CITY OF PALO ALTO OFFICE OF THE CITY AUDITOR

December 5, 2011

The Honorable City Council
Palo Alto, California

Finance Committee Recommendation to Accept the SAP Security Audit

The City Auditor's Office recommends acceptance of the SAP Security Audit. At its meeting on October 18, 2011, the Finance Committee approved and unanimously recommended the City Council accept the SAP Security Audit. The Finance Committee minutes are included in this packet.

Respectfully submitted,

Ian Hagerman
Senior Performance Auditor

Audit Staff:

Houman Boussina, Senior Performance Auditor
Mimi Nguyen, Senior Performance Auditor
Davina The, Performance Audit Intern

ATTACHMENTS:

- Attachment A: SAP Security Audit Report (PDF)
- Attachment B: Finance Committee Minutes Excerpt (October 18, 2011) (PDF)

Department Head: Ian Hagerman, Sr. Performance Auditor

Attachment A

Office of the City Auditor

SAP SECURITY AUDIT

The City Should Implement Additional Measures to Effectively Secure Its SAP Enterprise Resource Planning System

OFFICE OF THE CITY AUDITOR

OCTOBER 2011

Attachment A

CITY of PALO ALTO
Office of the City Auditor

October 18, 2011

Honorable City Council
Attn: Finance Committee
Palo Alto, California

SAP SECURITY AUDIT:

The City Should Implement Additional Measures to Effectively Secure Its SAP Enterprise Resource Planning System

The City Auditor's Office (Auditor's Office) presents its report on the security of the City's SAP Enterprise Resource Planning system (SAP), which supports core business functions and management of information. During the audit, the City's Administrative Services Department (ASD) was principally responsible for managing SAP.

In planning the SAP audit, which was included in the City Auditor's Fiscal Year (FY) 2011 Annual Audit Workplan, the Auditor's Office detected a significant SAP security vulnerability resulting from an unsecured system-provided SAP user account. The unsecured user account allowed the Auditor's Office unrestricted access to sensitive and confidential information. This initial finding prompted an audit to assess controls required to secure SAP access.

The audit report consists of four main findings related to SAP security. Finding 1 discusses the security vulnerability the Auditor's Office detected and ASD's actions to address the vulnerability. Findings 2 and 3 discuss specific security issues related to managing and securing user accounts and access levels in SAP. Finding 4 presents our limited assessment of ASD's management of SAP security and indicates ASD has not formally adopted and implemented all controls needed to secure SAP and comply with the Payment Card Industry Data Security Standard and other applicable security control frameworks.

The four findings in the audit report are summarized below:

Finding 1: ASD did not secure powerful system-provided user accounts, resulting in significant security vulnerabilities

The Auditor's Office detected a powerful "SAP*" account that was not properly secured and allowed access to sensitive and confidential information. Such access could have allowed a motivated and sufficiently capable person to destroy or modify data, expose sensitive employee and customer information, or defraud the City. This SAP* account was not properly secured for extended periods of time. However, SAP logs lacked sufficient information to definitively establish the periods SAP* was not secured and to establish individual accountability for the security vulnerability. In addition to SAP*, other standard accounts were also unsecured. ASD did not have adequate policies and procedures to secure these powerful standard accounts. ASD has taken steps to identify and secure SAP* and other standard accounts. ASD also needs to develop policies and procedures to improve the timeliness and effectiveness of its response to security incidents.

Finding 2: ASD violated two critical security principles by not properly restricting access for all user accounts

ASD has not abided by the principles of "least privilege" and "segregation of duties" to control access to SAP. Since 2003, SAP user administrators assigned the powerful "SAP_ALL" profile to 31 SAP user accounts, providing them unrestricted SAP access. SAP user administrators did not abide by security principles by having multiple accounts and incompatible functions in creating users, assigning "roles" and "profiles" to users, and creating or changing profiles. We recommend ASD establish and implement policies and procedures in support of these two security principles.

Finding 3: ASD has not effectively managed all SAP user accounts to ensure system security

ASD has not consistently removed or disabled SAP employee user accounts in a timely manner and has not adequately secured and controlled non-employee user accounts. While ASD lacks an effective user account identity management system, improvements were made during the audit.

Finding 4: The City needs to formally adopt and implement a recognized information systems control standard to ensure SAP security

The City has not adopted and implemented a recognized information systems security control standard or framework needed to demonstrate control effectiveness in a consistent and repeatable manner, and it has not complied with requirements for business entities that process credit card transactions. Missing or inadequate controls include:

- Security policies and procedures and assignment of responsibility for SAP security.
- Security awareness and training program.
- Information systems risk assessment.
- Proper configuration of SAP system security settings.
- Effective management of SAP audit trails (logs).
- Safeguarding and controlling sensitive production data used for testing.
- Ensuring the Auditor's Office access levels in SAP is optimized.

During audit fieldwork, ASD developed and began implementing procedures and processes to address some areas of concern including security of system-provided accounts and user account administration. We recommend ASD assess SAP security risks and implement needed security controls through a risk-based and comprehensive process that is informed by the Payment Card Industry Data Security Standard, National Institute of Standards and Technology Special Publication 800-53, and other applicable frameworks.

Our report includes a total of 21 recommendations to improve the security of the City's critical information systems. The audit recommendations in the report are addressed to ASD, however, the former Information Technology Division in ASD has been established as a City department with a Chief Information Officer reporting to the City Manager. The new department will be responsible for implementing these recommendations.

I will present this report to the Finance Committee on October 18, 2011.

Respectfully submitted,

Michael A. Edmonds

Michael Edmonds
Interim City Auditor

Audit Staff:

Houman Boussina, Senior Performance Auditor
Mimi Nguyen, Senior Performance Auditor
Davina The, Performance Audit Intern

Page intentionally left blank

TABLE OF CONTENTS

List of Exhibits

Page intentionally left blank

Glossary

(Due to the technical nature of this audit report, we have included this glossary to assist in reading and understanding the report.)

Access control The process that limits and controls access to an information system to protect against unauthorized entry or use.

Access privileges The extent to which an individual can access computer systems and use or modify the programs and data. SAP user administrators may customize and restrict levels of access to SAP through assignment of roles and/or profiles to user accounts, which provide access to SAP transactions, reports, and other functions and define a user's ability to create, delete, or display information.

Account Management The processes that involve:

- Requesting, establishing, issuing, and closing user accounts.
- Tracking users and their respective access authorizations.

Accountability The security goal requiring that systems are designed and configured so that actions of a user in an information system may be traced uniquely to the user. In the event of a security incident, a properly configured system with adequate security reports should support an investigation to determine who was responsible, assess the level of exposure, and facilitate recovery and any legal action required.

Anonymize To remove identifying characteristics from sensitive data in order to prevent misuse or unauthorized disclosure. Anonymized data is useful for system testing in order to simulate real conditions as closely as possible while safeguarding sensitive data.

Audit Information System (AIS) A free tool delivered with SAP for use by external, internal, system, and data security auditing functions. AIS is designed to improve audit quality and facilitate the audit process.

Application controls Controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of data.

Attack Attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's integrity, availability, or confidentiality.

Backdoor An undocumented way to gain access to a program, data, or an entire computer system. Although backdoors may have a business purpose, they usually constitute a security risk.

Control Framework A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an organization.

Enterprise Resource Commercial software that integrates all the information flowing

Planning (ERP) system through the entity. ERP systems contain functional modules such as financial, accounting, human resources, supply chain, and customer information, which are integrated within the core system or interfaced to external systems.

Fraud A type of illegal act involving the obtaining of something of value through willful misrepresentation.

Generic user account An information system user account that is not assigned to an individual user. The use of generic user accounts generally conflicts with the security requirement for ensuring user actions in a computer system may be uniquely identified with an individual.

Hard-coding The practice of storing information, such as a default username and password into an application's code. SAP systems include a hard-coded user account known as "SAP*" that could pose a security risk if not properly secured. Unlike other user accounts, SAP* does not require a user master record because it is defined in the code itself and may allow an unauthorized user unrestricted system access if not properly secured.

Incident An occurrence that:

- Actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or
- Constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Least Privilege Principle requiring that each user be granted the most restrictive set of access privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system. SAP administrators may customize and restrict levels of access to SAP through assignment of roles and/or profiles to user accounts, which provide access to SAP transactions, reports, and other functions and define a user's ability to create, delete, or display information.

Log A record of the events occurring within an organization's systems and networks.

National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53) A published document that outlines specific controls to implement, based upon the risk level of the system, in order to preserve the confidentiality, integrity, and availability of the agency's data.

Payment Card Industry Data Security Standard (PCI DSS) A minimum set of requirements for protecting cardholder data which may be enhanced by additional controls and practices to mitigate risks. Because the City of Palo Alto processes and stores credit card data, it is required to comply with PCI DSS to protect cardholder data.

Personally identifiable information
Any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, or biometric records, and any other information which is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Production environment
The system environment where the entity performs its operational information processing activities. Testing and development of an information system should be done in segregated development and testing environments to prevent unauthorized changes to the production environment and to help ensure system security.

Profile
A component of the SAP authorization structure used to protect transactions, programs, and services in SAP systems from unauthorized access. SAP profiles contain the authorization data that determines which transactions, programs, and services a user can access after he or she has successfully logged on to the system. SAP user administrators may customize and restrict levels of access to SAP through assignment of roles and/or profiles to user accounts, which provide access to SAP transactions, reports, and other functions and define a user's ability to create, delete, or display information.

Role
A component of the SAP authorization structure used to protect transactions, programs, and services in SAP systems from unauthorized access. SAP roles contain the SAP profiles defined above, along with additional components such as user menus. SAP user administrators may customize and restrict levels of access to SAP through assignment of roles and/or profiles to user accounts, which provide access to SAP transactions, reports, and other functions and define a user's ability to create, delete, or display information.

SAP
Founded in 1972, the company SAP has headquarters in Walldorf, Germany and produces enterprise application software. SAP stands for "Systems, Applications, and Products in Data Processing." The company's products include the SAP ERP Central Component, Release 6.0 application, which the City of Palo Alto has purchased and implemented along with other SAP products.

SAP Library
All of the online documentation for all SAP components, including guidance on SAP security.

Security policy
The set of management statements that documents an organization's philosophy of protecting its computing and information assets. These statements may be enforced by an information system's security features.

Segregation of duties
A basic control that prevents or detects errors and fraud by assigning responsibility for initiating transactions, recording transactions, and custody of assets to separate individuals. Because ERP systems are

highly integrated and support a broad range of entity activities, access controls (particularly least privilege) and segregation of duties controls are needed. SAP user administrators may customize and restrict levels of access to SAP through assignment of roles and/or profiles to user accounts, which provide access to SAP transactions, reports, and other functions and define a user's ability to create, delete, or display information.

Standard user accounts (also known as "special users")

User accounts that are created upon installation of SAP clients or systems. These user accounts are delivered with standard usernames and passwords that are well-known.

System administrator

The person responsible for administering use of a multi-user computer system, communications system, or both.

System developer

A person who develops and maintains system software.

User Master Record (UMR)

User master records define the user accounts for enabling access to SAP. The user master record contains access information, including user id, passwords, roles, and profiles, which are needed by the system to validate a user and assign access rights. Generally, only users who have a UMR can log on to the system.

User (Account)

Individual, or process acting on behalf of an individual, that is authorized to access an information system.

The City's SAP user accounts were classified as one of the following types:

- **Dialog:** User type for exactly one interactive user (all logon types including internet users).
- **Communications:** User type for dialog-free communication between systems.
- **System:** User type for background processing and communication within a system.
- **Reference:** User type for general, non-person related users that allows the assignment of additional identical authorizations. You cannot log on to the system with a reference user.
- **Service:** User type that is a dialog user available to a larger, anonymous group of users.

User Administrator

An individual who performs the following tasks:

- Maintains user master records
- Assigns roles and profiles to users
- Uses the SAP user information system
- Views roles and profiles
- Manages roles

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation.

Introduction

In planning the SAP audit, which was included in the City Auditor's Fiscal Year (FY) 2011 Annual Audit Workplan, the City Auditor's Office (Auditor's Office) detected a significant SAP security vulnerability that allowed the Auditor's Office unrestricted access to sensitive and confidential information. As a result, the Auditor's Office conducted an audit to assess controls required to secure access to SAP.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In July 2002, the City selected and began implementing an SAP Enterprise Resource Planning (SAP ERP) application, which currently supports the City's core business functions, including accounting, finance, purchasing, human resources, and utilities.[1] The City has implemented other SAP applications and components beyond the original core application selected in 2002. According to a staff report, the City's SAP installation and upgrade costs totaled approximately $15 million as of April 19, 2011. The report also identifies annual maintenance costs of approximately $3 million, which is comprised of staffing costs ($2.2 million), hardware and software licensing costs ($0.5 million), and external consultant costs ($0.25 million).[2]

The City's SAP applications support a broad range of functions, including processing and storing financial transactions and confidential information for both City employees and customers. The City's FY 2012 Adopted Operating Budget and staff reports illustrate the range of activity SAP supports:

- $440.5 million in total citywide revenues
- $460.8 million in total citywide expenditures
- 1,016.6 citywide positions
- $130.9 million in salaries & benefits
- 13,000 accounts payable checks
- 370,000 utility bills
- $220.8 million in utility charges

[1] "Utilities" includes electric, gas, water, wastewater collection, and fiber optic services in the Utilities Department, and refuse, storm drain, and wastewater treatment services in the Public Works Department.

[2] The Auditor's Office has not audited these figures.

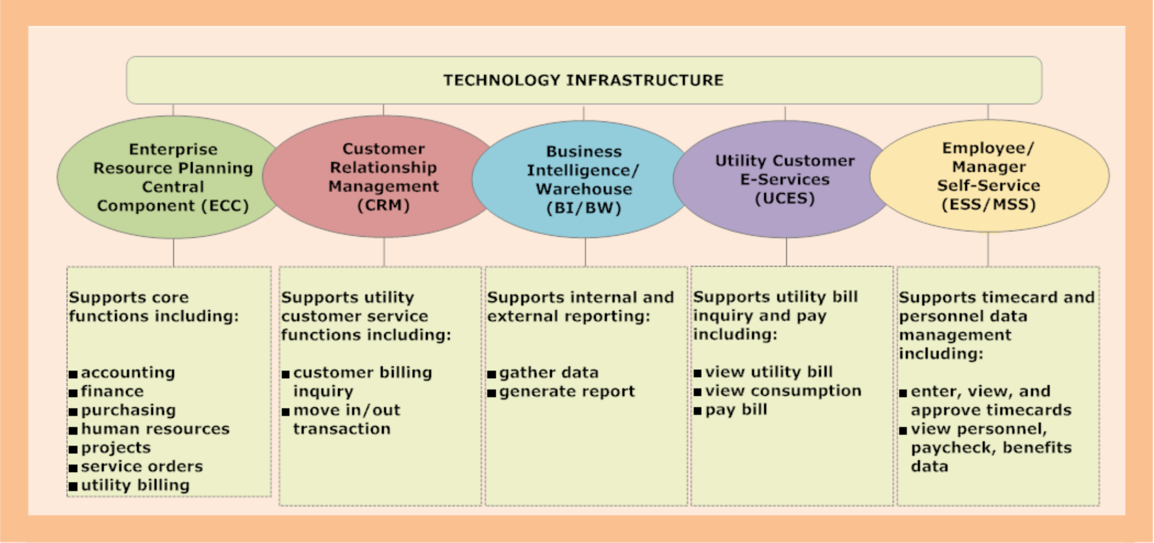
City of Palo Alto SAP applications

The City has implemented the following five SAP applications to support its business needs:

1. ***Enterprise Resource Planning Central Component (ECC)*** – The City's core SAP application used by departments to support the City's key business functions including accounting, finance, purchasing, human resources, and utilities.
2. ***Customer Relationship Management (CRM)*** – Supports utilities department customer service functions.
3. ***Business Intelligence/Business Warehouse (BI/BW)*** – Supports generation of utilities reports.
4. ***Utility Customer E-Services (UCES)*** – Used by City customers to view their consumption and pay bills.
5. ***Employee Self-Service/Manager Self-Service (ESS/MSS)*** – Used by City employees and managers to manage time sheets, pay stubs, and other information.

Exhibit 1 represents the City's five networked SAP applications and describes some of the specific business functions the applications support.

Exhibit 1: Overview of the City of Palo Alto's five SAP applications


TECHNOLOGY INFRASTRUCTURE
Enterprise Resource Planning Central Component (ECC)
Customer Relationship Management (CRM)
Business Intelligence/ Warehouse (BI/BW)
Utility Customer E-Services (UCES)
Employee/ Manager Self-Service (ESS/MSS)
Supports core functions including:
■ accounting
■ finance
■ purchasing
■ human resources
■ projects
■ service orders
■ utility billing
Supports utility customer service functions including:
■ customer billing inquiry
■ move in/out transaction
Supports internal and external reporting:
■ gather data
■ generate report
Supports utility bill inquiry and pay including:
■ view utility bill
■ view consumption
■ pay bill
Supports timecard and personnel data management including:
■ enter, view, and approve timecards
■ view personnel, paycheck, benefits data

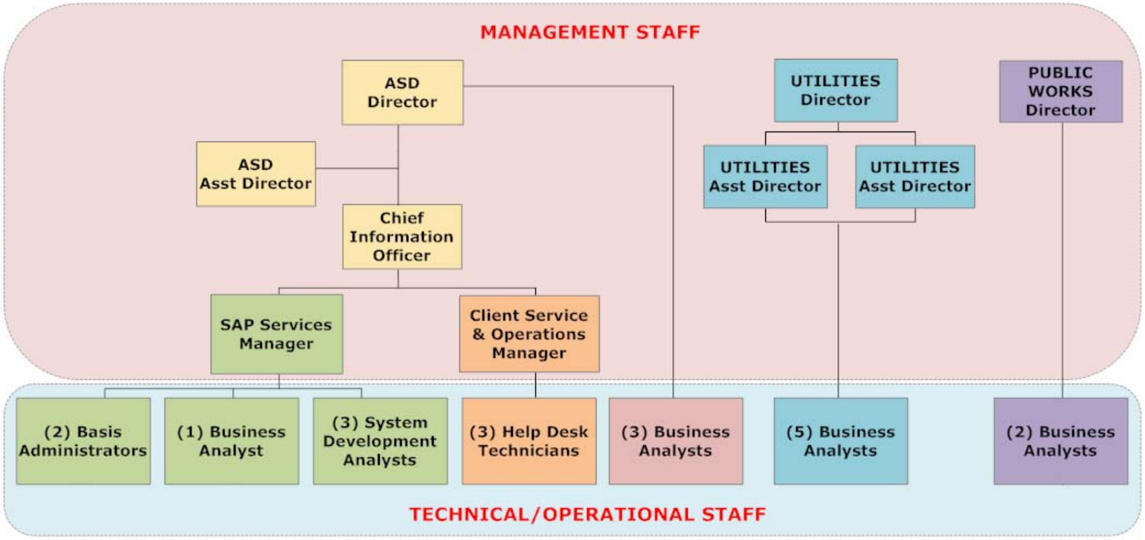
Source: ASD records

Staffing and Management

The City established an SAP Steering Committee and Program Management Office to manage SAP investment direction and provide overall guidance for SAP governance and control. These teams are comprised of management and operational staff from the Administrative Services, Utilities, and Public Works departments. Technical and operational staff consists of basis administrators, system development analysts**,** help desk technicians, and business analysts from the Administrative Services, Utilities and Public Works departments.

