



**Office of the City Auditor**

---

**Report to the City Council  
City of San José**

---

**AUDIT OF INFORMATION  
TECHNOLOGY GENERAL  
CONTROLS**

---

**Report 12-02  
January 2012**

January 18, 2012

Honorable Mayor and Members  
Of the City Council  
200 East Santa Clara Street  
San José, CA 95113

## **Audit of Information Technology General Controls**

General controls are the basic policies and procedures that ensure the City's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions. Our review of general controls found that many of the weaknesses identified in previous reviews remain.

**The City Should Address Data Security Vulnerabilities.** We found weaknesses in internal controls over access to the City's network. In addition, top priority recommendations from a 2008 information security audit and policies on securing private information by employees have not been completely implemented. To address these vulnerabilities, we recommend regular reviews of access to the City's network by the Information Technology Department (ITD) and line departments, tighter username and password controls, increased accountability by third party vendors that handle credit card and personally identifiable information, and guidance to City departments and employees who handle credit card and personally identifiable information. Finally, ITD needs internal and external policies and procedures to ensure standardized and consistent practices citywide.

**The Information Technology Department's Backup Process is Inconsistent and Resource-Intensive.** Backups are copies of data and systems that can be deployed if primary data and applications are unavailable. ITD has an unwritten backup process and retention schedules for "mission-critical" and "day-to-day" backups, but we found the process was not always being followed. Specifically, we found that some mission-critical financial, payroll, personnel and billing data had not been sent offsite according to ITD's own self-prescribed timelines. In addition, we found that the tape-based backup process has inherent inefficiencies in terms of resources required. Lastly, we found that ITD's backup process does not necessarily align with the needs of end-users and citywide document retention schedules. To address problems with ITD's backups, we recommend tighter adherence to its own internal process, outreach to end-users, and development and implementation of a formal, documented backup process.

**The City Does Not Have A Disaster Recovery Plan for Information Technology.** Disasters are events that can threaten the availability of data or network infrastructure. Power outages, hardware failures, data corruption, and hacking attacks are examples of such disasters. Among other things, an ideal disaster recovery plan would define the processes and responsibilities for accessing and deploying business systems and data in the event of such a disaster, and to ensure that critical data is recoverable. While some departments maintain their own formal disaster recovery plans, formal disaster recovery

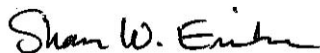
plans have not been developed for several of the City's mission critical applications. We recommend that ITD take the lead to develop a disaster data recovery plan and ensure the coordination of end-user business needs are included.

**ITD Should Improve its Inventory Practices.** ITD is responsible for approving most technology purchases, however each City department is generally responsible for determining and budgeting for their own technology purchasing needs. Partly because of this, non-personal technology expenditures are difficult to capture. Furthermore, ITD does not have a centralized inventory of technology assets. Recent citywide staffing reductions have resulted in potentially under-utilized computer equipment and software. To improve inventory practices, we recommend that ITD formalize inventory practices and use a regularly updated inventory to redistribute technology assets. We also recommend that to the extent possible, ITD pursue opportunities to centrally-install software packages rather than installing packages at individual workstations. Lastly, we recommend ITD develop, distribute and implement a citywide policy for securely decommissioning computer equipment.

**Many of the City's Computer Systems are Outdated and Should be Replaced.** The City of San Jose is located in the heart of Silicon Valley, but operates with 20<sup>th</sup> century technology. Some of the City's main enterprise systems, operating systems, and software applications are operating well beyond their life expectancies. Given scarce funding, we recommend the Administration review the age of its critical computer applications and determine a replacement schedule and budget for the highest risk systems.

I will present this report at the January 26, 2012 meeting of the Public Safety, Finance, and Strategic Support Committee. We would like to thank the management and staff of the Information Technology Department (ITD) and the other City departments for their time, information, insight, and cooperation during the audit process. The Administration has reviewed the information in this report and their response is shown on the attached yellow pages.

