE: M/S/C MEANS MOTION SECONDED AND CARRIED AND, UNLESS OTHERWISE INDICATED, THE MOTION PASSED UNANIMOUSLY.

Chairperson Herrera stated she has great respect for VTA and the Auditor General staff. She noted everyone involved has a shared commitment to making VTA the best transportation agency that it can be.

CONSENT AGENDA

4. Minutes of November 4, 2010

M/S/C (Page/Liccardo) to approve the Minutes of November 4, 2010.

REGULAR AGENDA

5. Elect Standing Committee Vice Chairperson for 2011

Chairperson Herrera opened the nominations from the floor for the position of Audit Committee Vice Chairperson for 2011.

Member Page nominated Member Yeager to serve as the Vice Chairperson for 2011.

M/S/C (Page/Liccardo) to close the nominations and elect Member Yeager as the Audit Committee Vice Chairperson for 2011.

6. Audit Committee Mission & Responsibilities

Michael T. Burns, General Manager and Staff Liaison, reported, as part of the Hay Group's Organizational Financial Assessment, the recommendation that VTA establish an Audit Committee and hire an Auditor General. Deloitte Touche was subsequently contracted as the Auditor General. The Auditor General has been primarily focused on compliance audits, with performance audits anticipated in the future. Mr. Burns stated VTA's financial audits are conducted by Vavrinek, Trine, Day and Co., LLP and the financial audits will also come before the Audit Committee.

Greg Thomas, Auditor General, Deloitte & Touche, LLP, stated he has been with Deloitte Touche for thirteen years and is working in the San Francisco office. He reported that he leads the Deloitte Touche Risk Service Practice including the internal audit for the State of California.

Mr. Thomas introduced Farah Faruqui, Partner, Deloitte Touche. He noted Ms. Faruqui is located in Deloitte Touche's San José office and is his partner on the VTA account.

On order of Chairperson Herrera and there being no objection, the Committee reviewed the Audit Committee's Mission, Responsibilities and Background.

7. AG Recommended FY12 Internal Audit Work Plan

Mr. Thomas reviewed the Auditor General's Recommended FY12 Internal Audit Work Plan.

Member Page referenced Deloitte Touche's proposed consultative role with regard to

VTA record retention and questioned whether that was the best use of VTA's funding for this project. Mr. Thomas stated Deloitte Touche's expertise and understanding of the rules and regulations allows them to facilitate the project and bring best practices to VTA. He noted his belief that VTA would achieve good savings as the outcome of this project.

Chairperson Herrera stated a need to look at the types of returns achievable on the new performance audits being proposed. She requested that Deloitte & Touche provide this information to the Audit Committee.

Upon inquiry of Chairperson Herrera, Mr. Thomas stated the proposed 300 hours for the Paratransit Program Audit was an educated guess based upon previous experience with contracts of this size and nature.

M/S/C (Page/Liccardo) to approve the following Internal Audit Projects: 1) Proposed Projects: a) Paratransit Program; and b) Fraud Risk Assessment; 2) Required Projects: Investment Controls; and 3) Other Activities: a) Estimated FY12 Audit Follow Up; b) FY13 Risk Assessment Refresh; and c) Auditor General Services Support of the Fiscal Year 2012 (FY12) Internal Audit Work Plan developed and recommended by the VTA Auditor General.

Public Comment

Katie Heatley, Outreach & Escort Inc., stated her belief that the estimated 300 hours for the Paratransit Program Internal Audit Project was too high. Ms. Heatley reported that Outreach is a small, nonprofit organization and suggested some of the money earmarked for the Paratransit Program Audit be reprogrammed.

M/S/C (Liccardo/Page) to approve staff to identify funding for the following Internal Audit Projects: 1) Related Expenses; 2) Recommended Value-Add Projects: a) Efficiency Assessment from Ad-Hoc Financial Recovery Committee; b) IT Organizational Assessment; and c) Record Retention.