Exhibit 2 provides a generalized representation of staff associated with the management and operation of SAP during the audit.

Exhibit 2 – Staff associated with management and operation of SAP



Note: This exhibit provides only a generalized depiction of full-time equivalents (FTE) and reporting lines. Some staff perform duties related to SAP in support of their department but are not exclusive to SAP Services.

Source: ASD records and City of Palo Alto Adopted Operating Budget

In FY 2012, the former Information Technology Division in ASD has been established as a City department with a Chief Information Officer reporting to the City Manager.

Overview of Enterprise Resource Planning (ERP) system risks[3]

ERP systems are highly integrated and support a broad range of entity activities, resulting in certain increased risks that should be controlled with:

- System development/configuration management controls to provide reasonable assurance that the system will operate as intended.
- Service continuity/contingency planning to recover critical ERP systems.
- Access and other general controls to prevent unauthorized access.

In addition, general information systems controls should protect the technology infrastructure that supports ERP applications.

Although efficiencies may be gained with ERP systems, these systems heighten the need to control access to sensitive transactions and to ensure proper segregation of duties compared with entities having multiple applications for business processes. Entities lose the inherent segregation in integrated applications since more of the process is performed in the same application.

Proper control over levels of access in SAP applications is a key overall aspect of system security. An employee with improperly restricted levels of access could potentially have inappropriate access to sensitive information, master data files, financial

[3] Based on information presented in the United States Government Accountability Office Federal Information System Controls Audit Manual.

transactions, system administration functions, security functions, and other areas not related to his or her role in the organization.

Guidance on information systems security

Governmental and private agencies have developed and published control frameworks to provide guidance on securing information systems to preserve the confidentiality, integrity and availability of an agency's data. We based our review on recognized security control frameworks for information systems and SAP-specific guidelines. The proper implementation of security controls is recommended to:

- Demonstrate compliance with a variety of governmental, organizational, or institutional security requirements.
- Facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner, thus contributing to the organization's confidence of ongoing compliance with its stated security requirements.

Throughout the report, we refer to the following three sources of guidance on minimum security control requirements:

1. ***SAP Library*****:** The German software corporation SAP provides guidelines on use and configuration of SAP applications in an online manual known as the "SAP Library."
2. ***Payment Card Industry Data Security Standard, version 2.0 (PCI DSS)*****:** The Payment Card Industry Security Standards Council promulgates PCI DSS, a baseline of technical and operational requirements, to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.
3. ***National Institute of Standards and Technology Special Publication 800-53, Revision 3 (NIST SP 800-53)*****:** In 1996 the National Technology Transfer and Advancement Act, Public Law 104-113, was passed, authorizing NIST to coordinate federal, state and local government technology standards activities with private sector technical standards activities and assessments. The control catalog in NIST SP 800-53 outlines specific controls to implement in order to preserve the confidentiality, integrity and availability of the agency's data. The guidelines were developed to help achieve more secure information systems and effective risk management within the federal government. NIST also encourages state, local, and tribal governments, as well as private sector organizations to consider using the guidelines, as appropriate. NIST SP 800-53 states the final determination of the appropriate set of security controls necessary to provide adequate security for an information system is a function of an organization's assessment of risk, and that in many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system.

Audit Objectives, Scope, and Methodology

In planning the SAP audit, the Auditor's Office detected a significant SAP security vulnerability, which allowed the Auditor's Office unrestricted access to sensitive and confidential information. As a result, the Auditor's Office conducted an audit to assess controls required to secure SAP access. The audit had the following objectives:

1. Determine if staff has properly secured system-provided (standard) SAP user accounts[4] and timely addressed other related critical security vulnerabilities identified.
2. Determine if there has been unauthorized access to SAP through use of the standard user account "SAP*" or other standard accounts.
3. Determine if the City has an adequate security policy, procedures, and processes to ensure standard SAP user accounts and other accounts with unrestricted access are properly secured and monitored.
4. Assess the increased risk for fraud and abuse resulting from identified SAP security vulnerabilities.

As described in the background section of this report, the City has implemented five SAP applications to support its business needs. SAP Enterprise Resource Planning Central Component (SAP ECC) is the core SAP application used to support the City's key business functions including accounting, finance, purchasing, human resources, and utilities. ASD has implemented segregated "development," "quality assurance," and "production" systems for each of the five SAP applications in order to make and test application changes without interfering with live operational data and transactions.

The scope of this audit was limited to the objectives listed above and to the City's SAP ECC production system. This audit does not constitute a comprehensive security evaluation for the City's SAP applications. However, the security concerns raised in this report may also be applicable to:

- The City's other SAP applications and systems.
- The City's non-SAP applications.
- Components of the City's information systems infrastructure not included in the scope of this audit.

We encountered a limitation on access to an SAP Services administrator who was on extended leave during the course of the audit for reasons attributed to issues not related to the concerns raised in this report. As a result, we could not obtain further clarification on certain aspects of the security vulnerability identified in Finding 1.

Audit fieldwork and testing was guided by the SAP Library in addition to minimum information systems security standards primarily stated in the following sources:

- PCI DSS, version 2.0
- NIST Special Publication 800-53, Revision 3

To conduct this audit, we analyzed SAP ECC security and log reports in addition to ASD technical documentation on the City's implementation and management of its SAP

[4] The term "special user" is also used in the SAP Library to refer to these accounts.

applications. We researched information systems security standards and discussed security concerns with the City's external audit staff specializing in information systems, an independent SAP security director, and with an SAP consultant. We interviewed ASD and Human Resources Department staff. We also assessed the City's overall SAP security policies and procedures to determine if a recognized information systems security control framework was in place.

Due to limitations on our levels of independent access in SAP, we relied on ASD staff to provide requested SAP security reports and data, which we reviewed or tested to the extent possible to ensure reliability.

We apprised City management and staff of security concerns during the course of the audit to ensure the City's systems could be timely secured. We also met with the City Manager, the Interim City Attorney, and City Council members to apprise them of our concerns.

Our report includes a total of 21 recommendations to improve the security of the City's critical information systems. The audit recommendations in the report are addressed to ASD, however, the former Information Technology Division in ASD has been established as a City department with a Chief Information Officer reporting to the City Manager. The new department will be responsible for implementing these recommendations.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Finding 1: ASD did not secure powerful system-provided user accounts, resulting in significant security vulnerabilities

The Auditor's Office detected a powerful "SAP*" account that was not properly secured and allowed access to sensitive and confidential information. Such access could have allowed a motivated and sufficiently capable person to destroy or modify data, expose sensitive employee and customer information, or defraud the City. This SAP* account was not properly secured for extended periods of time. However, SAP logs lacked sufficient information to definitively establish the periods SAP* was not secured and to establish individual accountability for the security vulnerability. In addition to SAP*, other standard accounts were also unsecured. ASD did not have adequate policies and procedures to secure these powerful standard accounts. ASD has taken steps to identify and secure SAP* and other standard accounts. ASD also needs to develop policies and procedures to improve the timeliness and effectiveness of its response to security incidents.

The Auditor's Office detected SAP* was not properly secured and allowed access to sensitive and confidential information

During the installation process, SAP systems create a set of standard user accounts including "SAP*," which should be properly secured and protected from unauthorized use. SAP* has a well-known default password and may provide unrestricted system access. Another standard user account known as "DDIC" may also provide unrestricted access and should also be properly secured. Recognized information systems security standards explicitly address securing standard user accounts by methods including, but not limited to, changing passwords. Securing these accounts should be prioritized because their usernames and passwords are well-known and could be used by unauthorized users or hackers to access SAP systems. While certain standard user accounts are required for specialized tasks such as initial system implementation, these accounts should be secured to prevent an unauthorized user from accessing the system. Such access could potentially result in the following:

- Exposure and misuse of data such as personal identifying information
- Sabotage and operational disruptions
- Financial losses
- Damage to reputation

On January 6, 2011, the Auditor's Office staff logged in to SAP using SAP* with its default password. Our initial evaluation of the security vulnerability confirmed the well-known SAP* user account with its default password grants unrestricted SAP access if not secured. Specifically, the unsecured SAP* account granted access to:

- View and modify sensitive and confidential data, including City employee social security numbers, payroll records, and customer billing and credit information.
- Execute high risk business transactions, such as changes to employee salaries, changes to utility rates, and changes to customer billing and credit information.
- Create vendors and approve invoice payments.
- Modify key system settings, including opening and closing of accounting periods and other changes to financial system settings.

On January 10, 2011, ASD detected unauthorized access with the SAP* user account from two computer terminals in the Auditor's Office. SAP Services staff prepared an incident report dated January 11, 2011, that states the Auditor's Office had used the SAP* account on January 6, 2011, and January 10, 2011, to access 125 SAP transactions. SAP system records show staff enabled a security parameter on January 11, 2011,[5] to prevent use of the SAP* user account with its default password.

The Auditor's Office met with ASD on January 13, 2011, to discuss the security vulnerability. ASD staff stated:

- The SAP* user account is usually "locked," but an SAP Services administrator had "opened" the SAP* user account because of a technical issue encountered during the installation of an SAP support pack during the period from December 10, 2010, through December 12, 2010.
- The SAP Services administrator did not secure the SAP* user account subsequent to successful installation of the support pack.
- ASD did not have automated controls to detect unauthorized SAP access, but staff had contacted a consultant to implement an automated script to notify staff if SAP* was not secured.

Due to the significance of the security vulnerability resulting from the unsecured SAP* user account, the Auditor's Office immediately communicated to ASD the preliminary audit scope and objectives and commenced fieldwork to further assess the duration and potential impact of the exposure, and the overall adequacy of the City's management of SAP access and related controls.

The powerful standard user account SAP* was likely not secured during extended periods, causing a serious security vulnerability

Our preliminary assessment could not validate ASD staff assertions that the SAP* user account was activated to install the SAP support pack in December 2010, or that SAP* was needed for the installation. SAP system reports suggest SAP* was likely accessible using its default password since May 23, 2010, and was likely left unsecured during other extended periods since the inception of SAP. The rationale for this conclusion is described below.

SAP* is the only user account in the SAP system that does not require a "user master record" (UMR),[6] but is defined in the system code itself. If the SAP* UMR is never created or is deleted and a special security parameter used to secure SAP* is disabled, the hard-coded SAP* user account can be accessed by anyone using its default and well-known password, and it will have unrestricted system access resulting in a serious security vulnerability. The SAP online manual warns the SAP* UMR should not be deleted, and that use of the hard-coded SAP* account should **never** be required. An SAP Services manager stated in some situations, such as during installation of certain SAP upgrades, use of SAP* may be required if indicated by SAP guidance.

[5] The incident report prepared by staff states the security parameter was enabled on January 10, 2011, at 9:00 pm.

[6] "User master records" define the user accounts for enabling access to SAP. The user master record (UMR) contains access information needed by the system to validate a user and assign access rights. This information includes user id, password, roles, and profiles. Generally, only users who have a UMR can log on to the system.

We were able to access SAP using the hard-coded SAP* user account and its default password because the security parameter protecting against its use was disabled and the SAP* UMR was missing. SAP Services staff initially reported the SAP* user account had been "opened" to install an SAP support pack during the period December 10, 2010, through December 12, 2010, implying the period of vulnerability was from approximately December 10, 2010, to January 11, 2011. SAP system reports did not validate ASD staff's assertions it was "opened" in December 2010. Furthermore, an SAP system report indicated that the security parameter was disabled for over seven months from May 23, 2010, to January 11, 2011, and during at least one other extended period, from April 4, 2008, to April 18, 2008.

In reviewing available SAP system log records and security reports, we concluded:

- SAP* was likely accessible using the default password during the entire period from May 23, 2010, to January 11, 2011, resulting in a serious security vulnerability.
- SAP* may have been accessible using the default password between April 4, 2008, and April 18, 2008.
- SAP* was accessible using the default password for an unknown period(s) from January 16, 2003, to December 15, 2005.

Available SAP system logs suggest the SAP* account was not accessed from August 4, 2010, until January 6, 2011, when the Auditor's Office accessed the account. Records prior to August 4, 2010, were not available due to system configurations limiting the amount of data retained. ASD staff we interviewed stated they did not have any direct knowledge of fraud or abuse related to the security concerns addressed in this audit.

SAP logs lacked sufficient information to determine exactly how long the system was unsecured and to establish individual accountability for the SAP* incident

SAP creates various logs to help ensure individual accountability and to provide a means for investigating security incidents. Access to SAP logs should be properly secured and review of logs should be effectively managed to ensure system security.

Although the SAP* UMR was likely missing during some or all of the periods the protective security parameter was disabled, the SAP system log used to monitor and ensure accountability for any user account changes did not include records showing deletion of the UMR at any point. Moreover, a subsequent security report generated on February 14, 2011, showed the SAP* UMR had been recreated, presumably to secure the system, but again the SAP log report did not include a record of this activity. The missing log records raised serious concerns regarding the integrity and security of the SAP system logs.

In order to address concerns regarding missing SAP log records, ASD and the Auditor's Office discussed the incident with an external consultant.[7] The analysis conducted by the consultant and ASD concluded there are two possible explanations for the missing SAP log records:

[7] The City had an existing contract with the consultant for SAP support and maintenance services.

- Someone deleted then recreated the SAP* UMR by accessing the underlying SAP database system.
- Someone deleted the SAP log records showing deletion and recreation of the SAP* UMR.

Staff stated there were only two SAP Services administrators with direct access to the SAP database system. We interviewed one of the SAP Services administrators who stated he did not delete or recreate the SAP* UMR. We could not interview the other administrator because he was on extended leave for reasons attributed to issues not related to the concerns raised in this report**.**

In either case, we concluded any activity conducted to delete the SAP* UMR or SAP log records undermined SAP security. We discussed the need to further investigate and address these concerns with the City's ASD Director, ASD Assistant Director, and SAP Services manager.

Findings 2, 3, and 4 address the need to control and limit SAP Services administrator access in SAP and other controls, such as securing and monitoring of the system logs needed to prevent or detect unauthorized activity.

ASD did not secure other standard user accounts

In addition to SAP*, other standard user accounts are created during installation of SAP systems, and these accounts should also be properly secured to prevent unauthorized system access.

A standard SAP security report generated on January 10, 2011, identified five other standard user accounts in the SAP Enterprise Resource Planning Central Component (SAP ECC) production system, which still had their well-known default passwords, indicating they had not been properly secured since inception of the SAP system. In attempting to access these standard accounts, we found that SAP generated error messages suggesting the passwords had expired at some point in time, and in that sense, the accounts appeared secure.

ASD did not have formal procedures to secure SAP* or other standard user accounts

Because standard SAP user accounts may have privileged or unrestricted access and do not have staff names or identification numbers associated with them, they could be used without individual accountability to perform unauthorized activity. The SAP online manual provides specific procedures to ensure standard user accounts, including SAP* are properly secured. These procedures include:

- Ensuring the SAP* UMR is present and the protective security parameter is enabled.
- Changing passwords and locking standard user accounts when not in use.
- Restricting access to standard user accounts so that only selected authorized staff can manage them.
- Using a special SAP report to monitor the status of all standard user accounts.

ASD did not have any formal policies or procedures to authorize, monitor, or ensure accountability for use of SAP* or other standard user accounts. Moreover, ASD did not have any policies and procedures to properly secure these accounts.

ASD took steps to secure standard SAP user accounts in all SAP systems

As of the end of audit fieldwork, ASD implemented controls to secure standard user accounts, including an automated notification system to alert ASD if the security parameter used to secure the hard-coded SAP* user account with its default password is disabled.[8]

ASD conducted a comprehensive review of standard user accounts in all of the City's SAP systems. An April 7, 2011, in-progress report provided by an SAP Services manager showed staff had identified a total of 83 standard user accounts, of which 64 percent had not been properly secured.

SAP system reports dated June 1, 2011, showed a total of 107 standard user accounts, including the 83 stated above, in the City's SAP systems and that staff had implemented controls to secure the accounts. The reports show:

- The default passwords for all standard accounts have been changed.
- The security parameter preventing use of the hard-coded SAP* user account was enabled in all applicable SAP systems.
- Although most standard user accounts were locked, staff did not lock DDIC, because according to an SAP Services manager, it is needed to execute certain processes. DDIC may provide unrestricted access and should be properly secured.