Respectfully submitted,



Sharon W. Erickson  
City Auditor

finaltr  
SE:lg

Audit Team: Gitanjali Mandrekar  
Michael Houston

cc: Vijay Sammeta  
Debra Figone  
Ed Shikada  
Rick Doyle  
Sharon Covarrubias

# Table of Contents

<b>Cover Letter</b> .....	<b>i</b>
<b>Introduction</b> .....	<b>1</b>
Background .....	1
Audit Objective, Scope, and Methodology .....	9
<b>Finding I</b>	
<b>The City Should Address Data Security Vulnerabilities</b> .....	<b>13</b>
Password and Access Controls Should Be Improved .....	13
The City Has Not Implemented Top Priority Recommendations from the 2008 Information Security Audit to Ensure Compliance With Data Security Standards (PCI-DSS) .....	16
The City Has Work to do to Fully Implement Its Identity Theft Protection Plan.....	22
Additional Written Policies and Procedures Are Needed.....	25
<b>Finding II</b>	
<b>The Information Technology Department’s Backup Process Is Inconsistent and Resource-Intensive</b> .....	<b>27</b>
ITD Has an Informal and Undocumented Backup Process.....	27
Opportunities Exist to Improve the Current Back-up Process .....	28
<b>Finding III</b>	
<b>The City Does Not Have a Disaster Recovery Plan for Information Technology</b> .....	<b>31</b>
ITD Supports and Maintains Mission-Critical Data and Systems .....	31
<b>Finding IV</b>	
<b>The Information Technology Department Should Improve Its Inventory Practices</b> .....	<b>35</b>
Most Departments Fund Their Own Computer Equipment and Software .....	35
There Is No Centralized Tracking of Technology Inventory .....	36
There Is No Centralized Policy for Decommissioning Old or Unused Computer Equipment.....	38
<b>Finding V</b>	
<b>Many of the City’s Computer Systems Are Outdated and Should be Replaced</b> .....	<b>41</b>
The City’s Outdated Computer Systems.....	41
<b>Conclusion</b> .....	<b>45</b>
<b>Administration’s Response</b> .....	<b>yellow pages</b>

# Table of Exhibits

<b>Exhibit 1: Information Technology Core Functions.....</b>	<b>3</b>
<b>Exhibit 2: Technology Functions by Department.....</b>	<b>4</b>
<b>Exhibit 3: ITD’s Network Operations Center.....</b>	<b>5</b>
<b>Exhibit 4: ITD’s Adopted Operating Budgets .....</b>	<b>6</b>
<b>Exhibit 5: Interdepartmental Roles and Responsibilities for Ensuring PCI-DSS Compliance.....</b>	<b>20</b>
<b>Exhibit 6: Key ITD Backup Retention Schedules.....</b>	<b>28</b>
<b>Exhibit 7: Unused City Computer Equipment Collecting in a Cubicle.....</b>	<b>39</b>

# Introduction

In accordance with the City Auditor’s fiscal year 2011-12 Audit Work Plan, we have completed an audit of the City of San José’s Information Technology Department (ITD).

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. We limited our work to those areas specified in the “Audit Objective, Scope, and Methodology” section of this report.

The City Auditor’s Office thanks the management and staff of the Information Technology Department (ITD) for their time, information, insight, and cooperation during the audit process.

---

## Background

The Information Technology Department’s (ITD) mission is to “*enable the service delivery of our customers through the integration of citywide technology resources.*” Primarily a behind-the-scene internal service, ITD supports citywide technology needs. ITD’s key areas of responsibility include operating and maintaining the City’s enterprise systems, customer contact center, and information technology infrastructure (including phones).

*Enterprise Technology.* The City has key “enterprise systems” that serve critical functions citywide including:

- Email – ITD staff work to ensure that these systems are reliably available to effectively store, process, and transmit data. Citywide, the email system transmits on average, about 7 million emails per day through 7,400 email accounts.
- Payroll and Personnel – ITD provides maintenance, programming and testing to the City’s payroll and personnel system to ensure timekeeping, earnings and benefits information is available and accurate so that Finance and Human Resources (HR) can administer payroll and benefits. ITD also implements compensation changes.
- Financial Management System (FMS) – ITD maintains the hardware, software and systems that store the data to support the City’s financial activities. ITD also ensures that employees

are provided access when requested by individual departments, and that the system is updated and backed up on a regular basis.

- Geographic Information Systems (GIS) – ITD maintains the citywide basemap used by a number of departments including public safety.
- Integrated Billing System (IBS) – The Integrated Billing System (IBS) is an invoicing and revenue management system for Recycle Plus, Municipal Water, and Storm Water and Sanitary Programs. ITD staff maintain and provide ongoing support for this system.

ITD staff are responsible for facilitating access to these systems, performing maintenance so that systems are reliably available, and resolving issues that affect system performance. ITD reports that the City's enterprise systems were available during business hours 99.95 percent of the time in Fiscal Year (FY) 2010-11.