8. Auditor General's internal audit report on Investment Controls Design Assessment

Ms. Faruqui provided a brief overview of the Auditor General's internal audit report on Investment Controls Design Assessment.

M/S/C (Liccardo/Page) to review and receive the Auditor General's internal audit report on Investment Controls Design Assessment.

9. SVRT Soft Cost Internal Audit Report

Ms. Faruqui provided the Auditor General's follow-up report.

M/S/C (Page/Liccardo) to review and receive the Auditor General's follow-up report on the implementation status of recommendations contained in the SVRT Soft Cost Internal Audit Report.

10. Investment Controls Effectiveness Audit Follow-up

Ms. Faruqui provided a brief overview of the Investment Controls Effectiveness Audit Follow-up.

M/S/C (Page/Liccardo) to review and receive the Auditor General's follow-up report on the implementation status of recommendations contained in the Investment Controls Effectiveness Testing Internal Audit Report.

11. Review Status of Internal Audit Work Plan

Mr. Thomas provided the status report on the Internal Audit Work Plan.

On order of Chairperson Herrera and there being no objection, the Committee received an update from Auditor General staff on the status of the audits in the current Internal Audit Work Plan.

OTHER ITEMS

12. Items of Concern and Referral to Administration

There were no Items of Concern and Referral to Administration.

13. Review Committee Work Plan

On order of Chairperson Herrera and there being no objection, the Committee reviewed and accepted the revised Committee Work Plan.

14. Committee Staff Report

There was no staff report.

16. Determine Items for the Consent Agenda

Items forwarded to the May 5, 2011, Board of Directors Meeting:

CONSENT

Agenda Item #8. Review and receive the Auditor General's internal audit report on Investment Controls Design Assessment.

Agenda Item #9. Review and receive the Auditor General's follow-up report on the implementation status of recommendations contained in the SVRT Soft Cost Internal Audit Report.

Agenda Item #10. Review and receive the Auditor General's follow-up report on the implementation status of recommendations contained in the Investment Controls Effectiveness Testing Internal Audit Report.

REGULAR

Agenda Item #7. Approve the Fiscal Year 2012 (FY12) Internal Audit Work Plan developed and recommended by the VTA Auditor General.

17. ANNOUNCEMENTS

There were no announcements.

18. ADJOURNMENT

M/S/C (Page/Liccardo) to adjourn the meeting at 4:59 p.m.

Respectfully submitted,

Susan E. Garcia, Board Assistant
VTA Office of the Board Secretary



Date: April 27, 2011
Current Meeting: May 5, 2011
Board Meeting: August 4, 2011

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
Audit Committee

FROM: Auditor General, Greg Thomas

SUBJECT: IT Network Security Internal Audit

Policy-Related Action: No

Government Code Section 84308 Applies: No

ACTION ITEM

RECOMMENDATION:

Review and receive the Auditor General's internal audit report on Information Technology Network Security.

BACKGROUND:

The VTA Board of Directors in January 2009 approved the contract with Deloitte & Touche, LLP 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 December 2010, Deloitte & Touche, LLP, in its capacity as VTA's Internal Auditor, initiated the fourth and last internal audit identified in this plan: IT Network Security.

DISCUSSION:

The purpose of the Network Security Internal Audit was a technical assessment of the security of VTA's networks, networking devices, and server operating systems. It evaluated the network security controls protecting critical network assets from unauthorized access to systems, devices and data and identified specific areas of vulnerability. The audit was performed in accordance with the Standards for Consulting Services issued by the American Institute for Certified Public Accountants.

In April 2011, the Auditor General's Office completed its technical assessment of the security of VTA's networks. The results of this internal audit are presented in Auditor General Report No.

2011-02 (see Attachment A). This report describes in detail the objectives established for this audit, its scope, the approach used and the findings reached by the Auditor General's internal audit team. The report presents the internal audit team's observations, the risk rating associated with each observation as well as an overall risk rating to the VTA organization, and the Auditor General's recommendation for addressing each observation. The report also includes VTA management's response to each observation, and the steps that have or will be taken to address the Auditor General's recommendations.