ASD implemented other key controls to secure standard user accounts including:

- Policies and procedures to ensure use of standard user accounts is properly authorized and monitored, and that they are secured when not in use.
- Procedures to detect unsecured standard user accounts.
- An automated notification system to notify staff if the security parameter for SAP* is disabled.
- Restricting access to standard user accounts so that only an authorized individual has access to manage these accounts.

It was beyond the scope of this audit to assess the adequacy of the preliminary actions ASD has taken to address concerns raised in this audit.

[8] The Auditor's Office did not assess the effectiveness of this notification system or the other controls implemented to secure these accounts.

RECOMMENDATION #1: ASD should develop and implement formal policies and procedures addressing standard SAP user accounts in order to:

- Secure standard user accounts and prevent unauthorized use.
- Detect on an ongoing basis any unsecured standard accounts and any unauthorized use.
- Ensure standard user accounts can only be managed by a designated individual(s).
- Authorize use only if appropriate, and ensure there is accountability for any use.
- Ensure any authorized use is monitored.

RECOMMENDATION #2: ASD should further investigate the following:

- Staff's account that SAP* was left unsecured after installing an SAP support pack in December 2010.
- Responsibility for the deletion and recreation of the SAP* user master record.
- Responsibility for missing log records.

ASD should develop policies and procedures to improve the timeliness and effectiveness of its response to security incidents

The Auditor's Office's testing of SAP vulnerability through access to the unsecured hard-coded SAP* user account was not announced in advance, and it presented an opportunity to assess staff's response to a simulated security incident. Policies and procedures addressing response to security incidents should ensure:

- The incident is effectively contained, managed, and investigated.
- The City timely and effectively identifies and corrects inadequate controls.
- Accountability is established for any breach in security.

The PCI DSS control framework requires organizations to have a formal incident response plan to respond effectively and immediately to a system breach. The plan should include provisions to address:

- Roles and responsibilities
- Incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements in reporting compromises

In addition, designated staff should be available to respond to alerts in a timely manner, and the incident response plan should be tested annually and revised as appropriate to ensure it is current and effective.

NIST also addresses the need for adequate incident management through implementing appropriate controls including incident response policies and procedures, training, exercises, monitoring, and reporting.

<u>ASD did not timely detect unauthorized use of the hard-coded SAP* account</u>

In testing SAP system vulnerability, the Auditor's Office had access to the unsecured hard-coded SAP* user account from January 6, 2011, through January 10, 2011, before ASD staff detected the auditors' activity and preliminarily secured SAP*, effective January 11, 2011. Based on our testing results, we concluded that use of the SAP* account by a motivated and sufficiently capable user during the 4-day period could have had serious consequences. An SAP Services administrator stated he detected use of the unsecured SAP* user account through a routine manual review of SAP system logs. As previously discussed, ASD subsequently implemented a notification system to notify staff if the security parameter to disable the hard-coded SAP* user account is deactivated. However, as of the end of audit fieldwork, an SAP Services manager stated review of SAP logs remains a manual process.

<u>The SAP Incident Report was not independent, contained unsupported information, and was incomplete</u>

The City did not have any policies or procedures addressing incident response and reporting. SAP Services staff identified and documented the SAP* incident in an SAP Incident Report. According to an SAP Services manager, the SAP Incident Report was jointly prepared by SAP Services staff and contained unverified information provided by the SAP Services administrator responsible for the lapse in security. We found several weaknesses in the SAP Incident Report (report):

- The report contained information that could not be supported by SAP system records. In particular, the report suggested the hard-coded SAP* account was "opened" to apply a support pack in SAP over the weekend from December 10, 2010, through December 12, 2010. As previously stated, SAP system records did not show any activity using the SAP* account during this period. Rather, the records suggest the SAP* account was likely activated and left unsecured as of May 23, 2010.
- The report implied the SAP* account may be used to apply support packs in the future. We could not find any valid business reason to use the hard-coded SAP* account, except for rare emergencies.
- The report did not address other related security issues revealed during the audit, such as the unsecured standard SAP accounts in other SAP systems and clients.
- Important report elements were not addressed. In particular, the following important sections of the template were left blank:
    - Evidence of approval
    - Affected policies or procedures
    - Remedial training requirements

The staff member responsible for the security incident had unrestricted access

The SAP Services administrator identified as responsible for the SAP* security incident had a personal SAP user account with unrestricted system access. The City did not take steps to assess or restrict the access level of the administrator until after he had left on extended leave due to reasons attributed to issues not related to the incident.

Efforts to secure SAP access were uncoordinated

Staff did not have a formal process to secure the SAP system once unauthorized access using the unsecured hard-coded SAP* account was detected. Subsequent to detection of the unauthorized access, SAP Services staff disabled the lead auditor's personal SAP user account. However, the lead auditor regained access to his personal account by simply contacting the City's help desk staff who enabled the account. Subsequently, SAP Services staff again locked the lead auditor's personal SAP account and help desk staff were instructed not to unlock the account.

The steps taken to presumably secure the SAP system by locking the lead auditor's personal SAP user account appeared inconsistent and uncoordinated. The City's incident response process may not have been effective in responding to a malicious intruder because:

- The majority of vulnerability testing using the hard-coded SAP* account was executed by another auditor whose personal SAP user account was not locked.
- Locking the lead auditor's personal SAP user account did not provide any additional security since the personal user account was unrelated to the unsecured hard-coded SAP* account or other unsecured standard SAP accounts.
- Staff did not contact the Auditor's Office or the assigned owners of the computers used to access SAP using the unsecured SAP* account in order to properly investigate the incident and determine if there had been unauthorized use or theft of the auditors' computers.

ASD should refer to NIST Special Publication 800-61 (Computer Security Incident Handling Guide) in developing and implementing competent and adequate incident handling policies and procedures to ensure the City is able to effectively detect, analyze, and prioritize security incidents.

RECOMMENDATION #3: To ensure the City can appropriately respond to SAP security incidents, ASD should develop and implement a comprehensive incident response plan that meets PCI DSS and NIST control standards and includes provisions to address:

- Incident response policies and procedures
- Incident response training
- Monitoring and reporting
- Roles and responsibilities
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements in reporting compromises

Finding 2: ASD violated two critical security principles by not properly restricting access for all user accounts

ASD has not abided by the principles of “least privilege” and “segregation of duties” to control access to SAP. Since 2003, SAP user administrators assigned the powerful “SAP_ALL” profile to 31 SAP user accounts, providing them unrestricted SAP access. SAP user administrators did not abide by security principles by having multiple accounts and incompatible functions in creating users, assigning “roles” and “profiles” to users, and creating or changing profiles. We recommend ASD establish and implement policies and procedures in support of these two security principles.

31 SAP user accounts had unrestricted SAP_ALL profile access

The Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology (NIST) state organizations should abide by the principles of “least privilege” and “segregation of duties.” Least privilege requires limiting user access based on job responsibilities to accomplish assigned tasks in accordance with organizational missions and business functions, while segregation of duties ensures clear separation of roles and responsibilities across the functions within an organization. These principles help reduce the risk of possible fraud and abuse, exposure of sensitive and confidential information, and data breach.

SAP administrators may customize and restrict levels of access to SAP through assignment of “roles” and/or “profiles” to user accounts, which at a granular level can determine an SAP user’s level of access. In order to ensure SAP access security, policies and procedures should ensure only authorized individuals have access to the system, and that roles and profiles are managed to ensure authorized individuals have the appropriate level of system access based on the employee’s role in the organization and business needs.

Although the City has a process to administer access using SAP roles, ASD did not have any policies, procedures, or practices to control access in SAP through assignment of standard profiles. In practice, ASD has assigned both roles and profiles, including the SAP_ALL profile which grants unrestricted access similar to the SAP* standard user account discussed in Finding 1.

The SAP online manual states:

1. SAP_ALL should not be assigned to ANY users in the organization.
2. Only one user account should be created with the SAP_ALL profile, and the password for the user account should be kept secret (by storing it in a safe).
3. The single user account with SAP_ALL should only be used in emergencies.

Although SAP guidance recommends against assigning the SAP_ALL profile to users within the organization, the City’s SAP system records show:

- 31 user accounts were assigned the SAP_ALL profile since 2003.
- As of January 12, 2011, 12 user accounts were still assigned the SAP_ALL profile.

- 8 SAP user accounts were used to grant unrestricted access to various users through the SAP_ALL profile.
- The SAP_ALL profile was assigned to generic user accounts[9] and other user accounts associated with the City's external consultants or SAP service providers.[10]

By granting unrestricted access, ASD has violated the principles of least privilege and segregation of duties. The SAP_ALL profile inherently grants user access privileges beyond the job responsibilities to accomplish assigned tasks in accordance with organizational missions and business functions. In addition, SAP_ALL does not support clear separation of roles and responsibilities across the functions within an organization. According to the United States Government Accountability Office Federal Information System Controls Audit Manual (FISCAM), work responsibilities should be segregated so that one individual does not control all critical stages of a process. FISCAM further states effective segregation of duties starts with effective entitywide policies and procedures that are implemented at the system and application levels. If ASD grants the SAP_ALL profile, it cannot effectively abide by the principles of least privilege and segregation of duties.

RECOMMENDATION #4: To mitigate risks associated with assignment of unrestricted SAP access, ASD should:

- Formally adopt policies and procedures addressing SAP user access that are consistent with the principles of least privilege and segregation of duties.
- For emergency purposes, ASD should consider creating a single unrestricted account assigned the SAP_ALL profile that is appropriately secured and controlled in accordance with SAP guidelines and industry standards.
- Implement policies and procedures to either prohibit or control the use of all other powerful system-provided SAP profiles.
- Ensure needed SAP roles and profiles are approved by management and included in the City's role authorization procedures, and that unauthorized roles and profiles are not assigned.
- Develop procedures to detect any unauthorized roles or profiles assigned to users.

[9] Generic user accounts do not include identifying information associated with an individual.

[10] Risks associated with non-organizational user accounts are discussed in Finding 3.

SAP user administration practices violated information systems security principles

Staff responsible for the administration of SAP user accounts should not be able to modify their own authorizations, or perform combinations of other incompatible functions that would allow them to give themselves (or a user account they created) powerful access. According to authoritative guidance on SAP security, an individual should not have authorization in SAP to perform more than one of the following functions:[11]

- Creating and maintaining roles/profiles
- Assignment of roles/profiles
- Creating and maintaining user accounts

If any of these functions cannot be properly segregated, there should be adequate mitigating controls, such as formal and well-documented reviews of SAP system log reports to prevent and detect any unauthorized activity resulting from the control weakness.

Below are significant findings and areas of concern noted during a limited review of SAP user account management activity:

- At least five user administrators performed incompatible functions in creating users and assigning profiles/roles to users. Three of the five also created or changed profiles.
- The same SAP Services administrator associated with Finding 1 had two active personal[12] user accounts in SAP as of January 2011, and at least a third personal user account deleted in April 2008:
  - All three of the user accounts had unrestricted access at various points in time through assignment of the powerful profile SAP_ALL.
  - The administrator created a user account and assigned the SAP_ALL profile to himself.
  - One user account was assigned the SAP_ALL profile for an uninterrupted period of approximately 10 months, until removed by another SAP Services administrator.
- An SAP Services developer, who should not have privileged access in the SAP ECC production system, had use of three user accounts in the City's SAP ECC production system. Information systems security control standards require separation of duties for development, testing, and production systems to prevent any unauthorized changes to production systems. We found:
  - Two of the developer's accounts were assigned unrestricted SAP_ALL profile access in the production system.
  - The developer created a user account for himself.

[11] SAP user administrators may customize and restrict levels of access to SAP through assignment of roles and/or profiles to user accounts, which at a granular level can determine an SAP user's level of access.

[12] We deemed an account to be a "personal" account if it could be clearly identified with an individual based on name or employee identification number.

- SAP Services staff stated they use powerful system-provided user accounts by resetting passwords or sharing passwords.
- SAP Services staff performed incompatible duties by directly accessing Human Resources department records and entering identification information for City employees.

Cybercrime reports suggest the need to restrict and control system administrator access

A 2009 CERT Software Engineering Institute report on insider threats[13] warns that system administrator and technical or privileged users have the technical ability, access, and oversight responsibility to commit and conceal malicious activity. The report states:

- A majority of the insiders who committed sabotage, and over half of those who stole confidential or proprietary information, held technical positions.
- System administrators and technical or privileged users can usually conceal their actions, since their privileged access typically provides them the ability to log in as other users, to modify system log files, or to falsify audit logs and monitoring reports.

The “2010 CyberSecurity Watch Survey: Cybercrime Increasing Faster Than Some Company Defenses” report[14] stated:

- 60% of survey respondents experienced at least one cybersecurity event, an adverse event that threatens some aspect of computer security.
- Respondents experiencing a cybercrime experienced a mean monetary loss of $394,700.
- Those experiencing a cybersecurity event reported 26% (on average) of events were caused by an insider (current employees or contractors).

Exhibit 3 shows some of the mechanisms used by insiders in committing electronic crimes from August 2008 through July 2009.

[13] The “Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1” report was published by the Software Engineering Institute CERT Program at Carnegie Mellon University.

[14] The survey was conducted from July 29, 2009 through August 20, 2009, with 523 responses being collected by *CSO (Chief Security Officer)* magazine in cooperation with the United States Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte. Respondents were asked to report based on cybersecurity events occurring in the past 12 months (August 2008 through July 2009).

Exhibit 3: Examples of mechanisms used by insiders to commit electronic crimes

Mechanism used **(August 2008 through July 2009):**	
Shared account	33%
Used their own account	33%
Compromised an account	28%
Used authorized system administrator access	25%
Remote access	25%
Escalated privileges	22%
Backdoors	13%

Source: 2010 CyberSecurity Watch Survey

The reports summarized above highlight the need for appropriately restricting and controlling system administrators' access. Accordingly, ASD should take steps to ensure:

- SAP administration functions are properly segregated.
- System access is appropriately restricted or controlled for all technical staff.
- Detective and monitoring mechanisms compensate for any control weaknesses.

RECOMMENDATION #5 To ensure SAP user account administration functions are properly separated, ASD should:

- Segregate responsibilities for creating and maintaining roles/profiles, assignment of roles/profiles, and creating and maintaining user accounts.
- Prohibit IT staff from maintaining Human Resources Department employee records.
- Assign all SAP user administrators to a designated SAP user group, preventing them from managing their own and other administrators' accounts and access levels, and designate an individual to manage the SAP user group.

Page intentionally left blank

Finding 3: ASD has not effectively managed all SAP user accounts to ensure system security

ASD has not effectively managed all SAP user accounts to ensure system security. Specifically, ASD has not consistently removed or disabled SAP employee user accounts in a timely manner and has not adequately secured and controlled non-employee user accounts. While ASD lacks an effective user account identity management system, improvements were made during the audit.

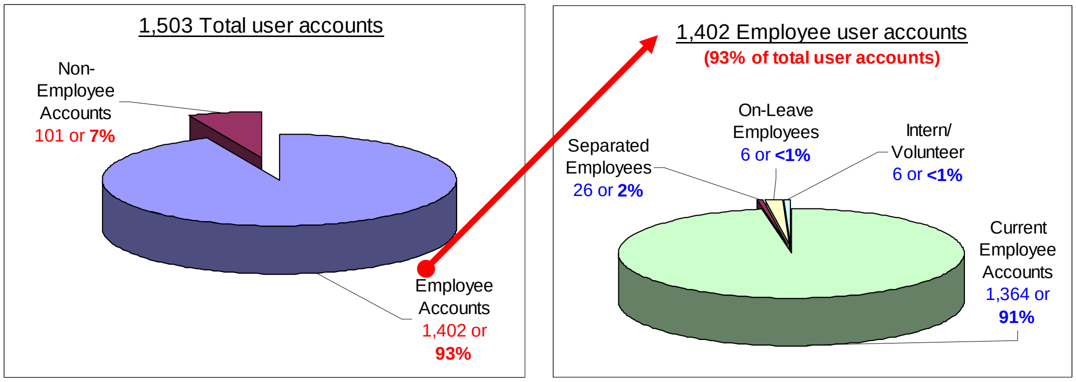
ASD has not removed or disabled SAP employee user accounts in a timely manner

As of January 25, 2011, an SAP system report listed a total of 1,503 user accounts including, 1,402 employee accounts[15] and 101 non-employee accounts.

Exhibit 4 below shows the 1,402 SAP employee user accounts:

- 1,364 matched Human Resources Department records of current employees.
- 38 did not match Human Resources Department records, and consisted of 26 separated employees, 6 on-leave employees, and 6 intern or volunteer employees.

Exhibit 4: Analysis of SAP Employee User Accounts



Source: Auditor's analysis of SAP user accounts and Human Resources Department records

Recognized information systems security control frameworks require timely termination of user access:

- PCI DSS states access should be immediately terminated for any separated users, and that organizations should remove/disable inactive user accounts at least every 90 days.
- NIST SP 800-53 states organizations should secure information systems and information formerly controlled by a separated individual, and that timely termination of information system access is especially important if employees or contractors are terminated for cause.

Of the 26 separated employee user accounts, 17 were not removed or disabled in a timely manner after the employee separated. These accounts remained enabled on

[15] Interns and volunteers are included under the general category of employee user accounts.

average for 577 days after the separation date,[16] and in one instance an account remained enabled for 1,727 days. As of February 15, 2011, staff had removed all but three of these user accounts.

We compared Human Resources Department records of City employee separations with SAP records of user account removals. The comparison revealed lags and spikes, in SAP user account removal, suggesting the level of coordination between SAP user account management and Human Resources Department activity was not optimal, and that access to SAP for separated employees may not have been terminated in a timely manner.

ASD lacks policies and procedures for ensuring separated employees' SAP access is terminated in a timely manner and coordinated with Human Resources Department processes.