*Customer Contact Center.* The Customer Contact Center is perhaps the most publicly visible component of ITD. Staff at the customer contact center field questions and concerns from residents, merchants and City employees, and process resident payments for garbage, recycling and water services. Callers may call seeking anything from general information to assistance within recycling, and garbage billing, animal care services, and street light issues. ITD reports that the Customer Contact Center handled approximately 264,000 calls in 2010-11. ITD operates two service areas in City Hall (the main lobby Information Desk and a lobby cashier window for walk-in residents and visitors).

*Help Desk.* The Help Desk service provides technical assistance to City departments that are supported by ITD. Help Desk employees respond to an array of requests for assistance which include email problems, desktop issues, service outages, etc. Requests for service can be done via e-mail or by calling a Help Desk number. All service requests, including requests for technology purchases are first sent to the Help Desk which then forwards the request to the appropriate division in ITD. ITD reports that in 2010-11 service desk employees received 32,800 service requests.

*Information Technology Infrastructure.* ITD's technology infrastructure team is responsible for preserving the functionality of the City's technology, including maintaining the City's network which contains hundreds of servers on which City data and enterprise systems are stored, and for ensuring the continuous availability of data and voice communication. The infrastructure team also provides for the service needs of over 2,000<sup>1</sup> desktop computers. ITD's network

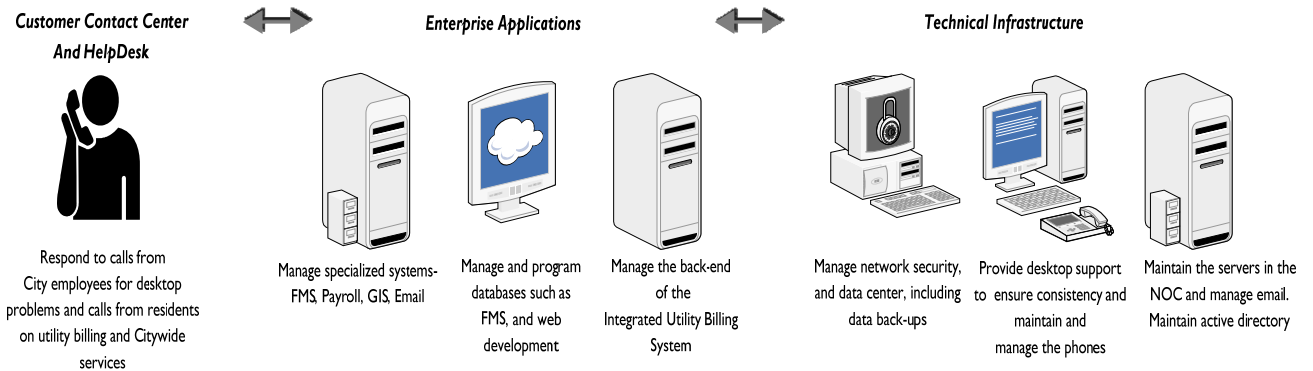
---

<sup>1</sup> Based on information from ITD's asset management system which only recognizes active users within the last two weeks. Does not include departments that ITD does not support.

stores about 120 terabytes of data in the Storage Area Network (SAN). ITD reports that the converged City network had zero network outages in 2010-11. The infrastructure team also manages the network operations center (NOC), preserves the City's data security, manages and maintains City servers, and provides internet connectivity to employees.

The exhibit below summarizes these core functions.

### Exhibit I: Information Technology Core Functions



Source: Auditor summary based on Budget documents and interviews of IT staff.

### Other Technology-Related Functions Are Located Throughout the City

ITD's role involves extensive support to the various City departments, but notably, some departments have their own department-specific technology functions supported by departmental resources. For instance, Airport Technology Services (ATS) has its own hardware and network that is independent of ITD. The San José Library, San José Police Department and the Water Pollution Control Plant are set up similarly. However, all departments are part of the City network and access citywide systems that ITD supports.

Other departments do not necessarily have their own separate technology functions but have staff dedicated to performing technology duties such as maintaining their own department-specific computer applications or providing desktop support services. Some departments have staff that are not specifically dedicated to such duties, but perform in such capacity. The exhibit below highlights the way information technology service needs are met across the various City departments.