An overall risk rating of Medium was issued, based on three primary observation categories, two of which were rated Medium Risk and the other High. The report concluded that although VTA had security measures in place and an established plan for hardening, it still has a number of significant vulnerabilities, especially regarding legacy systems and software, and the hardening actions are not sufficiently comprehensive or robust to effectively safeguard the organization's networks, devices and data. It should be noted that VTA has recently implemented significant security improvements, with plans for additional actions in the near future.

VTA agreed with these findings. The one High Risk area was addressed immediately after identification. A portion of the other recommendations are targeted for implementation by September 30, 2011, with the remaining recommendations targeted for implementation by June 15, 2012. Some of the recommendations requiring network equipment replacement are subject to funding availability.

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

Receipt of the report does not indicate that VTA's Board of Directors or Audit Committee agrees with or endorses the findings. Instead, it signifies that the report was provided for their use.

FISCAL IMPACT:

There is no financial impact associated with acceptance of this report.

Prepared by: Greg Thomas, Auditor General
Memo No. 2977

AUDITOR GENERAL REPORT No. 2011-02

TO: Rose Herrera, Chairperson
Audit Committee, VTA Board of Directors

FROM: Greg Thomas, Auditor General
Auditor General's Office

DATE: April 20, 2011

SUBJECT: **Network Security Internal Audit**

Attached is our report for the Network Security Internal Audit.

Our internal audit was performed in accordance with the terms of the agreement between Santa Clara Valley Transportation Authority ("VTA") and Deloitte & Touche LLP ("Deloitte & Touche") for Auditor General Services, Contract No. SO9022 dated January 9, 2009 and its amendment dated March 25, 2011, and in accordance with the Standards for Consulting Services issued by the American Institute of Certified Public Accountants. Our procedures were performed during the month of February, 2011. This report is intended solely for the information and use of VTA's Board of Directors, 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, and management is responsible for the effective implementation of corrective action plans.

Questions or concerns should be addressed to Greg Thomas in the VTA Auditor General's Office at: Auditor.General@VTA.org.

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. 2011-02

Network Security Internal Audit

April 22, 2011

Table of Contents

- I. EXECUTIVE SUMMARY 3
- II. OBJECTIVE, SCOPE & APPROACH 4
 - A. Objective 4
 - B. Scope..... 4
 - C. Approach..... 5
- III. RATINGS: 6
- IV. RESULTS: 7
 - A. Payroll Data 7
 - B. Security Hardening 8
 - C. Network Design 10

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.

I. EXECUTIVE SUMMARY

The network security internal audit was a technical assessment of the security of VTA's networks, networking devices, and server operating systems. It evaluated the network security controls protecting critical network assets and identified specific areas of vulnerability. The scope of our audit consisted of 98 systems and 133 network devices as identified by the VTA Information Technology department ("IT") team.

This internal audit project identified three primary observations.

1. Personally Identifiable Information on an unsecured server
2. Hardening process
3. Network Design

Personally Identifiable Information

Personally Identifiable Information (PII) of VTA personnel from 1996 to 2000 was found on a legacy server, protected by a weak default password.

Hardening Process

Hardening is a method where the security of network devices and servers are strengthened systematically across the network environment. A number of security issues were identified in VTA's legacy server and legacy network environment resulting in the observation that VTA's hardening process was either insufficiently robust or incompletely deployed, which may result in increased security risk:

- Several network devices and systems were using weak passwords which may be publically known on the legacy network.
- Several servers were found to be configured to enable services (such as telnet) that are not being used. Turning off unused and unnecessary services reduces the risk of viruses and security vulnerabilities.
- Several legacy network devices sampled were using a network communication channel that was not protected and can easily reveal username and password credentials.
- There was no audit trail or log to evidence the analysis of why certain security patches were not applied.
- Several fileshares, which are repositories for a collection of files accessible across the VTA network, were misconfigured to allow unauthorized users to access to the files.
- Legacy operating systems (systems that are no longer supported by the vendor and do not receive security patches) are still in production without a plan for migration. This included operating systems (Microsoft Windows 2000) and some old applications (e.g. VMware that is no longer in use).