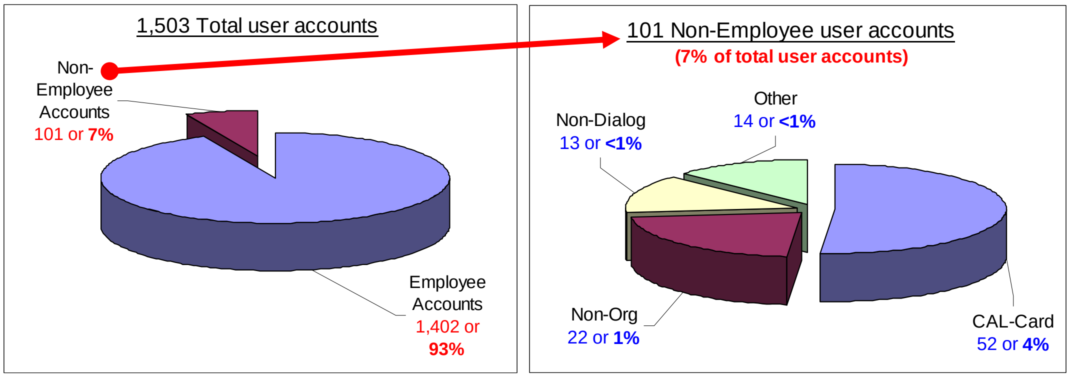
RECOMMENDATION #6: Develop and implement policies and procedures to ensure SAP access for separated City employees is terminated in a timely manner and coordinated with Human Resources Department processes.

ASD has not adequately secured and controlled non-employee user accounts

We classified the 101 non-employee user accounts that did not reconcile to Human Resources Department records into groups. These user accounts pose unique, inherent risks varying in type and degree.

Exhibit 5 shows our classification of the 101 non-employee user accounts based on identification information available in SAP.

Exhibit 5: Analysis of SAP Non-Employee User Accounts



Source: Auditor's analysis of SAP user accounts and Human Resources Department records.

52 "CAL-Card" user accounts

PCI DSS states that generic accounts and passwords should not be used to ensure an organization can identify who is responsible for system activity. Any use of such

[16] This is an average of the total number of days from employee separation date to the earlier of January 25, 2011, or the date the account was removed or disabled.

accounts should be specifically authorized by management on an exception basis to meet business needs.

We found 52 active generic[17] SAP user accounts associated with the City's Purchasing Card (CAL-Card) program. These generic accounts are "dummy accounts" used by ASD to transfer and retain records of CAL-Card transactions associated with a cardholder account that has been compromised. Upon receiving a new purchasing card, a cardholder's transaction history up until the incident may be transferred to the generic user account. These generic user accounts could be used to perform unauthorized transactions without accountability if enabled through assignment of "roles" and/or "profiles."

Currently ASD does not have a formal process for managing these "dummy accounts." At a minimum, the City should take precautions and lock these accounts and assign them to a restricted user group to prevent unauthorized access or use. The City did not have any policies or procedures addressing use of these accounts or controls to secure them. ASD should develop, design, and implement specific controls to mitigate risks associated with any use of these accounts.

RECOMMENDATION #7: ASD should either eliminate the 52 generic CAL-Card user accounts, or develop policies and procedures to implement compensating controls to:

- Ensure these accounts are secured.
- Establish individual accountability for their use.
- Allow use on an exception basis in meeting the City's business needs.

22 non-organizational user accounts

NIST states that vendor personnel and consultants may legitimately require privileged access to an information system; however, based on a prior assessment of risk, an organization should issue temporary access for a very limited period. NIST also provides that organizations should ensure individuals requiring access to organizational information and information systems sign appropriate access agreements, such as nondisclosure agreements, acceptable use agreements, and conflict-of-interest agreements, prior to being granted system access.

We identified 22 non-organizational accounts assigned to the City's SAP consultants (Sierra Infosys Inc. and Mindworks) and the City's solid waste, recyclable materials, organic materials, and yard trimmings collection and processing services provider (Greenwaste Recovery, Inc.). These 22 user accounts were comprised of:

- 12 enabled Sierra Infosys Inc. accounts
- 9 enabled Greenwaste Recovery, Inc. accounts
- 1 disabled Mindworks account

[17] Generic user accounts do not include identifying information associated with an individual.

According to an SAP Services manager, the City does not currently require non-organizational users to sign any type of access agreement or formally acknowledge the City's applicable information systems security policies.

We found the following areas of concern in reviewing these user accounts:

- Greenwaste Recovery, Inc. had 9 user accounts that did not have expiration dates to control potential unauthorized access resulting from staff turnover.
- The Sierra Infosys Inc. had 11 user accounts that had expiration dates of July 30, 2013, which is approximately three weeks beyond the contract expiration date. An expiration date that is that far in the future is not an adequate control.
- One Sierra Infosys Inc. user had privileged access, including authorization to manage SAP user accounts. SAP records indicated the account is valid through December 31, 2011. This level of privileged access combined with an expiration date far into the future could allow the user to enable other user accounts, such as one of the City's many generic user accounts, to conduct unauthorized activity without individual accountability.

During audit fieldwork, the ASD updated the "SAP Basis Administration" manual to provide guidance addressing proper levels of access and duration of access for external consultants. A detailed review of access levels provided to non-organizational users and their activity in SAP is beyond the scope of this audit.

RECOMMENDATION #8: ASD should develop formal policies and procedures that clearly classify non-organizational users and define for each class:

- Authorized access levels.
- Duration of access.
- Controls to ensure each class abides by the City's security policies.
- Controls to monitor SAP activity and to ensure SAP access levels and duration is consistent with policies and procedures.

<u>13 "non-dialog" accounts</u>

The NIST SP 800-53 concept of "least privilege" is defined in Finding 2 as limiting user access based on job responsibilities to accomplish assigned tasks in accordance with organizational missions and business functions. The concept of least privilege also applies to non-dialog accounts, which are generally used by administrators for a variety of technical purposes, such as background processing and communication within a system and between multiple systems. Non-dialog accounts should only have the level of access necessary to accomplish assigned tasks in accordance with organization's mission and business functions.

Of the City's 1,503 SAP user accounts, 1,490 were "dialog" accounts, which by definition are designed for individual interactive access in SAP, and 13 were non-dialog user accounts, which are generally used by administrators for technical purposes. We found that ASD had assigned the SAP_ALL profile to 6 of the 13 non-dialog accounts, allowing unrestricted system access. As discussed in Finding 2, by assigning the standard

SAP_ALL profile, ASD violated the principles of least privilege and segregation of duties. A user account with unrestricted access could allow misuse and exposure of sensitive data including confidential City employee and customer information, sabotage and operational disruptions in SAP, financial losses, and damage to reputation.

According to an SAP Services manager, removing the SAP_ALL profile assigned to non-dialog user accounts would result in disruptions in SAP. However, authoritative literature on SAP states the SAP_ALL profile should not be assigned to any user account, including non-dialog accounts. The City did not have any policies or procedures addressing non-dialog user accounts to ensure their use is properly authorized, restricted, and monitored.

RECOMMENDATION #9: ASD should develop policies and procedures to address use of non-dialog user accounts. These policies and procedures should address:

- Authorization to use and assignment of non-dialog accounts.
- Permitted use for each account.
- Individual accountability for use.
- Controls to monitor use.

<u>14 other generic accounts</u>

As previously stated, recognized information systems security control frameworks recommend against the use of generic user accounts. The remaining 14 user accounts we identified did not have adequate identifying information needed to ensure individual accountability for use, and were not documented or addressed in ASD policies and procedures. These consisted of:

- 9 user accounts whose function or use could not be identified.
- 2 user accounts associated with a non-organizational SAP services provider (these were assigned unrestricted access through assignment of the SAP_ALL profile, as discussed in Finding 2).
- 1 user account whose stated function is “data migration.”
- 1 powerful system-provided user account, which is addressed in Finding 1.
- 1 “template” user account.

Although there may be legitimate uses for all of these user accounts, ASD should ensure they are properly documented, authorized, and associated with the individual responsible for their use. Generic user accounts could be used to perform unauthorized transactions without accountability if enabled through assignment of roles and/or profiles. At minimum the City should take precautions and lock these accounts when not specifically authorized for use, and assign them to a restricted user group to prevent unauthorized access or use.

RECOMMENDATION #10: ASD should as a rule prohibit the use of generic user accounts, in following PCI DSS and NIST control frameworks. ASD should develop policies and procedures to address the use of any generic user accounts on an exception basis to meet the City's business needs and to ensure adequate compensating controls are implemented and include:

- Formal authorization for use
- Permitted levels of access
- Duration of use and procedures to disable or remove
- Permitted use or function
- Individual accountability for use

ASD should establish an effective user account identity management system

In accordance with NIST and PCI DSS standards, all users, employee and non-employee, should be uniquely and readily identifiable to ensure accountability and to facilitate any investigations or audits of user activity. Additionally, SAP system records should include a predetermined minimum level of identifying information for all SAP user accounts, including name, department (or organization), and employee identification number (if applicable), to ensure user accounts can be validated through a comparison with an independent source such as Human Resources Department records.

In assessing SAP user accounts, we noted a lack of consistent and reliable identifying information required to facilitate validation of SAP user accounts through a comparison with Human Resources Department employee records that are presumably independently maintained. For example, in our review of 1,402 City employee SAP user accounts, we noted only 301 included the unique employee identification number that is assigned to each employee. Therefore, we could not use the employee identification number to perform a direct comparison with Human Resources Department records.

ASD's use of a manual processes to administer, create, change, and terminate SAP user accounts is insufficient to manage user access.

<u>ASD implemented controls to facilitate reconciliation of Human Resource, Windows NT (network), and SAP user account and identification data</u>

During audit fieldwork, ASD developed a report set up to run on a weekly basis, which facilitates comparison of Human Resources Department, Windows NT (network), and SAP user account and identification data. Staff provided examples of the report that showed it will identify:

- Inconsistencies in the City's Human Resources, Network, and SAP user account identification information, including name, user id, and phone number.
- SAP user accounts that do not correspond to Human Resources department records of active employees.

ASD has also identified needed improvements to user account management including:

- A process to automate removal of SAP user accounts upon employee termination.
- An automated process for entering and managing Human Resources Department user account identification information. Currently, SAP Services staff manually inputs user account identification information into Human Resources Department records.

A detailed review of the adequacy and effectiveness of these processes and controls is beyond the scope of this audit.

RECOMMENDATION #11: ASD should establish policies, procedures, and processes to ensure:

- SAP user administrators are aware of the required identification information for each type of SAP user account, and SAP is configured to require, to the extent possible, input of required information.
- SAP user accounts contain all required user identification information, consistent with Human Resources Department records and/or other applicable independent authorized lists for City employees.
- The City is compliant with PCI DSS and NIST SP 800-53 standards in its management of SAP user accounts.

Page intentionally left blank

Finding 4: The City needs to formally adopt and implement a recognized information systems control standard to ensure SAP security

The City has not adopted and implemented a recognized information systems security control standard or framework needed to demonstrate control effectiveness in a consistent and repeatable manner, and it has not complied with requirements for business entities that process credit card transactions. Missing or inadequate controls include:

- Security policies and procedures and assignment of responsibility for SAP security.
- Security awareness and training program.
- Information systems risk assessment.
- Proper configuration of SAP system security settings.
- Effective management of SAP audit trails (logs).
- Safeguarding and controlling sensitive production data used for testing.
- Ensuring the Auditor's Office access levels in SAP is optimized.

During audit fieldwork, ASD developed and began implementing procedures and processes to address some areas of concern including security of system-provided accounts and user account administration. We recommend ASD assess SAP security risks and implement needed controls through a comprehensive process that is informed by controls stated in the Payment Card Industry Data Security Standard, National Institute of Standards and Technology's Special Publication 800-53, and other applicable frameworks.

ASD has not adopted or implemented a recognized information systems security control standard

The City's SAP system is used to store and process City staff and City resident personally identifiable information.[18] Governmental and private agencies have developed and published control frameworks to provide guidance for securing information systems to preserve confidentiality, integrity and availability of an organization's data.

The City is required by the Payment Card Industry Security Standards Council (PCI SSC) and the City's merchant bank, Wells Fargo, to comply with the Payment Card Industry Data Security Standard (PCI DSS), which is a set of 12 high level control requirements for protecting cardholder data. The PCI DSS controls mirror security best practices, and are comparable with controls stated in other recognized frameworks such as the National Institute of Standards and Technology's Special Publication 800-53 (NIST SP 800-53). Both PCI DSS and NIST SP 800-53 frameworks provide a comprehensive set of controls to protect data in critical information systems. Effective

[18] Personally identifiable information refers to any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, or biometric records, and any other information which is linked or linkable to an individual, such as medical, educational, financial, and employment information.

implementation of these control frameworks would provide a strong foundation for information systems security, and would enhance the City's ability to prevent the security vulnerabilities identified in Findings 1, 2, and 3.

The PCI DSS requirements apply to all "system components" such as any network component, server, or application included in or connected to the cardholder data environment. In order to validate PCI DSS compliance, the City must successfully:

- Complete an annual "Self-Assessment Questionnaire" (SAQ), to validate compliance with each of the PCI DSS requirements.
- Complete a passing vulnerability scan with a PCI SSC "Approved Scanning Vendor" (ASV) and obtain evidence of passing scan from the ASV.
- Complete the "Attestation of Compliance" (AOC) in its entirety.
- Submit the SAQ, evidence of a passing scan, and the AOC, along with any other requested documentation to the "acquirer" (merchant bank).

In July 2010, Wells Fargo notified the City of the requirement to validate PCI DSS compliance or to become compliant by October 1, 2010. In the event of a security breach that exposes personally identifiable information, consequences for the City may include imposed regulatory notification requirements, loss of reputation and customers, financial liabilities, and litigation. According to Wells Fargo, if cardholder data is compromised, a merchant may be subject to the following liabilities and fines associated with non-compliance:

- Potential fines up to $500,000.
- All fraud losses incurred from the use of the compromised account numbers.
- Cost of re-issuing cards associated with the compromise.
- Cost of any additional fraud prevention/detection activities required by the card associations or costs incurred by credit card issuers associated with the compromise.

ASD has not adopted and implemented either the PCI DSS or NIST SP 800-53 control frameworks, and ASD does not have a coherent strategy to implement them. We also found the City's former external auditor, Maze & Associates, had consistently recommended adoption of the mandated PCI DSS standard and the optional NIST SP 800-53 control framework. In its fiscal year 2008 report to the City, Maze & Associates recommended the City comply with PCI DSS. The City's response to the 2008 report indicated it would comply. In a 2009 report, Maze & Associates concluded the City was not in compliance with PCI DSS and stated, "The City should make PCI DSS compliance a top priority." Maze & Associates also highly recommended compliance with the optional NIST SP-800-53 framework. Maze & Associates reiterated its recommendation that the City adopt and implement the PCI DSS and NIST frameworks in other reports dated 2009 and 2010. ASD reports the City implemented selected controls in September 2009 to protect credit card data, however, we did not find any evidence that the City made significant progress in planning, implementing, or validating full compliance with either the PCI DSS or NIST control frameworks despite the City's responses to the Maze & Associates reports. The need to adopt and implement a security standard is highlighted in a 2010 Maze & Associates report on the City's information systems, which states the City had a "HIGH" external attack risk, indicating some vulnerabilities could have been used to infiltrate or “hack” into the City’s information systems.

RECOMMENDATION #12: ASD should adopt and implement PCI DSS and NIST SP 800-53 information systems security control frameworks to help ensure security of the City’s key information systems.

ASD does not have a comprehensive security policy

PCI DSS requires organizations maintain a formal security policy that addresses information security for all personnel, sets the security tone for the whole entity, and informs personnel (including contractors and consultants) what is expected of them. PCI DSS states the information security policy should accomplish the following:

- Address all PCI DSS requirements.
- Include an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.
- Include an annual review and updates when the environment changes.

NIST SP 800-53 recommends policies and procedures addressing key security controls including access control, security awareness and training, configuration management, risk assessment, and incident response.

According to the City’s former Chief Information Officer, the City does not have a formal security policy that addresses SAP security. The City does have a formal computer use policy available on the City’s intranet, which addresses the security of the City’s information systems in a general sense. However, the policy is dated April 2005, and is not specific or adequate by itself to ensure SAP security or compliance with PCI DSS or other control standards.

We did not find any security formal policies and procedures addressing areas of concern discussed in this audit, such as**:**

- Use of system-provided (standard) user accounts
- Incident response
- Management of access to SAP logs and Oracle database logs
- Privileged or “superuser” access
- Use of system-provided SAP profiles (such as “SAP_ALL” and “SAP_NEW”)
- SAP system parameters (including security parameters and log settings)
- Use of unique user accounts and accountability issues
- Use of “generic” or “group” accounts
- Separation of duties in the context of SAP security, user account management, and SAP environments
- Security awareness and training
- Accountability for SAP security and consequences for any lapses in security

- Management of SAP user account identifying information
- Timely review of user accounts to ensure all access is valid

During audit fieldwork, the ASD began drafting procedures to address use of standard SAP user accounts.

In addition to implementing controls stated in PCI DSS and NIST SP 800-53, we suggest ASD refer to the following publications in developing a comprehensive security policy:

- NIST SP 800-18, Revision 1: Guide for Developing Security Plans for Federal Information Systems
- SANS Institute InfoSec Reading Room: Information Security Policy - A Development Guide for Large and Small Companies

RECOMMENDATION #13: ASD should develop and implement a formal and comprehensive security policy consistent with PCI DSS, NIST, the SAP Library, and other industry standards.

ASD has not formally assigned responsibility for SAP security

PCI DSS and NIST SP 800-53 require organizations formally assign responsibility for information security management. NIST SP 800-53 states an information security officer should have the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. According to PCI DSS, information security management responsibilities include:

- Establishing, documenting, and distributing security policies and procedures.
- Monitoring and analyzing security alerts and information.
- Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Administering user accounts, including additions, removals, and modifications.
- Monitoring and control of all access to data.

Although ASD has informal processes and/or procedures that directly or indirectly address these areas, the City does not have an information security officer and the responsibility for SAP security has not been formally assigned.

RECOMMENDATION #14: ASD should formally assign responsibility for SAP security.