**Exhibit 2: Technology Functions by Department**

Departments	Rely on ITD	Support Their Own Departmental Applications	Provide Their Own Customer Support
Airport	Y	Y	Y
Attorney	Y	Y	Y
Auditor	Y		
City Manager	Y		
Clerk	Y		
Emergency Services	Y	Y	Y
Environmental Services/WPCP	Y	Y	Y
Finance	Y		
Fire	Y	Y	Y
Housing	Y	Y	
Human Resources	Y		
Independent Police Auditor	Y		
Information Technology	Y		
Library	Y	Y	Y
PRNS	Y		
PBCE	Y	Y	
Police	Y	Y	Y
Public Works	Y	Y	
Redevelopment <sup>2</sup>	Y	Y	Y
Retirement	Y	Y	Y
Transportation	Y	Y	Y

Source: Auditor presentation based on ITD's descriptions

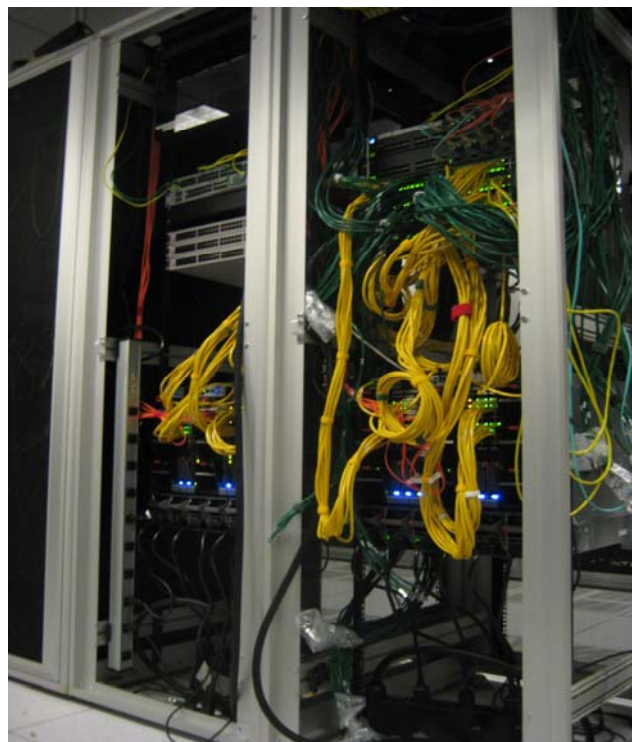
Exhibit 2 shows that even though many departments have technology functions, ITD is still key in all information technology throughout the City – even to those departments that have their own technology functions. ITD is responsible for infrastructure and enterprise systems. All City departments rely on this technology and these systems, hence all City departments rely on ITD to a large extent.

<sup>2</sup> This reflects Redevelopment Agency functions as of September 2011. Since then, Redevelopment Agency functions have been reduced.

### ITD's Network Operations Center

The City's network operations center (NOC) houses the City's computer equipment on which citywide enterprise systems are hosted, processes are run, and data are stored. The array of functions performed within the NOC is wide, and include such critical functions as round-the-clock hosting of the City's enterprise systems, traffic signaling, employees' document storage and online billing transactions. In addition to the NOC, a smaller data center at a separate City facility supports Heating, Ventilation, and Air Conditioning (HVAC) functions.

#### Exhibit 3: ITD's Network Operations Center



Source: City Auditor photo of hardware equipment (December 2011).