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.

Network Design

VTA's network does not use network access controls to minimize the potential impact from a security attack. Networks should be segmented with access control to compartmentalize groups of servers which would potentially prevent the spread of viruses and restrict malicious user attacks.

Overall, two additional factors should be noted. First, VTA was undergoing a network transformation moving from a larger network to a smaller, more manageable network that included enhanced security controls. It was noted that the migration was still in progress when Internal Audit performed the testing procedures. Second, the audit scope was limited to the servers and network devices in production as of February 2011, and included systems from the legacy and newer network environments.

In summary, our overall security assessment fell within a **Medium** level of risk exposure to the VTA organization.

This audit report is divided into two sections: (1) the main audit report suitable for public distribution; and (2) the detail section that contains the specifics on the security issues observed and that should not be shared with a wide audience due to the sensitivity of the security issues described and the information contained therein. We have provided a separate appendix containing the technical details behind our observations and recommendations. This appendix contains sensitive information security issues and information, and consequently the distribution of that appendix will be limited solely to VTA IT management only due to the sensitivity of those security issues.

OBJECTIVE, SCOPE & APPROACH

A. Objective

The objectives of this network security internal audit were to evaluate the network security controls protecting critical assets and identify specific areas of vulnerability to external penetration and insecure system configurations within the internal network environment.

B. Scope

The scope was limited to externally accessible VTA networks (networks connected to the Internet or third-party entities) and the internal VTA corporate network and included the following system types:

- ❖ Networking devices (firewalls, routers, switches)
- ❖ Servers at the Operating System level only (e.g., Windows servers)

The following items were considered out of scope:

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.

- ❖ Application security (websites, web servers, financial applications, etc.)
- ❖ Wireless networks
- ❖ Operations networks (e.g. SCADA, rail & bus network, data centers)
- ❖ Third-party systems, devices, and networks
 - Networks and devices owned by third-parties
- ❖ Other security areas not described as in scope above (physical security, disaster recovery, identity and access management, etc.)
- ❖ Denial of Service and social engineering

C. Approach

The internal audit was conducted in three phases, as described below:

Planning Phase:

1. Confirm scope, testing approach, and timing
2. Gather relevant documentation

Assessment Phase:

1. Inspection of documents
 - Documents were collected by VTA
 - Documents were inspected by Deloitte & Touche
 - Documents included the following:
 - a. A sample of network device configurations (firewalls, routers, and switches)
 - b. Network topology maps of the corporate network in San Jose
2. Execution of network and vulnerability scans
 - Network and vulnerability scans were performed by VTA in San Jose
 - Deloitte & Touche did not execute network or vulnerability scans or perform active security testing and only provided consultation on how scans can be executed
 - Network scans limited to lower-risk scans
 - a. Port scans, device fingerprinting (discovery & identification)
 - OS security scans (e.g., Microsoft Baseline Security Analyzer to test for Windows security vulnerabilities and configuration issues) of a sample of servers and systems, such as critical business applications, as well as the base images used to deploy servers and desktops
3. Analysis
 - Analyzed documents, configurations, and scan results for security vulnerabilities

Delivery Phase:

1. Discussed observations with respective groups or departments to assess potential risks associated with identified vulnerabilities.
 - Developed recommendations to address identified vulnerabilities

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.

II. 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 each individual observation.

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

Overall Risk Rating: Medium

III. 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 Payroll Data, Security Hardening, and Network Design.

A. Payroll Data

Sensitive historical payroll data was insecurely protected on a server with a weak password. The sensitive data included current and former VTA employee names, addresses, social security numbers (SSN) and salary information on W-2 documents from 1996 to 2000. Internal Audit observed that the AccuImage server containing the Personally Identifiable Information (PII) was accessible with a shared account with a weak password to access the application and data. Without the use of strong passwords, there is an increased risk for unauthorized access to VTA systems and sensitive data leakage.