ASD does not have a formal information systems security awareness and training program

PCI DSS and NIST SP 800-53 address the need for a formal security awareness program, security training, and a process to manage and monitor training records. An adequate information systems security awareness and training program should ensure:

- SAP technical staff is aware of current SAP system controls and practices required to secure the City's information systems.
- The City is able to plan, monitor, and assess the adequacy of individual and collective staff skills and competencies pertaining to SAP security administration.
- City staff and any consultants provided access to SAP (and other information systems) are aware of relevant security risks and their responsibilities for complying with applicable security policies and procedures.

ASD has not established a formal information security awareness and training program. Such a program would aid the City in ensuring that technical staff, as well as City staff and consultants that have access to SAP and other information systems, are aware of relevant security risks and their responsibilities for complying with applicable policies and procedures.

Furthermore, ASD has not established formal development plans or maintained training records for staff responsible for administering or managing SAP system security. An SAP Services manager confirmed SAP Services administrators have not received formal training on SAP security. Moreover, staff stated there is no training budget for SAP Services staff, and that SAP-specific courses are expensive. ASD has developed an informal system to track the competency of staff, and to track internal "study" meetings designed to enhance competencies and capabilities. The SAP Services manager provided a summary on the education, training, and experience of key SAP Services staff for the purposes of this audit. There was no evidence staff attended training on information systems security or SAP security. Moreover, available City records do not show any formal training provided to two key SAP Services administrators with security roles and responsibilities.

ASD should refer to guidance in NIST SP 800-50 (Building an Information Technology Security Awareness and Training Program) and NIST SP 800-16 (Information Technology Security Training Requirements: A Role and Performance Based Model) in implementing a comprehensive security awareness and training program.

RECOMMENDATION #15: ASD should implement a formal security awareness and training program that meets minimum control standards stated in PCI DSS and NIST control frameworks. The program should include provisions to ensure SAP technical staff is trained on current SAP security controls and practices.

ASD does not have a formal risk assessment process to effectively identify and manage information systems security and business risks

PCI DSS and NIST SP 800-53 require organizations establish a formal process to effectively and routinely identify, rank, and record threats, and vulnerabilities. A formal risk assessment process is needed to help identify and assess actual and potential vulnerabilities, threat sources, and security controls planned or in place, and the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the City's information systems and the information it processes, stores, or transmits.

ASD has not developed and implemented a formal risk assessment process for SAP. The City's SAP system is a complex and integrated information system. Without a formal risk assessment process, the City may not be able to effectively identify, assess, and manage risks associated with SAP and other integrated information systems.

NIST SP 800-39 (Managing Information Security Risk), NIST SP 800-18 (Guide for Developing Security Plans for Federal Information Systems), and NIST SP 800-30 (Risk Management Guide for Information Technology Systems) provide guidance on how to implement a risk assessment process for information systems. ASD should refer to these documents in developing and implementing a formal risk assessment process for SAP and other information systems.

RECOMMENDATION #16: ASD should implement a formal risk assessment process that meets minimum standards stated in PCI DSS and NIST SP 800-53 to ensure key information system threats and vulnerabilities are routinely (at least annually) and effectively identified, ranked, and addressed.

ASD has not properly reconfigured key SAP system security parameters

SAP supplies default settings for system parameters, which are not always consistent with the minimum level of security required by PCI DSS or suggested by other authoritative sources. PCI DSS specifies organizations should not use vendor-supplied security settings because these settings are well known and could allow malicious individuals to compromise or misuse systems. PCI DSS requires organizations develop and implement configuration standards consistent with current information systems security standards to address all known security vulnerabilities. Similarly, NIST SP 800-53 states organizations should establish and document mandatory application configuration settings that reflect the most restrictive mode consistent with operational requirements, and that these settings are appropriately monitored and controlled.

Our review of 16 SAP security parameters related to password and login controls security found:

- 12 of the 16 default settings did not support the minimum level of security required by PCI DSS or suggested by an authoritative ISACA (formerly the Information Systems Audit and Control Association) publication on SAP security.
- ASD changed only 2 of the 16 system parameters from the SAP default settings.[19] In both cases where the setting was changed, the new setting did not support the minimum level of security required by PCI DSS.

We selected 7 of the 16 settings for a more detailed review. As shown in Exhibit 6, five SAP system security parameters included in our review did not support the minimum level of security required by PCI DSS.

[19] The two system parameters are shown in Exhibit 6, which shows 7 of the 16 system parameter settings that should support the minimum level of security required by PCI DSS.

Exhibit 6: Comparison of seven selected SAP parameter settings with PCI DSS

SAP Parameter Description	City of Palo Alto SAP Setting	PCI DSS Recommended Setting	Was Parameter Reconfigured?	Does Setting Comply with PCI DSS?
Number of times a user can enter an incorrect password before being locked out of the system	5	6 or less	**N**	**Y**
Minimum number of digits in passwords	0	More than 0	**N**	**N**
Minimum number of letters in passwords	0	More than 0	**N**	**N**
Minimum password length	6	7	**N**	**N**
Number of days after which a password must be changed	180	90 or less	**Y**	**N**
Number of records to be stored in the password history (to prevent reuse)	5	4	**N**	**Y**
Number of seconds a user can be idle before the user is logged off automatically	14,400 (4 hours)	900 or less (15 minutes or less)	**Y**	**N**

Source: SAP parameter report and PCI DSS

Most SAP system parameter settings in the above exhibit heighten the risk of unauthorized access to the City's SAP system because the settings:

- Permit a user to remain idle for 4 hours before being automatically logged off instead of the recommended 15 minute (or less) interval. The drastically increased interval may create an opportunity for an unauthorized user to take over and perform unauthorized activity in SAP if the authorized user walks away from their workstation. The risk is heightened considering access to SAP is provided not only to in-house staff, but also to consultants and others who access SAP remotely.

- Do not require password changes until 180 days instead of the recommended 90 days. The increased interval could allow more time for a malicious individual to find weak accounts.

- Do not require the use of digits and letters in passwords, and require passwords be only 6 characters (instead of the recommended 7 characters). Strong passwords are the first line of defense for information systems since a malicious individual will often first try to find accounts with weak, short, or simple to guess passwords.

ASD does not have an approved policy addressing SAP system parameter settings. ASD's policy addressing SAP system parameter settings should be consistent with a formal citywide policy on security settings for information systems. In order to meet security standards, the City should consider using a “security configuration checklist,” which is a series of instructions or procedures for configuring information systems to meet operational requirements.

RECOMMENDATION #17: ASD should develop and implement formal policies and procedures to ensure SAP security parameters are properly configured and compliant with PCI DSS, NIST SP 800-53, and other applicable industry standards.

ASD has not restricted access to SAP security parameters

The capability to configure SAP system parameters should be restricted to avoid unauthorized changes to critical system parameters, including security settings. NIST SP 800-53 states organizations should establish and document mandatory configuration settings and implement controls to ensure information system configuration changes are properly planned, authorized, executed, and monitored. It also states organizations should define, document, approve and enforce access restrictions associated with changes to an information system that could have significant effects on the overall security of the system.

ASD does not have policies and procedures to restrict to SAP security parameters. We identified 17 SAP user accounts (9 of which were “dialog” accounts) with authorization to modify the SAP system parameters. Some of the 17 user accounts were generic and could not be associated with staff names. In addition, the user accounts that could be associated with staff names suggest that staff with different reporting lines had access to modify the SAP system parameters.

RECOMMENDATION #18: ASD should ensure access to SAP system parameters is restricted to only authorized staff, and that policies and procedures incorporate change controls stated in NIST SP 800-53 to ensure all changes are properly planned, authorized, executed, and monitored.

ASD has not developed policies and procedures to retain, review, and analyze SAP audit trails (logs)

SAP systems provide a variety of logs for system administration, monitoring, problem solving, and auditing purposes. The logs are important for monitoring system security and to support investigations in the event of a security breach. SAP systems can be configured to determine the amount and type of log data, if any, that is retained by the system and where it is specifically stored. Formal policies and procedures should ensure SAP logs are properly configured, secured, and effectively and timely analyzed in order to:

- Establish accountability for transactions processed and any important changes in SAP.
- Facilitate detection and assessment of security incidents.

NIST and PCI DSS security standards detail specific minimum controls required to properly manage and secure information system logs. These include:

- Policies and procedures to effectively manage system logs.
- Procedures to review and analyze system logs and report any findings to designated organization officials.
- Performing a risk assessment to determine what needs to be logged.
- Protection of logs from unauthorized access, modification, and deletion through processes such as recording logs on "write-once" media and/or backing up logs onto a separate system or media.
- Retaining logs for a specified period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.[20]

ASD does not have any policies and procedures addressing SAP log management. Specifically, we did not find any procedures addressing log configuration, retention, security, and roles and responsibilities for monitoring and analyzing logs. Because SAP logs were not effectively managed, we could not independently determine with certainty the duration of the security vulnerability resulting from the SAP* incident discussed in Finding 1, and individual accountability for the vulnerability. Specifically, our analysis in Finding 1 was limited because:

- The SAP log of user activity contained records dating back only to August 4, 2010, and ASD did not have a process to archive logs. As a result, records were not available to support our efforts in detecting potentially unauthorized SAP access using the unsecured SAP* user account prior to August 4, 2010**.** Moreover, staff also reported the Oracle database system[21] logging mechanism was not enabled. This further limited our ability to assess the SAP* security vulnerability identified in Finding 1 in terms of duration and accountability**.**

- The SAP logs that should indicate key security-related events did not appear reliable or complete, restricting our ability to assess the duration of the SAP* security vulnerability and to independently determine accountability for the vulnerability.

<u>ASD has not restricted access to audit logs for SAP Services staff with system security responsibilities</u>

NIST SP 800-53 requires separation of incompatible duties. It states that system administrators responsible for user access control functions should not administer audit functions. Monitoring and overall management of the logs for security reasons should be assigned to an individual responsible for SAP security who is not responsible for day-to-day administration of SAP and user account management. Segregating the responsibility for monitoring and managing logs from duties assigned to administrators with already privileged system access would enhance security by avoiding**:**

- Assignment of self-monitoring duties to SAP administrators and other technical staff whose activities should be subject to independent oversight.

[20] PCI DSS requires maintaining logs for at least one year.

[21] The underlying SAP database is an Oracle database.

- Assignment of monitoring duties to staff who may not have adequate expertise or dedicated time to review and analyze logs and security reports.
- Unauthorized modification or deletion of system logs in the event an administrator's user account, which has access to logs, is hacked.

ASD has not restricted access to audit logs for SAP Services staff with system security responsibilities. Specifically, SAP Services administrators responsible for user account management and management of access levels also perform monitoring activities using SAP logs. Our finding is consistent with a report dated June 9, 2009 from the City's former external auditor, Maze & Associates, which states: "The system administrators of the SAP system also review the audit logs of the system. The review of the audit logs, which is a security function, should be separate from the system administration function."

RECOMMENDATION #19: ASD should develop policies and procedures and implement minimum NIST SP 800-53 and PCI DSS controls applicable to log management in order to ensure:

- SAP and Oracle log data is secured using appropriate "write-once" media and/or backup procedures.
- Access to SAP and Oracle logs is restricted based on the principles of least privilege and segregation of duties.
- Accountability is established for monitoring SAP and Oracle logs and for reporting any incidents to the appropriate levels of management.
- SAP and Oracle are properly configured to ensure logs capture appropriate information and retain the information for an appropriate duration.

ASD uses live "production" data in the SAP quality assurance system without measures to "anonymize" or protect the data

The SAP manual recommends implementation of three separate systems in order to make and test changes to SAP applications without interfering with live operational data**.** ASD records indicate that for each of the City's five SAP systems, the City has implemented three discrete working environments:

1. Production – contains live operational data and transactions
2. Development – used mainly by developers to conduct program testing
3. Quality Assurance – used by analysts and users to conduct system and acceptance testing

Recognized information systems control frameworks require safeguards to protect sensitive data[22] used in testing or development of information systems:

[22] Sensitive data includes information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

- NIST SP 800-122 states that while testing generally should simulate real conditions as closely as possible, any personally identifying information should be protected at the same level that it is protected in the production environment, which can add significantly to the time and expense of testing the system. NIST SP 800-122 states personally identifying information may be anonymized[23] prior to use in testing or development environments to protect the information.

- PCI DSS states production data containing credit card holder account numbers should not be used for testing or development because security controls are usually not as stringent in these environments.

According to an SAP Services manager, all live production data is transferred to the SAP quality assurance SAP system. The manager stated the SAP quality assurance system is configured like the production system. As discussed in this report, we noted significant security vulnerabilities in the SAP Enterprise Resource Planning Central Component (SAP ECC) production system, which raised concerns regarding the use of any sensitive production data in the quality assurance system. Our concerns were further validated by a report suggesting standard user accounts in the quality assurance system were not properly secured.[24]

ASD does not have policies and procedures to provide safeguards in using live production data for testing purposes in the quality assurance system or to ensure transfer of production data is properly authorized. An assessment of security controls in the SAP quality assurance system was beyond the scope of this audit.

ASD should refer to NIST Special Publication 800-122 (Guide to Protecting the Confidentiality of Personally Identifiable Information) in developing detailed policies and procedures to protect sensitive data in SAP.

RECOMMENDATION #20: ASD should develop policies and procedures consistent with PCI DSS, NIST SP 800-53, and NIST SP 800-122 to ensure:

- Any sensitive production data used in the SAP quality assurance system is anonymized or otherwise properly safeguarded through implementation of recommended controls.
- Transfer of any sensitive production data is formally authorized by departments or individuals responsible for the data.

Implementing the SAP system-provided tool Audit Information System (AIS) would enhance the Auditor's Office access and the effectiveness of future security reviews

The Palo Alto City Charter and the Palo Municipal Code provide the Auditor's Office the authority to conduct audits and examinations of any City department, program, service, or activity. The purpose of these audits and examinations is to provide the City Council and City management with information and evaluations regarding the effectiveness and

[23] Anonymizing information involves removal of identifying characteristics from sensitive data in order to prevent misuse or unauthorized disclosure. The anonymized information can retain its useful and realistic properties for the purpose of system testing.

[24] Finding 1 provides an overview and detailed discussion of SAP standard user accounts.

efficiency with which City resources are employed, the adequacy of the system of internal controls, and compliance with City regulations and policies and procedures.

The Municipal Code also requires that the Office of the City Auditor conduct audits in accordance with Government Auditing Standards, as established by the United States Government Accountability Office. These standards require the findings and conclusions identified in performance audits be supported by sufficient and appropriate evidence.

The Palo Alto Municipal Code provides that the Office of the City Auditor will have unrestricted access to obtain sufficient and appropriate evidence to conduct audits. Specifically, the Palo Alto Municipal Code states, “The city auditor will have <u>unrestricted</u> (emphasis added) access to all sources of information, property, and personnel relevant to the performance of a council-approved audit, unless prohibited by law.”

Because SAP supports the City’s core business functions, unrestricted read-only access is essential to conducting most audits. The Auditor’s Office, however, did not have the optimum level of access in SAP to conduct this audit. For instance, we did not have independent access in SAP to key reports such as system security reports and logs needed to independently assess system security and the risk of fraud and abuse. To obtain the required information, the Auditor’s Office needed to rely on ASD to provide reports and logs. Although ASD provided most of the requested information, this process wasted the time of both ASD and audit staff.

SAP offers a free auditing tool called “Audit Information System” (AIS) for external, internal, system, and data security auditing functions that is designed to improve audit quality and facilitate the audit process. AIS was delivered with the City’s SAP system, and we confirmed it is operational, however, it has not been configured or tested by staff, and the Auditor’s Office does not have access to it. AIS is also designed to be compatible with other audit tools and techniques, such as the data analytic software known as ACL, which is actively used by the Auditor’s Office staff. In reviewing guidance on AIS, we also found that it includes reports to review system security, including system logs and reports on the status of standard users including “SAP*,” which is discussed in Finding 1.

Providing the Auditor’s Office with direct access to required SAP reports would have both enhanced our independence and minimized our reliance on staff. Future SAP audits and all other audits requiring access to the City’s information systems will benefit from an established and optimized level of access for the auditors.

During the course of the audit, the Auditor’s Office met on several occasions with the ASD Director and staff to discuss the Auditor’s Office’s access to SAP and access to AIS. While ASD staff is not opposed to providing the Auditor’s Office with AIS, it is not high priority for implementation considering that ASD is behind in implementing other projects.

RECOMMENDATION #21: To enhance the Auditor’s Office’s efficiency and independence in conducting audits, and its ability to ensure compliance with generally accepted government auditing standards, we recommend ASD implement the AIS tool and provide the Auditor’s Office with access to it.

Conclusion

The City's SAP Enterprise Resource Planning system supports its core business functions and management of information. An unsecured system-provided SAP user account with unrestricted access resulted in a significant security vulnerability, and ASD violated two critical security principles by not properly restricting access for all user accounts. Moreover, ASD has not formally adopted and implemented all controls needed to effectively manage SAP user accounts to ensure system security. The Auditor's Office recommends formal adoption of the PCI DSS and NIST SP 800-53 security control frameworks and further security assessments of the City's information systems using a risk-based approach.

Recommendations

Our report includes a total of 21 recommendations to improve the security of the City's critical information systems. The audit recommendations in the report are addressed to ASD, however, the former Information Technology Division in ASD has been established as a City department with a Chief Information Officer reporting to the City Manager. The new department will be responsible for implementing these recommendations.

RECOMMENDATION #1: ASD should develop and implement formal policies and procedures addressing standard SAP user accounts in order to:

- Secure standard user accounts and prevent unauthorized use.
- Detect on an ongoing basis any unsecured standard accounts and any unauthorized use.
- Ensure standard user accounts can only be managed by a designated individual(s).
- Authorize use only if appropriate, and ensure there is accountability for any use.
- Ensure any authorized use is monitored.

RECOMMENDATION #2: ASD should further investigate the following:

- Staff's account that SAP* was left unsecured after installing an SAP support pack in December 2010.
- Responsibility for the deletion and recreation of the SAP* user master record.
- Responsibility for missing log records.