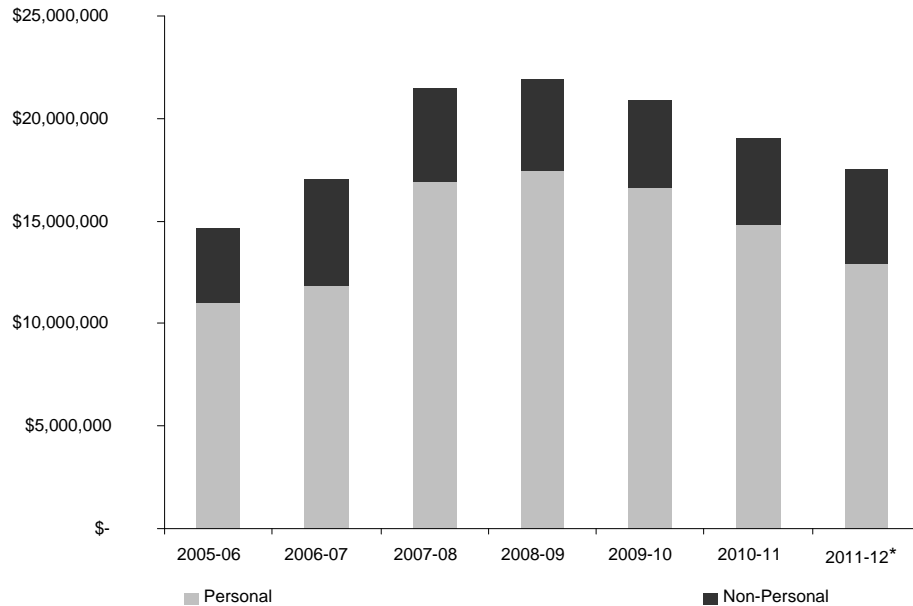
### ITD Budget and Staffing

ITD's 2010-11 Operating budget was \$19 million. The General Fund accounted for \$14.2 million of this (74 percent). The remaining millions are sourced from 8 other fees, taxes, and special funds. As with other City departments, ITD staffing has been steadily declining. In 2007-08 ITD staffing was 157 FTEs.<sup>3</sup> Staffing in 2011-12 is 101 FTEs. Exhibit 4 below shows ITD personal and non-personal

<sup>3</sup> The City's Customer Call Center moved to ITD in 2007-08, which explains much of the increase in ITD's staffing levels and expenditures.

budgets since 2005-06. We should note that ITD has had a significant upper management turnover in the past 11 years - a total of **seven** Chief Information Officers (CIOs) since 2000-01.

**Exhibit 4: ITD's Adopted Operating Budgets**



\*2011-12 Adopted Operating Budget

Source: Auditor summary based on the City's Operating Budget.

As discussed earlier, technology-related staff and resources are not limited to ITD. These figures do not include the resources directed to technology outside of ITD.

**ITD Is in the Process of a Multi-Year Technology Consolidation and Staff Redistribution Effort**

As approved in the City's 2010-2011 Adopted Operating Budget, ITD has initiated a multi-year consolidation effort of resources, staffing, infrastructure, applications, and tools. Completed consolidation activities include:

- Moving Customer Call Center staffing from Environmental Services Division (ESD) to ITD in 2007,
- Centralized citywide server access and privilege protocols (Active Directory),
- Email consolidation in 2008, and
- Consolidated network data storage on a Storage Area Network (SAN) in 2009.

In addition, ITD is currently in the process of migrating its database infrastructure, such as the Financial Management System (FMS), to Windows-based servers to lower total cost of ownership.

### **Summary of Previous Reviews**

Over the past 10 years ITD has been the subject of various reviews which resulted in recommendations. Several of these reviews are summarized below.

*IT Master Plan.* In May 2000 the City published the IT Master Plan (Plan). One outcome of the Plan was the formation of the Information Technology Planning Board (ITPB).<sup>4</sup> The ITPB is discussed below. In addition to the ITPB, the Plan recommended various long-term strategies:

- The IT organization must strike an appropriate, cost effective balance between distributed and centralized management of IT service delivery.
- Departmental IT support should focus on the success of the department being served, be responsive to local user needs, and yet accountable to support and maintain the City's IT policies, standards, and values.
- IT should coordinate the delivery of distributed support, ensure economies of scale (e.g., in the acquisition of training and standard software and hardware) are available to all units, retain negotiating power with vendors, and determine minimum standards to deliver a consistent quality of service.
- The City should seek to improve IT lifecycle cost estimates, IT project cost management and accountability, and coordinated IT investing.

The Plan also pointed out inherent weaknesses in Citywide IT. These included:

- Unknown Budget — How much does the City spend annually on technology resources?
- Fragmented Investments — Investments in systems and projects have not been prioritized or optimized.
- Lack of Formal Information Technology Governance — The City's Information Technology governance structure has been informal and inadequate.

---

<sup>4</sup> The Plan recommended that the effectiveness, membership, responsibilities, and authorities of the ITPB should be reviewed on a regular basis. Appropriate adjustments should be made over time to ensure that the ITPB is fulfilling its purpose.

- Dated or Nonexistent Policies, Standards, and Guidelines — The City's current technology standards, policies, and guidelines are informal and not widely understood.
- Recruitment and Retention — Recruitment and retention of information technology development and support staff is especially difficult for government organizations that can't compete with the private sector.
- Limited Training Budget — Historically, training for information technology support staff and end users has been insufficient and uneven.