Observation Details

- During testing, weak passwords were noted on some devices and systems:
 - AccuImage server with Payroll / W-2 documents from 1996 to 2000 for all VTA employees
 - Information accessible includes name, social security number (SSN), address, salary
 - Noted the use of a shared account to access database containing PII

Comments/Recommendations

Management should consider identifying other sensitive information and evaluating the security of the user accounts used to access those applications. Management should also consider removing unnecessary user accounts that can access the AccuImage server (application, database and operating system) and change the password to require a more complex password for the user accounts that need to access the AccuImage server. A detailed hardening process should include password complexity.

Risk Rating: High

Management Response:

VTA concurs and has already implemented a change in management of the legacy AccuImage server. VTA also agrees to re-evaluate our processes for managing decommissioned devices by July 15, 2011 for implementation by September 30, 2011.

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.

B. Security Hardening

Internal Audit observed several vulnerabilities demonstrating the security hardening process was not sufficiently detailed and not consistently applied across the new and legacy environment.

NOTE: Due to the sensitivity of the devices' names and IP addresses, such information is documented in the separate technical appendix with distribution limited to VTA IT management only.

A security “hardening” process is the act of configuring and enhancing the security controls of a system. The hardening process should apply to applications, databases, operating systems and network devices, at a minimum. Depending on the actual system, the hardening process typically includes securing the following (as applicable):

- Restricting access (access control - e.g. passwords, user accounts, remote access, local accounts)
- Secure network communications
- Applying security patches
- Turning off unnecessary services/features and secure configuration settings

Restricting access

Throughout the security testing, Internal Audit observed examples of missing passwords, weak passwords, and default passwords.

Secure communications

As a result of security testing, Internal Audit observed that system administration can be conducted over insecure communication protocols, such as telnet and http (unencrypted) on some systems. Additionally an application (AccuImage) with sensitive data is using http (unencrypted web) to provide W2 information to the user.

Applying security patches

Several security patches were identified as missing on some Microsoft Windows systems and Cisco IOS networking devices. VTA IT had determined that the security patches were not applicable; however, an audit trail or log documenting the decision to not implement the patches was not available. It was also noted by VTA IT that some of the vulnerabilities for the Cisco networking devices may apply to services or features not enabled on the device (i.e., the vulnerability is applicable to the version of the operating system running, but may relate to features that are not enabled).

Internal Audit observed several instances of legacy systems still in production. These legacy systems include operating systems and applications that are no longer supported by the vendor, which means security patches are no longer provided, but may be vulnerable to security vulnerabilities. It was noted that VTA IT has recently upgraded some networking devices in

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.

2010 (new Cisco networking devices) and has plans to upgrade some legacy Windows systems to newer versions of Windows in the current year.

Turning off unnecessary services or features/configuration

Internal Audit observed servers that are running services that are installed during a default operating system build, but should be removed through the hardening process if not used.

Additionally, Internal Audit observed File Transfer Protocol (FTP) and web (HTTP) services that are running but do not appear to be used. These include FTP services without user access configured (i.e. anonymous FTP) and default web servers containing just the example web page (e.g. default Apache, default Oracle, default Windows IIS web page). Lastly, login banners were inconsistently configured to warn unauthorized users that they are accessing VTA systems.

Comments/Recommendations

Restricting Access

Management should consider creating and implementing an access control/password standard for applications, servers, network devices and databases. The standard should define and enforce a minimum password complexity on all systems and increase access control requirements based on the criticality of the system and role (i.e., administrator).

Although password complexity is just one aspect of access control, Management should also consider a comprehensive hardening process to include other elements of access control, including user account management actions such as disabling/disallowing the use of generic or shared user accounts, default user accounts/passwords and password complexity to mitigate weak passwords.

Management should also consider addressing the password issues identified in the VTA Network Security Audit Observation Detail report, such as default passwords, weak passwords and shared passwords on generic user accounts

Secure communications

Management should evaluate the risk of using administrative access on unsecured network protocols, such as unencrypted web/http and telnet.