RECOMMENDATION #3: To ensure the City can appropriately respond to SAP security incidents, ASD should develop and implement a comprehensive incident response plan that meets PCI DSS and NIST control standards and includes provisions to address:

- Incident response policies and procedures
- Incident response training
- Monitoring and reporting

- Roles and responsibilities
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements in reporting compromises

RECOMMENDATION #4: To mitigate risks associated with assignment of unrestricted SAP access, ASD should:

- Formally adopt policies and procedures addressing SAP user access that are consistent with the principles of least privilege and segregation of duties.
- For emergency purposes, ASD should consider creating a single unrestricted account assigned the SAP_ALL profile that is appropriately secured and controlled in accordance with SAP guidelines and industry standards.
- Implement policies and procedures to either prohibit or control the use of all other powerful system-provided SAP profiles.
- Ensure needed SAP roles and profiles are approved by management and included in the City's role authorization procedures, and that unauthorized roles and profiles are not assigned.
- Develop procedures to detect any unauthorized roles or profiles assigned to users.

RECOMMENDATION #5 To ensure SAP user account administration functions are properly separated, ASD should:

- Segregate responsibilities for creating and maintaining roles/profiles, assignment of roles/profiles, and creating and maintaining user accounts.
- Prohibit IT staff from maintaining Human Resources Department employee records.
- Assign all SAP user administrators to a designated SAP user group, preventing them from managing their own and other administrators' accounts and access levels, and designate an individual to manage the SAP user group.

RECOMMENDATION #6: Develop and implement policies and procedures to ensure SAP access for separated City employees is terminated in a timely manner and coordinated with Human Resources Department processes.

RECOMMENDATION #7: ASD should either eliminate the 52 generic CAL-Card user accounts, or develop policies and procedures to implement compensating controls to:

- Ensure these accounts are secured.
- Establish individual accountability for their use.
- Allow use on an exception basis in meeting the City's business needs.

RECOMMENDATION #8: ASD should develop formal policies and procedures that clearly classify non-organizational users and define for each class:

- Authorized access levels.
- Duration of access.
- Controls to ensure each class abides by the City's security policies.
- Controls to monitor SAP activity and to ensure SAP access levels and duration is consistent with policies and procedures.

RECOMMENDATION #9: ASD should develop policies and procedures to address use of non-dialog user accounts. These policies and procedures should address:

- Authorization to use and assignment of non-dialog accounts.
- Permitted use for each account.
- Individual accountability for use.
- Controls to monitor use.

RECOMMENDATION #10: ASD should as a rule prohibit the use of generic user accounts, in following PCI DSS and NIST control frameworks. ASD should develop policies and procedures to address the use of any generic user accounts on an exception basis to meet the City's business needs and to ensure adequate compensating controls are implemented and include:

- Formal authorization for use
- Permitted levels of access
- Duration of use and procedures to disable or remove
- Permitted use or function
- Individual accountability for use

RECOMMENDATION #11: ASD should establish policies, procedures, and processes to ensure:

- SAP user administrators are aware of the required identification information for each type of SAP user account, and SAP is configured to require, to the extent possible, input of required information.
- SAP user accounts contain all required user identification information, consistent with Human Resources Department records and/or other applicable independent authorized lists for City employees.
- The City is compliant with PCI DSS and NIST SP 800-53 standards in its management of SAP user accounts.

RECOMMENDATION #12: ASD should adopt and implement PCI DSS and NIST SP 800-53 information systems security control frameworks to help ensure security of the City's key information systems.

RECOMMENDATION #13: ASD should develop and implement a formal and comprehensive security policy consistent with PCI DSS, NIST, the SAP Library, and other industry standards.

RECOMMENDATION #14: ASD should formally assign responsibility for SAP security.

RECOMMENDATION #15: ASD should implement a formal security awareness and training program that meets minimum control standards stated in PCI DSS and NIST control frameworks. The program should include provisions to ensure SAP technical staff is trained on current SAP security controls and practices.

RECOMMENDATION #16: ASD should implement a formal risk assessment process that meets minimum standards stated in PCI DSS and NIST SP 800-53 to ensure key information system threats and vulnerabilities are routinely (at least annually) and effectively identified, ranked, and addressed.

RECOMMENDATION #17: ASD should develop and implement formal policies and procedures to ensure SAP security parameters are properly configured and compliant with PCI DSS, NIST SP 800-53, and other applicable industry standards.

RECOMMENDATION #18: ASD should ensure access to SAP system parameters is restricted to only authorized staff, and that policies and procedures incorporate change controls stated in NIST SP 800-53 to ensure all changes are properly planned, authorized, executed, and monitored.

RECOMMENDATION #19: ASD should develop policies and procedures and implement minimum NIST SP 800-53 and PCI DSS controls applicable to log management in order to ensure:

- SAP and Oracle log data is secured using appropriate “write-once” media and/or backup procedures.
- Access to SAP and Oracle logs is restricted based on the principles of least privilege and segregation of duties.
- Accountability is established for monitoring SAP and Oracle logs and for reporting any incidents to the appropriate levels of management.
- SAP and Oracle are properly configured to ensure logs capture appropriate information and retain the information for an appropriate duration.

RECOMMENDATION #20: ASD should develop policies and procedures consistent with PCI DSS, NIST SP 800-53, and NIST SP 800-122 to ensure:

- Any sensitive production data used in the SAP quality assurance system is anonymized or otherwise properly safeguarded through implementation of recommended controls.
- Transfer of any sensitive production data is formally authorized by departments or individuals responsible for the data.

RECOMMENDATION #21: To enhance the Auditor’s Office’s efficiency and independence in conducting audits, and its ability to ensure compliance with generally accepted government auditing standards, we recommend ASD implement the AIS tool and provide the Auditor’s Office with access to it.

CITY MANAGER'S RESPONSE TO THE SAP SECURITY AUDIT REPORT

Attachment A

Date: October 6, 2011

To: City Auditor

From: James Keene, City Manager

Prepared by: Lalo Perez, Director of Administrative Services (ASD)

The Administrative Services Department staff acknowledges and appreciates the detailed work of the City's Auditor Office (Auditor's Office) and is pleased to respond to the "SAP Security Audit". Listed below after the summary are the responses to the auditor's recommendations.

Summary

Staff acknowledges the importance of the SAP security vulnerability incident and has made it a top priority to rectify and taken action to address many of the findings in the audit. After reviewing the system and potential impacts, staff feels comfortable in stating the impact was limited to access of personal or sensitive information by a very limited number of highly skilled City employees committed to SAP operational standards. The City's network access was not compromised and since an outsider would have to first breach the firewall and then SAP security, the incident was limited to internal users. Furthermore, the system was setup with financial controls that would prevent an individual from processing transactions such as issuance of checks or dispersing of funds on their own. There are check validation systems in place as well that would prevent an unauthorized check from being charged to the City's account. While it is unacceptable that sensitive information was exposed, the limited number of staff with the ability to access the information is trained to access sensitive information while upholding confidentiality standards.

The Information Technology (IT) Department (Formerly a Division of the Administrative Services Department) has been working in recent months with the Auditor's Office to address inquiries and findings arising from the audit of SAP. Significant security changes to IT processes have been made since the initial findings were released by the City Auditor.

The IT Department was created in the FY2012 Budget as a stand alone department. The organizational unit was formerly housed in the Administrative Services Department (ASD). The City Manager established IT as a stand alone department to give greater emphasis and focus to the IT function, including the area of security.

During the last several months staff has collaborated with the Auditors Office in developing a SAP Special Account Monitoring and SAP System Monitoring Policy and Procedures to address the internal security incident involving SAP* user account. As a result, staff has significantly improved the security of the SAP system.

It is important to emphasize that staff acknowledges the importance of the findings in the audit. At the same time it is important to point out that the task of effectively managing and mitigating vulnerability risks associated with SAP* user accounts as well as developing a comprehensive IT security policy[1] is the responsibility of a handful of employees in charge of the day to day operations of maintaining the enterprise-wide SAP system comprised of six systems, as outlined in the audit finding #4, the implementation of the information Security System Standard will require the involvement of the SAP team as well as the network operations, infrastructure and business process teams. With many IT teams involved the complexity of mitigations can become great.

Since the IT function has become its own department, the new Department Head, once hired, will need to undertake a comprehensive security evaluation for all technology systems and determine the appropriate resources needed to address enterprise security requirements.

To summarize, of the twenty-one recommendations, staff believes that seven have been completed, two are work-in-progress, and the remaining twelve will require further evaluation. In order to address the remaining recommendations on the list we believe that the security risk, staffing requirements, and implementation costs need to be evaluated. We are recommending that an IT security expert be retained to perform these evaluations and prepare a cost benefit analysis to assist staff in making future recommendations. This analysis will be coordinated with the upcoming IT Strategic Plan recommendations, which include conducting a comprehensive Citywide IT Security Audit.

One of the key factors in determining future actions is determining the risk level posed by the vulnerabilities in the system. Not all risks listed in the recommendations are of equal magnitude. We have prepared an initial risk assessment using the recommended risk assessment framework from the National Institute of Standards and Technology (NIST SP800-30) which evaluates individual security vulnerability findings by determining business impacts[2] of the security event and likelihood of the event

[1] **IT security policy related standards**: a. Payment Card Industry Data Security Standard (PCI-DSS), b. National Institute of Standards and Technology (NIST) : NIST SP800-53 (Security Control), NIST SP800-30 (Risk Assessment,), NIST SP800-39 (Managing Security Risk)

[2] **Rick business impact definition**: High: highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury. Medium:

occurring. The results of our internal risk level assessment are referenced in the following response to each recommendation. Staff provides the risk rating as one piece of information to help evaluate the criticality of the recommendations and actions taken. Staff suggests that an independent security audit validate the risk rating.

RECOMMENDATION #1
ASD should develop and implement formal policies and procedures addressing standard SAP user accounts in order to:

- Secure standard user accounts and prevent unauthorized use.
- Detect on an ongoing basis any unsecured standard accounts and any unauthorized use.
- Ensure standard user accounts can only be managed by a designated individual(s).
- Authorize use only if appropriated, and ensure there is accountability for any use.
- Ensure any authorized use is monitored.

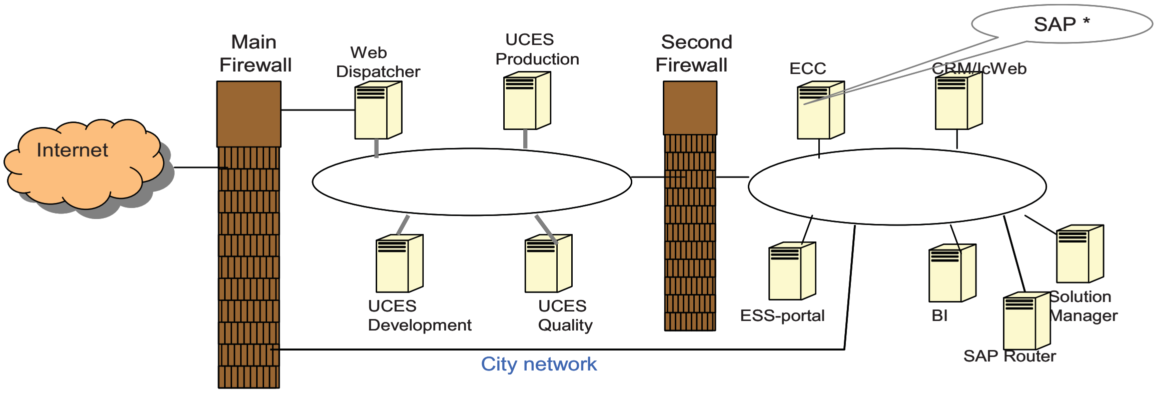
Staff concurs. Status: Completed. Risk level assessment: Medium (04/2011), Low (09/2011) to be further validated by external security expert

We have been working with the Auditor's Office to design control processes and procedures. As a result, the following changes have been implemented and are now included in SAP Special Account Monitoring and SAP System Monitoring Policy and Procedures

- SAP* Account has been locked and authorization removed
- Two levels of monitoring and alert mechanisms have been established to detect SAP* login
- SAP special accounts are now grouped and maintained by a separate individuals rather than just the Basis Administrator
- SAP special account access log will be reviewed on daily basis
- As shown below the City has multiple layers of security across the network with two firewalls standing in front of the internal SAP servers

SAP * incident in the Context of the Network

(1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury. Low: (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.



Protection

- Servers are physically locked
- Comprehensive backup and offsite backup
- Managed firewall - Main fire wall (BRODERWARE)
- Web dispatcher port address translation
- My Utilities Account logon user ID authentication
- Managed fire wall (Sonic) - second fire wall protection
- SAP graphic user Interface logon must be available
- SAP logon ID authentication
- SAPAuthorization checking protection

Preventative

- Window patches are updated automatically
- Auto SAP* monitoring and alert
- Auto SAP* logon monitoring and alert
- SAP* is locked and with no authorization
- Daily review SAP security audit log

RECOMMENDATION #2

ASD should further investigate the following:

- Staff's account that SAP* was left unsecured after installing an SAP support pack in
- December 2010
- Responsibility for the deletion and recreation of the SAP* user master record
- Responsibility for missing log records

Staff acknowledged. Status: an internal review of all available supporting materials, i.e. user change log, access log, security activity log was completed. IT has been working with the Auditor's Office to address the items above. Unfortunately IT was unable to continue further the investigation due to limited availability of data[3] (i.e. system log and security activity log were either not available or no longer

[3] SAP system log is configured to retain a specific amount of data which allows retention of approximately 8 months of rolling data.

existed and there was no change log record), which could be used to substantiate the responsibility for items 2 and 3. We've since refocused our efforts on lessons learned and tightened control of SAP* account maintenance by separating the administration rights from the SAP Basis function.

RECOMMENDATION #3

To ensure the City can appropriately respond to SAP security incidents, ASD should develop and implement a comprehensive incident response plan that meets PCI DSS and NIST control standards and includes provisions to address:

- Incident response policies and procedures
- Incident response training
- Monitoring and reporting
- Roles and responsibilities
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements in reporting compromises

Staff concurs and recommends an independent external security expert evaluation. Status: Open. Risk level assessment: Medium (09/2011), to be further validated by external security expert. Target review date: pending on external security audit. Incident management is one of the twenty-eight IT Security control points[4]. SAP Program Management Office (PMO) has implemented an incident management procedure, including the essential elements of an incident, (i.e. date, time, report by, incident description, action taken, root cause analysis, and mitigation plan). Staff recommends a comprehensive incident management review to be done by an independent external security expert. Target review date: pending on independent external security audit.

RECOMMENDATION #4

To mitigate risks associated with assignment of unrestricted SAP access, ASD should:

- Formally adopt policies and procedures addressing SAP user access consistent with the principles of least privilege and segregation of duties. For emergency purposes, ASD should

[4] IT Security Control includes nine categories, total 28 control point: including Risk Management, Contingency Planning, IT System Security, Logical Access Control, Data Protection, Facilities Security, Threat Management, and Asset Management

consider creating a single unrestricted account assigned the SAP_ALL profile that is appropriately secured and controlled in accordance with SAP guidelines and industry standards

- Implement policies and procedures to either prohibit or control the use of all other powerful system-provided SAP profile
- Ensure needed SAP roles and profiles are approved by management and included in the City's role authorization procedures, and that unauthorized roles and profiles are not assigned.
- Develop procedures to detect any unauthorized roles or profiles assigned to users

Staff concurs. Status: Completed. Risk level assessment: Low (09/2011) to be further validated by external security expert

During the audit period, staff has updated the relevant processes and procedures, including the SAP Authorization Management process and procedure, SAP Special Account Monitoring, and SAP System Monitoring Policy and Procedures to incorporate the above recommendations. Summary of the update includes:

- Roles ownership for business transactions are established and reviewed by the business role owner to ensure that the principles of least privilege and segregation of duties are practiced
- A semi annual authorization review is in place and findings and improvements are documented
- Adds, changes, and deletions to SAP authorization requests are tracked and approved by the Helpdesk
- Other SAP default special accounts are locked and password reset
- SAP default special accounts access logs are monitored daily

RECOMMENDATION #5

To ensure SAP user account administration functions are properly separated, ASD should:

- Segregate responsibilities for creating and maintaining roles/profiles, assignment of roles/profiles, creating and maintaining user accounts, transportation of roles/profiles
- Prohibit IT staff from maintaining Human Resources department employee records
- Assign all SAP user administrators to a designated SAP user group, preventing them from managing their own (and other administrators') accounts and access levels, and designate an individual to manage the SAP user group

Staff concurs and recommends independent external security expert evaluation. Status: Open. Risk level assessment: Low (09/2011) to be further validated by independent external security expert.
Segregation of duties is important but difficult to implement without additional resources.
We have implemented a mitigation control in the SAP System Monitoring Policy and Procedures to review all user change logs done by the SAP user administrator. In addition, request to transfer maintenance of Employee records back to Human Resources Department (HR) has been initiated. Target review date: 6/30/2012

RECOMMENDATION #6

Develop and implement policies and procedures to ensure SAP access for separated City employees is terminated in a timely manner and coordinated with Human Resources Department processes.

Staff concurs. Status: Open. Risk level assessment: Medium (09/2011) to be further validated by independent external security expert.

SAP user account will be terminated upon receiving a Termination Report from HR. The security risk resides largely on the employee termination business process, i.e. filling out Personnel Action Form (PAF) by business department for each terminated employee. To mitigate the risk, we've implemented controls to facilitate reconciliation between Human Resource, Windows NT (network), and SAP user account to ensure SAP access for separated City employees is monitored and terminated. Target review date: 6/30/2012

RECOMMENDATION #7

ASD should either eliminate the 52 generic Calcard user accounts, or develop policies and procedures to implement compensating controls to:

- Ensure these accounts are secured
- Establish individual accountability for their use
- Allow use on an exception basis in meeting the City's business needs

Staff concurs. Status: In Progress. Risk level assessment: Low (09/2011) to be further validated by independent external security expert.