As we will discuss throughout the report, many of the concerns raised by the Plan in 2000 still exist in the current technology environment in 2012 — nearly 12 years after being raised as concerns.

*Santa Clara Civil Grand Jury's Review of Information Technology Disaster Recovery Plans.* In 2003, the Santa Clara County Civil Grand Jury conducted a review of local agencies' information technology disaster preparedness and found that some local agencies including the City of San José, lacked written disaster recovery plans. It also found that when such plans have been prepared, they have not always been tested or updated. The Grand Jury recommended: "all cities/towns within Santa Clara County and all county agencies/authorities/districts should have written disaster recovery plans for mission-critical computer information systems, and should regularly test and update these plans."

*VeriSign Information Security Assessment.* In 2008, the City of San José contracted with VeriSign to perform an information security assessment. The scope of this assessment included:

- Vulnerability assessment of the City network,
- Security process management review,
- Preparation of a detailed report with a prioritized list of vulnerabilities, defined risk levels and remediation recommendations,
- Benchmarking the City's current security practices against industry best practices, and
- Assessment of the citywide governance model.

Results of the VeriSign review were presented to the San José City Council in a closed session meeting in May 2009. We will discuss the status of the VeriSign report recommendations in Finding I.

*Management Partners Optimization Study.* In August 2009, the City engaged Management Partners to develop recommendations to optimize its information technology program. The effort focused on management, structure and funding.

In its report, Management Partners raised concerns about the proportion of the City's resources dedicated to information technology, and ITD's governance structure. The report compared the City of San José's information technology-to-total budget ratio to those of comparable governments. It also made other recommendations with respect to developing a centralized information technology model and developing a viable committee made up of department directors to ensure that all departments are aware of IT policies, changes, and business plans. Most of Management Partners' recommendations have not been implemented.

### **ITPB Board Was Intended to Make Technology decisions**

The City attempted to create a common information technology governance structure with the creation of the Information Technology Planning Board in 2002. The ITPB was comprised of selected department directors and other senior managers from major City departments. The major goals of this board were to:

- Establish an enterprise technology infrastructure that is flexible, reliable, adaptable, and scalable and aligned with business requirements.
- Use technology to provide cost effective means to achieve business results and improve operating efficiency.
- Ensure that enterprise level policies align with business needs and are measured against industry best practices.
- Measure technology projects and support mechanisms to ensure cost-effective and consistent customer service.
- Ensure that the use of technology proactively assures integrity, privacy, confidentiality and availability of enterprise information.
- Ensure that if proprietary brand name standards for technology investments are used, proper purchasing procedures are followed and are reviewed on a regular basis.

Currently, the ITPB is inactive. ITD plans to reconstitute a new governance model that aligns with fiscal realities.

---

### **Audit Objective, Scope, and Methodology**

The objective of the audit was to assess general controls within ITD. Specifically, we sought to assess ITD's data security environment, data back-up and disaster recovery processes, and inventory processes. To meet our objectives, we reviewed various documents and processes including:

- Previous reports about ITD including the 2008 optimization study and the 2009 data security report;
- Current and past data security standards including the Payment Card Industry Data Security Standards (PCI-DSS)<sup>5</sup>;
- Policies and procedures from ITD and other technology functions across the City, as well as citywide policies and procedures related to information technology;
- Contracts between the City and its financial institutions, credit card vendors, and other service providers;
- Local, state, and federal laws and regulations related to privacy and identity protection;
- ITD's asset management system;
- ITD's backup processes and backup storage logs;
- ITD's process for retiring computer equipment;
- Physical controls in place at the network operations center;
- Access levels for current and terminated employees; and
- ITD budget and financial documents.

We also utilized interviews, which were particularly useful since ITD did not have many written policies and procedures. The following is a list of interviews we conducted during our audit:

- Various ITD staff to understand processes and functions;
- Information technology staff at the City and County of San Francisco to discuss and compare current information technology practices in place at San Francisco with those at the City of San José;
- Staff from various City departments such as Library, Airport, PRNS, Police, Finance, and the City's financial institution to understand data security issues and departmental processes and functions; and
- Information technology experts from Management Partners Incorporated and Macias Gini & O'Connell, LLP who worked on previous reviews of ITD.

---

<sup>5</sup> The Payment Card Industry Security Standards Council seeks to enhance payment account data security by driving education and awareness of security standards. The Council developed the *Payment Card Industry Data Security Standard* (PCI-DSS). PCI-DSS represent a common set of industry tools and measurements to help ensure the safe handling of sensitive information.