Management should consider changing the use of weak administrative password encoding on networking devices and use a stronger form of password encryption.

Management should consider creating a standard for using only encrypted network protocols to protect user credentials (e.g., usernames and passwords) and sensitive data being transmitted over networks.

Applying security patches

Management should consider enhancing and formalizing the current patch management process to include timeframes for evaluating patches, implementation of patches based on risk and tracking any patches that were not implemented on purpose. For any patches not applied,

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.

Management should establish a document to formally track the reasons for not applying the patch (due to issues during testing, acceptable level of risk, etc.).

Management should also consider upgrading or retiring legacy systems and systems running operating system software no longer supported by the vendor.

Turning off unnecessary services or features

Management should establish a standard for defining which services should be enabled or disabled for new servers. Common practice is to only enable the bare minimum set of services and enable more as needed, to reduce potential vulnerabilities.

In summary, Management should consider creating a more detailed security hardening process to more fully include access control, secure communications, patch management, and configuration. Management should also consider more fully implementing other aspects of the security hardening process, such as logging, file/folder permissions and malware management.

Risk Rating: Medium

Management Response:

VTA concurs and will continue to evaluate and implement the above recommendations as both funding for the unsupported legacy equipment becomes available and time permits. VTA will implement a portion of the above recommendations by June 15, 2012. However, additional funding will be required to implement those recommendations requiring hardware or replacement.

VTA has already initiated the process to evaluate specific findings and will update procedures and best practices around these finding by September 30, 2011. To maintain security, VTA will provide the Auditor General's Office a confidential detailed plan of specific changes and completion dates by July 15, 2011.

C. Network Design

VTA's internal corporate network does not implement any internal network access controls. As a result, VTA's internal corporate network acts as one large network from a network security perspective. Without the use of network access controls or network segregation, it may be more difficult to manage and monitor security to sensitive systems and contain security events (e.g., computer virus/botnets/worm outbreaks and other security events).

It was noted that, while there may currently be limited internal network access controls, VTA IT has recently migrated from the use of one very large ("flat") network to smaller, more

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.

manageable, network segments. This transition would make the implementation of internal network access controls possible.

Observation Details

Several large “Class B” networks are used on VTA’s corporate environment with no internal network access controls. Class B refers to the number of systems and devices that could be supported. The more systems within a given network results in greater overall vulnerability. For example, a Class B network can support over 65,535 systems and devices while a Class C network only supports 254. VTA IT has recently adopted the use of smaller, more manageable networks (multiple Class C networks that support around 254 systems and devices).

Comments/Recommendations

Management should consider continuing to migrate off of large Class B networks, if not needed, and implement internal network access controls to protect sensitive servers, facilitate greater ease of administration of network security, and help manage and contain security events. In addition, it should accelerate migration as much as possible to reduce network vulnerability.

Risk Rating: Medium

Management Response:

VTA concurs and will continue to evaluate and implement the above recommendations as both funding for the unsupported legacy equipment becomes available and time permits. VTA will implement a portion of the above recommendations by June 15, 2012. However, additional funding will be required to implement those recommendations requiring hardware replacement.

VTA has already initiated the process to evaluate specific findings and will update procedures and best practices around these findings by September 30, 2011. To maintain security, VTA will provide the Auditor General’s Office a confidential detailed plan of specific changes and completion dates by July 15, 2011.



Date: April 27, 2011
 Current Meeting: May 5, 2011
 Board Meeting: August 4, 2011

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
 Audit Committee

FROM: Auditor General, Greg Thomas

SUBJECT: Follow-up on the SAP GRC Segregation of Duties and Sensitive Access
 Internal Audit Report

Policy-Related Action: No

Government Code Section 84308 Applies: No

ACTION ITEM

RECOMMENDATION:

Review and receive the Auditor General's follow-up report on the implementation status of management's action plans contained in the SAP Governance Risk and Compliance (GRC) Segregation of Duties (SOD) and Sensitive Access Internal Audit Report.