The 52 generic Cal Card user accounts do not have any role or authorization assigned; therefore, the corresponding security risk is relatively low. The accounts are used to close out fraudulent charges to the City's Cal Cards and cannot be used to make purchases. To mitigate the risk, we have implemented a control where generic user accounts' activity will be monitored and reviewed on daily basis. Evaluation of a web-based solution to replace the customized Cal Card program is under way, which will offer staff better tools for handling fraudulent charges. Target review date: 06/30/2012

RECOMMENDATION #8

ASD should develop formal policies and procedures that clearly classify non-organizational users and define for each class:

- Authorized access levels
- Duration of access
- Controls to ensure each class abides by the City's security policies
- Controls to monitor SAP activity and to ensure SAP access levels and duration is consistent with policies and procedures

Staff concurs. Status: Completed. Risk level assessment: Low (09/2011) to be further validated by independent external security expert

Risk of this finding has been mitigated through the implementation of the following controls:

- Classification of non-organization users such as business partner Greenwaste or support maintenance partners
- Sierra Inforsys SAP support logins are reviewed and managed by the semi-annual authorization process
- Non-organizational User accounts creation to be tracked by the Helpdesk and approved by business owners with an expiration date
- Adds, changes, and deletions of authorizations are tracked by the Helpdesk and approved by the business owner
- Non-organizational user account activities are monitored and reviewed as part of the Daily System Monitoring process

RECOMMENDATION #9

ASD should develop policies and procedures to address use of non-dialog user accounts that address:

- Authorization to use and individuals authorized and assigned.
- Permitted use for each account
- Individual accountability for use
- Controls to monitor use

Staff concurs. Status: Completed Risk level assessment: Low (09/2011) to be further validated by external security expert
Non-dialog user accounts are broken down as follows: 7 “system” accounts, 3 “communication” accounts, 2 “service” accounts, and 1 “reference” user account. The accounts are used by SAP for specific purposes. These accounts cannot be used to logon to SAP; therefore, the risk is relatively low. To mitigate the risk, non-organizational user account activities are monitored and reviewed as part of the Daily System Monitoring process

RECOMMENDATION #10
ASD should as a rule prohibit the use of generic user accounts, in following PCI DSS and NIST control frameworks. ASD should develop policies and procedures to address use of any generic user accounts on an exception basis to meet the City’s business needs and to ensure adequate compensating controls are implemented to address:

- Formal authorization for use
- Permitted levels of access
- Duration of use and procedures to timely inactivate
- Permitted use or function
- Individual accountability

Staff acknowledged and actions have been taken. Status: Completed Risk level assessment: Low (09/2011) to be further validated by independent external security expert. Generic SAP user accounts such as “Data Migration” were setup during the Banner to SAP migration. The account has expired. There are other generic accounts such as EARLYWATCH used for SAP support. To mitigate the risk, non-organizational user account activities are monitored and reviewed as part of the Daily System Monitoring process

RECOMMENDATION #11
ASD should establish policies, procedures, and processes to ensure:

SAP user administrators are aware of the required identification information for each type of SAP user account, and SAP is configured to mandate, to the extent possible, input of required information. SAP user accounts contain all required user identification information, consistent with Human Resources Department records and/or other applicable independent authorized lists for City employees. The City is compliant with PCI DSS and NIST SP 800-53 standards in its management of SAP user accounts.

Staff concurs. Status: In Progress. Risk level assessment: Medium (09/2011) to be further validated by independent external security expert.

The SAP user account information combines HR employee master information and information from the active Directory (Network and Email account).Therefore, any attempt to address the issue only with SAP will be limited. We’ve documented the HR employee master, Active Directory and SAP account creation, change, and termination system processes and identified a set of improvement actions. However, implementing PCI DSS and NIST SP800-53 implementation would require network team resources and cooperation of the HR Department. To mitigate the risk, we've implemented controls to facilitate reconciliation between Human Resource, Windows NT (network), and SAP user account information. Target review date: 6/30/2012

RECOMMENDATION #12
ASD should adopt and implement PCI DSS and NIST SP 800-53 information systems security control frameworks to help ensure security of the City's key information systems.

Staff recommends external security expert evaluation. Status: Open. Risk level assessment: Low (09/2011) to be further validated by independent external security expert.
PCI DSS[5] contains six major categories and a total of 200 control points. NIST SP-53 contains a similar number of control points. Implementing both standards would require significant IT resources and business resources. Staff suggests a comprehensive security audit to determine the risk level and cost.

RECOMMENDATION #13
ASD should develop and implement a formal and comprehensive security policy consistent with PCI DSS, NIST, the SAP Library, and other industry standards.

Staff recommends external security expert evaluation. Status: Open. Risk level assessment: Medium (09/2011) to be validated by independent external security expert. Target review date: pending on external security audit.

RECOMMENDATION #14
ASD should formally assign responsibility for SAP security.

Staff concurs, but it will require additional staff. Status: Open. Risk level assessment: Low (09/2011) to be further validated by external security expert.

SAP Security is one facet in the overall administration of the landscape. SAP Basis Admin staffing levels are the same as in 2003 when only 1 production landscape existed. There are 5 now.
Staff suggests a comprehensive security audit to determine the risk level and if a SAP separate security role should be established.

[5] PCI DSS contains six main categories, twelve requirements: six categories include: Build and maintain Secure network, Protect card holder data, Maintain vulnerability program, Implement strong access control, Regularly monitor and test networks, and Maintain Information Security Policy

RECOMMENDATION #15
ASD should implement a formal security awareness and training program that meets minimum control standards stated in PCI DSS and NIST control frameworks. The program should include provisions to ensure SAP technical staff is trained on current SAP security controls and practices.

Staff recommends external security expert evaluation. Status: Open. Risk level assessment: Low (09/2011) to be further validated by external security expert.

RECOMMENDATION #16
ASD should implement a formal risk assessment process that meets minimum standards stated in PCI DSS and NIST 800-53 to ensure key information system threats and vulnerabilities are routinely (at least annually) and effectively identified, ranked, and addressed.

Staff recommends external security expert evaluation. Status: Open. Risk level assessment: Medium 09/2011) to be further validated by independent external security expert. Target review date: pending on external security audit.

RECOMMENDATION #17
ASD should develop and implement formal policies and procedures to ensure SAP security parameters are properly configured and compliant with PCI DSS, NIST SP 800-53, and other applicable industry standards.

Staff recommends external security expert evaluation. Status: Open. Risk level assessment: Medium (09/2011) to be further validated by independent external security expert.

SAP Security parameters were reviewed in 2008 before Enterprise Central Component (ECC) 6.0 go live, current parameters were approved by IT management to align with the network security parameters. In addition, security parameter changes often require organizational cooperation, i.e. PCI-DSS suggests idle time out setting is 15 minutes. When the system detects an inactive session longer than 15 minutes, it will force a session logoff. Idle time out setting must consider business impacts as well, and must be aligned with network idle time out setting. Staff suggests a comprehensive independent external security audit to determine the risk level and cost. Target review date: pending on independent external security audit

RECOMMENDATION #18
ASD should ensure access to SAP system parameters is restricted to only authorized staff, and that policies and procedures incorporate change controls stated in NIST SP 800-53 to ensure all changes are properly planned, authorized, executed, and monitored.

Staff recommends independent external security expert evaluation. Status: Open. Risk level assessment: Low (09/2011) to be further validated by external security expert

RECOMMENDATION #19
ASD should develop policies and procedures and implement minimum NIST SP 800-53 and PCI DSS controls applicable to log management in order to ensure:

- SAP and Oracle log data is secured using appropriate “write-only” media and/or backup procedures
- Access to SAP and Oracle logs is restricted based on the principles of least privilege and segregation of duties

- Accountability is established for monitoring SAP and Oracle logs and for reporting any incidents to the appropriate levels of management
- SAP and Oracle are properly configured to ensure logs capture appropriate information and retain the information for an appropriate duration

Staff recommends external security expert evaluation. Status: Open. Risk level assessment: Low (09/2011) to be further validated by independent external security expert

RECOMMENDATION #20
ASD should develop policies and procedures consistent with PCI DSS, NIST SP 800-53, and NIST SP 800-122 to ensure:

Any sensitive production data used in the SAP quality assurance system is anonymized or otherwise properly safeguarded through implementation of recommended controls. Transfer of any sensitive production data is formally authorized by departments or individuals responsible for the data.

Staff concurs. Status: Completed. Risk level assessment: Low (09/2011) to be further validated by independent external security expert

The following protections have been implemented to protect customer sensitive data:

- Credit card number is fully encrypted in the data base
- Credit card number transmission is secured via Secured Socket Layer (SSL)
- Customer identification number, including driver license number, bank account, social security number, etc. is masked; only the last 4 digits remain unmasked at all user interface (display, report, search) to a limited number of authorized customer service representatives
- Quality assurance system data needs to be refreshed from the production environment in order to perform a proper system integration test. Such transfer request is tracked by helpdesk system and must be approved by business owner.

RECOMMENDATION #21
To enhance the Auditor's Office's efficiency and independence in conducting audits, and its ability to ensure compliance with generally accepted government auditing standards, we recommend ASD implement the Audit Information System AIS tool and provide the Auditor's Office with access to it and suggest a comprehensive security audit to determine the risk level and cost.

Staff concurs. Status: Open. Risk level assessment: Low (09/2011) to be further validated by independent external security expert.

Audit Information System (AIS) is not a turnkey solution. Project funding and resource must be planned in advance. Staff suggests the Auditor's Office to initiate AIS implementation project during annual CIP planning.

Appendix: SAP Security Audit Self Risk Assessment (September, 2011)

Recommendation	Staff response	Status	Target date	effectivenss of control	Probability of threat occurance	Risk likelihood rating	Risk Impact	Risk level (likelihood + impact)
Recommendation 1 ASD should develop and implement formal policies and procedures addressing standard SAP user accounts	Concurs	Completed		M	L	Low	High	Low
Recommendation 2 ASD should further investigate the SAP* incident	acknowledged	Completed		M	L	Low	High	Low
Recommendation 3 ASD should develop and implement a comprehensive incident response	Staff recommends external security expert evaluation.	Open	Target review date: pending on external security audit	L	L	Medium	Medium	Medium
RECOMMENDATION #4 to mitigate risks associated with assignment of unrestricted SAP access, ASD should:	Concurs	Completed		M	L	Low	Medium	Low
Recommendation 5 to ensure SAP user account administration functions are properly separated (SOD)	Staff recommends external security expert evaluation.	Open	6/30/2012	L	L	Medium	Low	Low
Recommendation 6 Develop and implement policies and procedures to ensure SAP access for separated City employees is terminated in a timely manner and coordinated with Human Resources Department	Concurs	Open	6/30/2012	L	L	Medium	Medium	Medium
Recommendation 7 ASD should either eliminate the 52 generic Calcard user accounts, or develop policies and procedures to implement compensating controls	concurs	In progress	6/30/2012	M	L	Low	Low	Low
Recommendation 8 ASD should develop formal policies and procedures that clearly classify non-organizational users	concurs	Completed		M	L	Low	Medium	Low
Recommendation 9 ASD should develop policies and procedures to address use of non-dialog user accounts	concurs	Completed		L	L	Medium	Low	Low
Recommendation 10 ASD should as a rule prohibit the use of generic user accounts	Staff acknowledged and actions have been taken.	Completed		M	L	Medium	Low	Low

Recommendation	Staff response	Status	Target date	effectivenss of control	Probability of threat occurance	Risk likelihood rating	Risk Impact	Risk level (likelihood + impact)
Recommendation 11 ASD should establish policies, procedures, and processes to ensure SAP and HR consistency	Concurs	In progress	6/30/2012	M	L	Medium	Medium	Medium
Recommendation 12 ASD should adopt and implement PCI DSS and NIST SP 800-53	Staff recommends external security expert evaluation.	open		M	L	Low	Medium	Low
Recommendation 13 ASD should develop and implement a formal and comprehensive security policy consistent with PCI DSS, NIST, the SAP Library, and other industry standards	Staff recommends external security expert evaluation.	open	Target review date: pending on external security audit	L	L	Medium	Medium	Medium
Recommendation 14 ASD should formally assign responsibility for SAP security	acknowledged	open		L	L	Low	Medium	Low
Recommendation 15 ASD should implement a formal security awareness and training program	Staff recommends external security expert evaluation.	open		L	L	Medium	Low	Low
Recommendation 16 ASD should implement a formal risk assessment process that meets minimum standards stated in PCI DSS and NIST 800-53	Staff recommends external security expert evaluation.	open	Target review date: pending on external security audit	L	L	Medium	Medium	Medium
Recommendation 17 ASD should develop and implement formal policies and procedures to ensure SAP security parameters are properly configured and compliant with PCI DSS, NIST SP 800-53	Staff recommends external security expert evaluation.	open	Target review date: pending on external security audit	L	L	Medium	Medium	Medium
Recommendation 18 ASD should ensure access to SAP system parameters is restricted to only authorized staff, and that policies and procedures incorporate change controls stated in NIST SP 800-53 to ensure all changes are properly planned, authorized, executed, and monitored	Staff recommends external security expert evaluation.	open		L	L	Medium	Low	Low
Recommendation 19 ASD should develop policies and procedures and implement minimum NIST SP 800-53 and PCI DSS controls applicable to log management	Staff recommends external security expert evaluation.	open		M	L	Low	Medium	Low
Recommendation 20 ASD should develop policies and procedures consistent with PCI DSS, NIST SP 800-53, and NIST SP 800-122 to ensure: Any sensitive "production" data used in QAS is cntrolled	concurs	Completed		M	L	Low	Medium	Low
Recommendation 21 To enhance the Auditor's Office's efficiency and independence in conducting audits, and its ability to ensure compliance with generally accepted government auditing standards, we recommend ASD implement the AIS tool and provide the Auditor's Office with access to it.	acknowledged	open		L	L	Medium	Low	Low

Page intentionally left blank

CITY AUDITOR'S OFFICE RESPONSE TO THE CITY MANAGER'S RESPONSE

The City Auditor's Office (Auditor's Office) appreciates the assistance from the Administrative Services Department (ASD) in completing this audit. During the audit, problems were not only identified but measures were taken to address certain vulnerabilities. ASD, in several instances, assisted the Auditor's Office in identifying significant security issues which are included in the audit report.

The Auditor's Office, however, has two overarching areas of disagreement with the City Manager's response. In our opinion, the response minimizes the seriousness of the security vulnerability identified in Finding 1, and the Auditor's Office disagrees with the results of the risk assessment included in the City Manager's response. The City Manager's response states:

> *"…staff feels comfortable in stating the impact was limited to access of personal or sensitive information by a very limited number of highly skilled City employees committed to SAP operational standards. The City's network access was not compromised and since an outsider would have to first breach the firewall and then SAP security, the incident was limited to internal users. Furthermore, the system was setup with financial controls that would prevent an individual from processing transactions such as issuance of checks or dispersing of funds on their own. There are check validation systems in place as well that would prevent an unauthorized check from being charged to the City's account. While it is unacceptable that sensitive information was exposed, the limited number of staff with the ability to access the information is trained to access sensitive information while upholding confidentiality standards."*

In our opinion, the response attempts to minimize the seriousness of the security vulnerability identified in Finding 1. As noted in the report, SAP* has a well-known default password and may provide unrestricted system access, potentially resulting in the following:

- Exposure and misuse of data such as personal identifying information
- Sabotage and operational disruptions
- Financial losses
- Damage to reputation

Even if access to SAP* was restricted to a "very limited number of highly skilled City employees," unauthorized access to this powerful account could have serious consequences for the City.

The City Manager's response includes an "SAP Security Audit Self Risk Assessment." Staff reports they prepared the risk assessment based on guidance provided in the NIST SP 800-30 publication. The risk assessment lists the 21 audit report recommendations as a basis for assessing and rating SAP security and "criticality" of the audit recommendations. The resulting assessment states an overall "Low" risk for 15 of the 21 recommendations, a "Medium" risk level for 6 of the 21 audit recommendations, and no "High" risk ratings associated with any of the recommendations.

The Auditor’s Office disagrees with the results of the risk assessment presented in the response. The audit findings and recommendations are based on guidance provided in the SAP Library, PCI DSS, and NIST SP 800-53. PCI DSS compliance is required for entities processing credit card transactions and implementation of minimum security control standards stated in NIST SP 800-53 and the SAP Library is highly recommended to ensure the City effectively secures SAP. As stated in the report on page 42, the City’s former external auditor reported the City’s noncompliance with PCI DSS several times since fiscal year 2008. We consider the audit recommendations presented in the report to be high priority because they identify weaknesses in security controls that are both required through PCI DSS, but also work in aggregate to help prevent and detect, and recover from security incidents.

ASD has also reduced the risk level of audit issues because it has taken corrective action on some of the recommendations. Although we commend ASD for these actions, the Auditor’s Office does not believe the risk level should be reduced until the controls are fully implemented and institutionalized.

Attachment A

THIS REPORT IS INTENDED TO PROMOTE THE BEST POSSIBLE MANAGEMENT OF PUBLIC RESOURCES

You are welcome to keep this copy if it is useful to you. If you no longer need this copy, please return it to:

City Auditor's Office
250 Hamilton Avenue, 7th Floor
Palo Alto, CA 94301

We maintain an inventory of past audit reports, and your cooperation will help us save on extra copying costs.

If you need additional copies of this report, please contact us at 650.329.2667 or city.auditor@cityofpaloalto.org.

Our reports are also available on the web at:
www.cityofpaloalto.org/auditor/reports.html

Attachment B

FINANCE COMMITTEE - EXCERPT

Special Meeting
October 18, 2011

Chairperson Scharff called the meeting to order in the Council Conference Room, 250 Hamilton Avenue, Palo Alto, California.