We limited our review to the scope and objectives stated above. We did not review independent technology functions in Airport, San José Police Department (SJPD), San José Fire Department (SJFD), Library and Water Pollution Control Plant (WPCP).



**This page was intentionally left blank**

# Finding I The City Should Address Data Security Vulnerabilities

## Summary

According to the General Accountability Office's Federal Information Systems Audit Manual, "General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entitywide, system, and business process application levels. The effectiveness of general controls at the entitywide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the entitywide and system levels, business process controls generally can be rendered ineffective by circumvention or modification." Our general controls review identified several weaknesses in internal controls over passwords and access. In addition, top priority recommendations from the 2008 information security audit, policies on securing private information by its employees, and other Citywide IT policies have not been implemented. As a result, the City has no assurance that it has addressed data security vulnerabilities.

---

## Password and Access Controls Should Be Improved

### Key ITD Staff Share One Administrative Password Which Provides Them with Unlimited Access

We found that seven key ITD staff are members of a group account that uses a shared username and password to attain unrestricted access to the City's network and applications. Such access provides these employees with the power to grant or deny access to City systems, and make changes to the City's network. Allowing these employees to use the same username and password creates a significant security risk and undermines monitoring and logging procedures. As it is currently set up, employees enter and make changes using a master username and password — not their individual user accounts — and therefore the system cannot track who made the change. In this way, the single log-in presents accountability concerns.

### Critical Access Levels Are Not Reviewed on a Regular Basis

As mentioned above, ITD has assigned 7 employees with unfettered access to critical systems. Due to the sensitive and critical nature of the information systems to which these administrative users have access, ITD has required these

specific employees to undergo background checks through the SJPD. This requirement is in addition to the general checks for new employees initiated by the City's Human Resources.

We found that even though employees undergo a higher level background prior to receiving this access, there is no on-going review by ITD. Specifically, ITD does not review this access to determine whether there is still a business need for it. Nor has ITD routinely changed the master username and password when employees leave. This increases the risk that ITD could inadvertently allow inappropriate levels of access to important City systems.

In contrast, access to the NOC is reviewed and approved by not only ITD but also by City Security, and is terminated upon separation. In addition, the NOC has limited access through employee badges, and has multiple security cameras at various points in the NOC. For an added measure of security, ITD is in the process of completing a project to build a locked metal gate which would further restrict access to certain areas of the NOC.

**Recommendation #1: To ensure changes to the City's network and mission-critical enterprise systems are tightly controlled, ITD should immediately change the password to its shared administrative account, ensure that administrative log-ins to the City's network are traceable, and strictly limit administrative log-in privileges to those who absolutely need such privileges. Furthermore, we recommend that the ITD CIO annually review and approve the memberships of shared accounts that can access the City's network and enterprise systems, and if necessary make changes based on current business needs.**

### **Password Controls Are Weak**

We found that the City does not have strong password controls for its other users. The 2008 data security review observed that at the time of the review, employees' passwords to the City network were set to expire in two years. However, as of this audit, passwords have now been set to **never** expire. In addition, log-in attempts are limitless. Other agencies, including the City's own Airport Technology Services recommend stronger password controls. Specifically, according to Airport's Network Security Policies for Airport Information Systems, Airport employees must change passwords every **six** months and cannot use default passwords. According to Penn State's Information Technology Systems (ITS) policies, "*systems force expiration of Penn State Access Account passwords once a year. Further, ITS recommends changing passwords more frequently for higher security. In addition, ITS systems retain a history of three passwords. This means that the last three passwords cannot be reused.*" We believe tighter controls around passwords to the City's network is important and ITD needs to set stronger password controls in order to ensure greater system security.

### Former Employees Retain Access to Departmental Files

We found multiple instances of **transferred** employees who retained access to their former departments' server space, some of which contained potentially confidential or sensitive information. We also found some instances of employees whose access was terminated to the City's network and departmental file servers for up to 42 days after their separation from the City.

Generally, access to the City's enterprise systems are linked to employee status through the City's personnel management system. In other words, if employees are recorded as "terminated" in the personnel management system, they automatically lose their access to the citywide payroll, personnel and financial management systems. This relationship between the City's personnel system and departmental server space results in improved security for departmental records. Periodic reviews of departmental server access could be an alternative to an automated solution which could be difficult to establish.