BACKGROUND:

VTA's Auditor General's Office is responsible for conducting the internal audits specified in the Board-approved Internal Audit Work Plan. It is also responsible for determining the implementation status, adequacy and timeliness of corrective actions that VTA management committed to implement on reported observations and recommendations contained in these internal audits.

In July 2010, the Auditor General's Office completed one of the audits contained in the FY10 Internal Audit Work Plan: an assessment of SAP Access Control (SAP is VTA's enterprise resource planning software). 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 Governance Risk & Compliance tool that VTA had recently installed that reports on segregation of duties conflicts.

The resulting SAP GRC Segregation of Duties and Sensitive Access Internal Audit Report did not identify any significant risk issues but did issue observations or recommendations on several low-risk items. VTA agreed with these findings and committed to implement them all by September 15, 2010 except for one, which would be completed by November 2011. This report

was presented and discussed at the September 2010 Audit Committee meeting and received by the VTA Board at its October 2010 meeting.

Recommendations for improvement contained in this report were presented by the Auditor General for consideration by the VTA Board of Directors, Audit Committee and management, which are solely responsible for the effective implementation of any recommendation.

DISCUSSION:

In April 2011, the Auditor General's Office completed its follow-up process to assess if the management action plans specified in the SAP GRC Segregation of Duties and Sensitive Access Controls Internal Audit Report had been completed. The results of this follow-up, as well as a summary of the findings, recommendations and VTA management responses from the subject report, are shown on Attachment A.

Based on the evidence reviewed by the Auditor General, we have verified that the actions plans have been successfully implemented.

Receipt of this follow-up report does not necessarily indicate that the VTA Board, Audit Committee or management agrees with or endorses the findings. Instead, it signifies that the report was provided for their use.

FISCAL IMPACT:

There is no financial impact associated with acceptance of this report.

Prepared by: Greg Thomas, Auditor General
Memo No. 2978



AUDITOR GENERAL FOLLOW-UP REPORT

TO: Rose Herrera, Chairperson
Audit Committee, VTA Board of Directors

FROM: Greg Thomas, Auditor General
Auditor General's Office

SUBJECT: Follow-up on the SAP Segregation of Duties Design Assessment Report

DATE: April 22, 2011

Attached is our report for the Follow-up on the SAP Segregation of Duties (SOD) Design Assessment Report.

Our testing was performed in accordance with the terms of the agreement between Santa Clara Valley Transportation Authority and Deloitte & Touche LLP for Auditor General Services, Contract No. SO9022, dated January 9, 2009 and its amendment dated March 25, 2011; and in accordance with Standards for Consulting Services issued by the American Institute of Certified Public Accountants.

This report containing the remediation status is intended solely for the information and use of VTA's Board of Directors, 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.

Questions or concerns should be addressed to Greg Thomas in the VTA Auditor General's Office at: Auditor.General@VTA.org.

Objective of Follow-up

The purpose of the VTA Auditor General's follow-up on the SAP SOD Design Assessment Report is to determine whether VTA management has successfully implemented the corrective actions it committed to in the Management Response sections of the Report. It is the Auditor General's responsibility to periodically follow up on the status of audit recommendations and report on corrective actions implemented by VTA management.

Background on SAP SOD Design Assessment Report

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

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.

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.

The SAP SOD Design Assessment Internal Audit report was presented and discussed at the September 2010 Audit Committee Meeting and accepted by the VTA Board at its October 2010 meeting. The report concluded that there were areas that VTA management could improve upon with specific observations and recommendations in each area.

Follow-up Findings

In March 2011, the Auditor General's Office obtained evidence from management to assess whether the corrective actions in the SAP SOD Design Assessment Report that VTA management had committed to were completed. Based on this evidence, we have verified that all recommendations have been appropriately completed.

The following table summarizes from the original audit report the Auditor General's observations and recommendations for each key control as well as the corresponding VTA management responses. It also states the implementation status of recommendations agreed to by VTA.