Present: Scharff (Chair), Schmid, Shepherd, Yeh

Absent:

4. SAP Security Audit

Interim City Auditor, Mike Edmonds said the item before the Committee was the audit report on SAP Security. Staff recommendation was the review and acceptance of the report by the Finance Committee and full City Council. He introduced the auditors and acknowledged the work done by the auditors and acknowledged cooperation and work done by ASD Staff. He provided a brief overview of the audit, which was prompted because the auditors identified a security vulnerability resulting from an unsecured system-provided or "standard" SAP user account known as "SAP*," which provided unrestricted SAP access. He stated the audit had the following objectives:

- Determine if Staff has adequately secured the system.
- Determine if there has been unauthorized SAP access using standard user accounts.
- Determine if the City had adequate securities policies, procedures, and processes in place.
- Assess the risk of fraud and abuse resulting from the vulnerabilities identified.

Mr. Edmonds stated the auditors did not find any fraud or abuse, but that the audit was limited in testing in this area. He stated the audit scope and objectives were limited to the previously listed objectives and to the production environment of the City's SAP Enterprise Resource Planning Central Component. He stated the security concerns raised may be applicable to other applications and systems. There were several key documents used in assessing the adequacy of controls: 1) SAP library which is online documentation that provides guidance on SAP security, 2) Payment

Card Industry Data Security Standard (PCI DSS), a minimum security standard applicable to entities processing credit card transactions, and 3) National Institute of Standards and Technology (NIST) Special Publication 800-53, which also provided guidance on information systems security. He provided an overview of the audit findings and stated the audit had 21 recommendations.

Senior Performance Auditor, Houman Boussina informed the Committee that the auditors had researched SAP security and identified the high-risk area of standard user accounts, including SAP*. He stated SAP*, one of the most important and powerful standard user accounts, had not been secured. Staff was able to enter SAP using SAP* with the default password allowing unrestricted access to sensitive and confidential information and areas in the system that in theory would allow an intruder to execute any type of transaction. In reviewing SAP logs, security reports, and assessing the control environment, the auditors concluded SAP* was accessible using its default password during extended periods. SAP* was likely not secured during the entire period from May 23, 2010 to January 11, 2011. It was also not secured for an unknown period(s) from January 2003 to December 2005, and may also have been unsecured during a two week period in 2008. There were a number of other standard user accounts which the auditors tested and were not able to access. The system security reports indicated they had not been properly secured but rather their passwords had expired at some point which prevented the access. The auditors requested SAP Services Staff to review the other standard user accounts. SAP Services Staff subsequently identified 83 standard user accounts, 64 percent of which had not been properly secured as of April of 2011. By June of 2011 Staff provided reports to the auditors showing 107 standard user accounts throughout the various SAP systems. The auditors concluded Staff had implemented initial controls to preliminarily secure these accounts. The auditors concluded ASD did not have formal procedures or awareness to secure SAP* or other standard user accounts. The auditors assessed ASD’s incident response, to detect and understand the underlining control issues. There was a four day period between the time the auditors accessed the system using SAP* and the time Staff detected the unauthorized access. In investigating the security incident, the auditors found SAP logs were also incomplete, limited in terms of duration, and in some cases, log records were missing. The recommendations the first finding were to 1) secure the standard user accounts, 2) further investigate and establish accountability for the security vulnerability, and 3) implement improvements to the incident response process. Finding 2 discusses two critical security principles:

- “Least privilege” requiring limiting user access based on job responsibilities, and that only the minimum level of access required is provided.
- “Segregation of duties” to ensure clear separation of roles and responsibilities across the functions within an organization.

Mr. Boussina stated that because SAP and other Enterprise Resource Planning systems integrate data and support a wide variety of functions, the risk associated with unauthorized access is high if controls are not in place to ensure users only have the minimum level of access required. The auditors found there have been 31 SAP user accounts since 2003 that were granted unrestricted access through assignment of the "SAP_ALL" profile. The SAP Library states only one user account should have the SAP_ALL profile assigned and the user account should be secured by storing its password in a safe. SAP user administrators performed job functions that should be segregated such as creating user accounts, defining access levels, and modifying access levels. These functions should be segregated to ensure one individual does not have complete control over assigning system access. The recommendations for finding 2 were to 1) apply the security principles of least privilege and segregation of duties, 2) secure use of all powerful system-provided SAP profiles, such as SAP_ALL, 3) properly segregate SAP user account administration functions.

Senior Performance Auditor, Mimi Nguyen said in finding 3 the audit focused on the general population of user accounts and found there were 1,503 user accounts which were broken out into two different categories 1) employee accounts and 2) non-employee accounts. Within the group of employee accounts the auditors found 17 user accounts that had not been timely removed or disabled after the employee had separated from the organization. The average time it took to disable or remove the accounts was 577 days with one account taking 1,727 days. Guidance suggests access to user accounts be immediately removed for separated employees. In the category of non-employee accounts, there were 52 CAL-Card user accounts, which are dummy accounts used by Staff to transfer and retain transaction history when issuing a new CAL-Card. These generic accounts do not identify individuals and therefore do not support accountability. There were 22 non-organizational user accounts which were for consultants. The concern with those accounts was some had expiration dates that were beyond the expiration date of the contract for the consultant. In addition, there were no non-disclosure or conflict of interest agreements with the consultants to ensure consultants follow the City's security policies. There were 13 non-dialog user accounts used by technical Staff to run background processes. These accounts should be secured and controlled as other user accounts. Six of the 13 accounts had the SAP_ALL profile assigned to them. There were 14 other generic accounts without adequate indentifying information. It is recommended that each account be identifiable, traceable and tied back to a separate, independent source such as an HR database to ensure checks and balances are in place. The recommendations for finding 3 were to 1) define and manage security controls for all categories of user accounts and 2) establish an effective user account identity management system.

Mr. Boussina stated finding 4 addressed the underlying control environment and was more of a general overview of the controls that needed to be in place to ensure information system security. The initial review was to determine whether the City had adopted a recognized information systems security control standard. The PCI DSS standard is required and the auditors found implementation of PCI DSS was also recommended by the City's former external auditor in 2008. The auditors concurred and believed adopting security standards would provide a strong foundation for information system security. The auditors found the City had not implemented and did not have a coherent strategy for implementing the standard. The auditors found the City did not have a comprehensive security policy or that responsibility for SAP security had been formally assigned. PCI DSS requires a security policy that encompasses and supports all of the various required security controls. PCI DSS has over 250 specific controls that need to be adopted and implemented. Having a security policy sets the tone for the organization and ensures there is an effective means by which to implement the standard and to communicate it to Staff. Staff found the Administrative Services Department (ASD) did not have a formal information systems security awareness and training program. The auditors reviewed training records for SAP administrators and did not find a formal training plan or training records, especially in the area of SAP security, which was the subject of the audit. Therefore, the implementation of a formal security awareness and training program was recommended. IT risks and vulnerabilities change frequently and control standards require a formal risk assessment process to identify and manage information system risks whereby Management and Staff could ensure they had reviewed all of the various risks, rated them, and have properly establish a plan to implement controls. The SAP system security parameters and settings required to control access to the system were not properly configured to meet the level of security required by PCI DSS and other control frameworks. The auditors found there were a large number of user accounts that had access to the security parameters and it was recommended that access be secured. The auditors found ASD did not have policies and procedures to retain and analyze SAP audit trails or logs, and that SAP administrators responsible for managing user accounts are also responsible for reviewing logs. ASD uses live "production" data in the SAP quality assurance system without measures to "sanitize" or protect the data. Because quality assurance systems are typically not secured to the same level as production systems, this is a security concern.

Mr. Edmonds stated SAP has a free auditing tool that came with SAP called Audit Information System (AIS), which would assist the Auditor's Office. AIS could provide a number of reports, including reports to detect unsecured standard user accounts. The Auditor's Office has discussed AIS with ASD Staff, but it has not yet been implemented. The Auditor's Office advocates implementing AIS.

Council Member Scharff asked if the City Auditor's Office budget or the General Fund would fund AIS.

Mr. Edmonds noted at the present time he was uncertain as to the cost but believed it would be minimal, but that it would require some minimal programming.

Director of Administrative Services, Lalo Perez stated the IT budget would be charged.

Council Member Scharff asked if the Auditor's Office would be charged back for the cost.

Mr. Perez clarified each department received a charge for a portion of the cost. The practice had been to accommodate the needs of the organization through that Fund and now that IT was its own department he recommended the process remain.

Council Member Shepherd asked how Staff proposed putting the system back together with confidence.

Mr. Perez stated the security vulnerability resulted from human error. He felt the issue stemmed from decisions he and his predecessor made with respect to cutting resources when there were five dedicated SAP positions eliminated in 2005, and that one was added back with the SAP module upgrade, but it wasn't enough. SAP and the whole network was an important area for the organization and needed to be reviewed. He recommended the City Manager and the incoming Chief Information Officer (CIO) bring in a third party consultant for assistance.

Council Member Shepherd questioned the need for an outside consultant.

Mr. Perez felt based on the feedback from Council regarding the SAP system they did not desire to add resources whether it was a consultant or Staff. Because of that feedback he felt an outside review would help build a case and to support the system needs and better define the costs.

Council Member Shepherd expressed concerns regarding doing business with the City if there isn't additional security given the City processes credit card payments. She asked if the audit recommendations could not be performed or implemented without additional Staffing.

Mr. Perez stated there would be an impact on resources.

City Manager, James Keene informed the Committee that Staff had accomplished some of the recommendations. Retooling, reinvesting, and training needs should be communicated to the City Manager and Council, and a timeline should be brought forward to the Council for working with the audit recommendations.

Council Member Shepherd asked what was meant by retooling.

Manager of Information Technology, Jennifer Leu clarified there were 21 recommendations and Staff had implemented seven to date and there were two in progress. The remaining 12 involve a more comprehensive plan which was not something SAP Staff could accomplish alone. Staff was making the effort to mitigate the risks and was pulling resources into the area where the resources would be most valuable.

Council Member Shepherd asked which seven recommendations had been implemented.

Mr. Perez noted the seven had been listed within Staff Report and acknowledged there was room for improvement. He agreed with the City Manager that the priority was securing the system. He felt there were sufficient financial controls in place that those would not be jeopardized and the issues involved individuals with internal access to SAP, and not the outside world. He clarified it was still not acceptable.

Council Member Shepherd said any time a person was able to manipulate data within a restricted area without permission was unacceptable.

Mr. Perez acknowledged a significant amount of work was needed to reach the Best Practices level and at the present time there were not ample resources to complete all the necessary steps. He stated Staff would work together to bring forward recommendations. He suggested Council might prefer someone else to validate his recommendations.

Mr. Keene reiterated there were 21 recommendations, seven had been implemented, and two were in progress leaving twelve outstanding recommendations. The question was why the remaining recommendations have not been addressed or could not be met with the status quo.

Mr. Perez said the personnel needed to run the system and to implement the remaining twelve recommendations were more than what was available. The IT department had two Staff members to complete all of the SAP work which required four to six.

Ms. Leu referred to the NIST SP 800-53 standard and stated there were approximately 250 control points that not only involve SAP, but the entire network. The controls include firewall controls, identity management, access controls, and vulnerability checking. She stated considering the SAP team had only two Staff Members, it is beyond their capacity, and in some cases, beyond their knowledge to accomplish those tasks. It would also require the IT team collaboration and in some instances, business processes would require changing.

Mr. Perez located a Computer World article regarding citing that roughly half of the respondents blamed resource constraints for security issues, and about the same number cited network complexity as the main challenge.

Chair Scharff stated those were outside invasions but the City was concerned with internal security issues.

Mr. Keene understood the difference but Staff was letting the Committee know there were security vulnerabilities all over.

Council Member Shepherd stated her concern was the boiler plate being able to go in and mysteriously dump logs or change data, and that we don’t understand why this is happening.

Mr. Perez believed the issue was Staff had not activated or validated all of the systems that check the formal procedures and that took resources. He supported the idea that it could be done but his concern was being able to complete it prior to an external threat occurring.

Mr. Keene stated the issue at hand was the need to respond to the audit recommendations in as expeditious a manner as possible. He acknowledged the importance and significance of the audit recommendations and stated there would be an investment of time, money, and resources to address the audit issues.

Mr. Perez felt the SAP issue was another good reason ASD recommended IT should be a department.

Council Member Shepherd agreed and noted most company’s separated out their IT departments years ago and she looked forward to seeing the prioritization of the issues.

Council Member Yeh stated he felt the audit was very valuable and was glad that the issues were raised through the internal auditors and not through a reaction to an incident. He stated that after hearing the resource constraints, he thinks if an external consultant was brought in it would be important that they address the issues that were highlighted throughout the audit and to craft an implementation plan. He asked what would be envisioned in terms of planning an assessment.

Mr. Keene said there needed to be more invested in IT. There had been peer reviews and consultant work completed on the assessment as part of the swat analysis on the Strategic Plan. He stated Staff would be responding to the audit, and that beyond the security issues, there were other issues and that he advocated making investments to ensure a first rate IT operation in the City.

Vice Mayor Yeh clarified the reason behind his questioning was there were target review dates in response to the recommendations to be completed by June 2012.

Mr. Perez said the recommendation was based on bringing in the consultant and his uncertainty of when the Chief Information Officer (CIO) would be on-board. He acknowledged given that the CIO would be arriving shortly he felt they should be involved in the assessment of the department.

Mr. Keene was confident that Staff could return in the first quarter of 2012 with the CIO and provide a more detailed assessment of the issues.

Council Member Schmid said there had been four issues identified for the long-term 1) the internal Strategic Plan, 2) the external independent audit review, 3) the necessary resources, and 4) the entering CIO. He noted each item was a substantial matter and he wondered whether the City should wait for the incoming CIO.

Mr. Keene was confident the new CIO would be on board prior to the end of the 2011 calendar year. By the first quarter Staff should be able to adequately provide a necessary assessment.

Council Member Schmid said there was no mention of expenditures in the IT department in the update to the 2012 budget.

Mr. Perez said the only item added was the increased expense for the salary of the new CIO.

Council Member Schmid asked if some of the expenses were likely to show up in the 2012 budget.

Mr. Keene confirmed they would.

Chair Scharff was pleased to see the threat level within the audit recommendations were low.

Mr. Edmonds noted there may be a disagreement with the perception of risk. His opinion was that all of the areas identified were of a high risk since the exposure was to unauthorized access. While there had been areas of improvement, he stated until the processes had been institutionalized, the risk levels should not be assessed as low.

Chair Scharff asked if the City Auditor had read the City Manager’s response to the audit and whether they disagreed with it.

Mr. Edmonds clarified the Auditors office disagreed with the level of risk assigned to issues the auditors identified in the audit report.

Chair Scharff said there had been seven recommendations completed and Staff was currently working on two for a total of nine. He asked if the Auditor's office agreed not all of the issues carried the same level of risk.

Mr. Edmonds said the Auditor's office saw the recommendations as dealing with high risk areas, for example securing the standard user or default accounts was seen as a very high risk area. There may be other issues raised in the report that were of a high risk but not as high as securing those standard user accounts.

Chair Scharff clarified those accounts had been secured.

Mr. Edmonds acknowledged there had been several actions taken in regards to those accounts. He continued to view the security of standard user accounts as a high risk area and that they needed to be reviewed on an ongoing basis. He stated until the processes for securing the accounts are working, the Auditor's Office could not state the risk level has been lowered.

Chair Scharff asked if the Auditor's Office felt there were recommendations that should be prioritized, which Staff had not yet addressed.

Mr. Edmonds said there had been movement on issues and recommendations in findings 1, 2, and 3, which are more specific recommendations. He noted what was missing was the foundation for security, which is addressed in finding 4. He agreed with the City Manager that those issues needed to involve the new CIO to build a strategy to implement the recommendations.

Chair Scharff noted finding 4 was structural and those items could not be implemented over night. He asked if there were items within the report that had not been addressed and could be taken care of quickly.

Council Member Yeh stated in the City of Oakland, the auditors have read-only access to every single module in Oracle and that they could access the modules and pull out data to do preliminary analysis and other work. He was open to the AIS module being opened to the City Auditor's Office for data access where their office could log-in to review or extract information but not change it. He stated he didn't know if the AIS recommendation had been implemented and stated he thought it could potentially be implemented without additional cost.

Mr. Perez said Staff was in favor of granting that level of access although there would be a cost and approximately 30 days of Staff time to reconfigure the AIS system to allow their office access. He stated however it was more than just turning on the module.

Mr. Edmonds announced Mr. Boussina and Ms. Nguyen would be attending a course on the subject matter shortly where one of the purposes of the class was to achieve a better understanding of what it would take to implement AIS, and they would be able to provide more information soon.

Mr. Keene said it appeared the Auditor’s office was going to be involved in the process not only presently but for a period in the future not just in resolving the current audit. He felt it would be helpful to put the matter in context as it related to SAP customers and best practices. He noted there were recommendations that could be made by a vendor to shift any risk or exposure from themselves to their customer by having criteria and standards.

Chair Scharff agreed there needed to be a safe and secure system although he felt there were different levels of safety and the question was whether or not the City was willing to spend an uncertain dollar amount to achieve for example a security level 9 if the level 5 was adequate. He asked what the risk of loss was or how serious were some of the issues. He explained he was not in support of hiring 4 to 6 more Staff. He asked if the Auditor’s Office could provide some indication of the level of risk versus the cost. He stated some level of risk would be acceptable in a nimble organization. He was concerned that some of this could result in a bureaucracy that would not allow the organization to function.

Mr. Edmonds referred to the audit report which recommended a security policy and a risk assessment, which should help the City identify the level of security to establish and how the City would address the risks. He stated part of implementing PCI DSS would be asking these questions in order to build a system the City wants.

MOTION: Vice Mayor Yeh moved, seconded by Council Member Schmid that the Finance Committee recommend the City Council 1) accept the City Auditor’s report and the 21 audit recommendations, 2) return in the first quarter of 2012 with updates on the implementation process, and an explanation of auditor’s module.

MOTION PASSED: 4-0