#	Key Control Description	Observation / Recommendation	Management Response	Recommendation Implementation Status
1	Risk Rulesets	<ul style="list-style-type: none"> • Management should identify FM and Z transaction codes for the SOD risk rulesets and Sensitive Transaction Matrix. • Owners, approvers and monitors should be identified 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. 	Concurs with observation and will implement all recommendations	Auditor General's Office: Closed-Verified management has identified FM and Z transaction codes for SOD ruleset and developed policies or approval matrix to address the recommendations noted.
2	Segregation of Duties within the GRC RAR Tool Administration	<ul style="list-style-type: none"> • Implement SOD rules for risks and mitigation owners, approvers and monitors • Adopt an established approval process for continuous maintenance of the GRC rulesets. 	Concurs with observation and will implement all recommendations	Auditor General's Office: Closed-Verified management has identified SOD rules for risk and mitigation owners, approvers and monitors. Further, management has developed an approval process for the management of GRC rulesets.

#	Key Control Description	Observation / Recommendation	Management Response	Recommendation Implementation Status
3	Policies and Procedures	<ul style="list-style-type: none"> 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. 	Concurs with observation and will implement all recommendations	Auditor General's Office: Closed- Verified management has established a policy to monitor the on-going changes to GRC as well as the review of SOD results.
4	General Recommendations	<ul style="list-style-type: none"> 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. 	Concurs with observation and will implement all recommendations	Auditor General's Office: Closed- Verified the critical transactions have been added to the GRC tool. Further verified the usage of Firefighter access through observation of referenced policy. Lastly, management has created Form S and Form, T to standardize the SAP roles and user access change requests.



Date: April 19, 2011
Current Meeting: May 5, 2011
Board Meeting: N/A

BOARD MEMORANDUM

TO: Santa Clara Valley Transportation Authority
Audit Committee

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 selected by the VTA Board of Directors to provide Auditor General services to VTA, provides a report 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



Santa Clara Valley Transportation Authority

May 5, 2011 Audit Committee Meeting

FY2011 Internal Audit Work Plan Status Update

Auditor General's Office

Greg Thomas, Principal

Farah Faruqui, Partner

Sandra Koning, Manager

Emily Kwan, Manager

Internal Audit Plan for FY2011

Audit Project	Description	Timing*	Type of Audit	Risk Area
SVRT Contract Compliance	Conduct an assessment of the contract between Hatch-Mott MacDonald/Bechtel and VTA; evaluate how the contracts are organized and if there are clear deliverables and milestones enforced.	Q2 2011	Compliance Audit/ Value-Add Audit	SVRT
Investment Control Design Assessment	Evaluate the existing Investment controls by performing a design assessment on the adequacy and appropriateness of management's key controls.	Q3 2011	Annual Compliance Requirement	Fiscal Controls
IT Network Security <i>(deferred from prior year)</i>	Assess the security of the VTA network and external facing applications.	Q4 2011	IT Audit	Network
Follow Up Assessment	Evaluate and assess VTA management's progress on implementing management responses to audit observations for audits contained in FY10 and FY11 Internal Audit Work Plans.	Varies	Follow Up	N/A

* Q = quarter, a three-month period of the fiscal year. Q1 is July –September, Q2 is October –December, Q3 is January –March, and Q4 is April –June.

This report is intended solely for the information and use of VTA's Board of Directors, Audit Committee and management and is not intended to be used by anyone other than these specified parties.

Timeline & Reporting of Internal Audit (IA) Activities

Internal Audit Project	FY2010					FY2011											
	Feb	Mar	Apr	May	Jun	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
FY11 Internal Audit Plan Refresh		Completed															
SAP SOD				Completed													
IT Network Security													Completed				
SVRT Contract Compliance							Completed										
Investment Control Design Assessment										Completed							
FY12 Internal Audit Plan Refresh											Completed						
Follow-Ups																	In Progress

■ Completed
 ■ Planned
 ■ In Progress

This report is intended solely for the information and use of VTA's Board of Directors, Audit Committee and management and is not intended to be used by anyone other than these specified parties.