According to the University of Buffalo's security policies, "access to systems [...] should be reviewed regularly, and access for individuals should be removed when they no longer meet the criteria for which they were granted access. **Termination of employment, retirement, and job duty changes** are just some of the reasons that access may no longer be appropriate. Access can be removed by the system/application administrator changing the account password or removing the user id. At a minimum, monthly reviews of access should be performed for all systems handling sensitive data, regardless of their authentication method."

Per the above mentioned best practices, in our opinion, the City needs to develop a formal process for informing ITD when an employee separates or transfers from the City or department to ensure that the employee has appropriate access levels.

**Recommendation #2: To improve password and access controls over the City's network and data, ITD should:**

- a) **Establish minimum length and complexity requirements for users' passwords, automatic periodic expiration schedules, and "lock-outs" when users reach a pre-determined number of consecutive unsuccessful login attempts.**
- b) **While granting access to additional server drives, etc., ITD should by default, terminate transferring employees' access to the drives of the departments they are departing, or explore a system through which employees' access levels are tied to their employment status as recorded in the City's personnel system.**
- c) **Develop a review process requiring departments to periodically review the users with access to their departmental drives.**

---

**The City Has Not Implemented Top Priority Recommendations from the 2008 Information Security Audit to Ensure Compliance With Data Security Standards (PCI-DSS)**

As mentioned before, in 2008, the City of San José contracted with VeriSign to perform an information security assessment. The scope of this assessment included:

- Vulnerability assessment of the City network,
- Security process management review,
- Preparation of a detailed report with a prioritized list of vulnerabilities, defined risk levels, and remediation recommendations,
- Benchmarking the City's current security practices against industry best practices, and
- Assessment of the citywide governance model.

In addition to an overall security assessment, VeriSign reviewed the City's compliance with data security standards. The Payment Card Industry Data Security Standard (PCI-DSS) represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information.

## The City Has Work to do to be Fully Compliant with Data Security Standards (PCI-DSS)

In 2009, the City changed its banking provider. As part of this change, the City's new bank provided the City with payment gateway services. This service allows the City to authorize, settle, and manage credit card transactions online. It also provides access to a virtual terminal where a website is not required. Transactions take place via phone, fax or mail and are processed through the internet via a secure payment page provided by the gateway. However, the City still has some locations that rely on ITD's network to process credit card transactions. In addition, various City departments also contract with providers to provide credit card payment services which may occur through secure websites.

The City's bank requires the City to assess and ensure compliance with Payment Card Industry Data Security Standards (PCI-DSS)<sup>6</sup> at all the sites that accept credit card transactions. This **requires** each unit that accepts credit card transactions complete an **annual** self-assessment of its data security controls. We found that ITD has started only 13 of the 31 required assessments. As of the writing of this report, all these self assessments have expired.

While PCI-DSS relies on a secure network, merely assessing **network** security is not sufficient for PCI-DSS compliance. In addition, the City needs to meet various operational requirements such as securely storing physical customer credit card data. A comprehensive information security policy is required; however, the City has not yet implemented one. Per the VeriSign report, an information security policy would:

- *“Require an annual risk assessment;*
- *Establish daily operational procedures;*
- *Develop usage policies for critical employee-facing technologies; and*
- *Address Security Awareness Training and Education (SATE).”<sup>7</sup>*

---

<sup>6</sup> Payment Card Industry Data Security Standards were developed by the *Payment Card Industry Security Standards Council*, and serve as an industry authority on controls around cardholder data security.

<sup>7</sup> SATE is an overall security program which establishes training and education. This includes not only formal training upon hire and at least annually thereafter, which is signed by the employee/contractor, regular information security updates, and multiple methods of communicating awareness (such as posters, intranet, emails, meetings).

**The City Has Work to do to Ensure On-Going Vendor Compliance with Data Security Standards (PCI-DSS)**

To ensure its own PCI-DSS compliance, the City is required to ensure its vendor partners are PCI-DSS compliant. We found that the City's process for ensuring PCI-DSS compliance from its vendors is inconsistent.

There is no central repository to ensure that third-party vendors actually provide the certificates. Furthermore, we found that some contracting departments had never requested certificates for their third-party vendors. For instance, City staff did not have the required annual certificate for vendors supporting the Happy Hollow Park and Zoo, or the integrated billing system.<sup>8</sup> Moreover, for its vendor for the PRNS class registration system, staff has not requested a compliancy certificate for the current year. On-going annual compliance is crucial as a vendor's PCI-DSS status may change.

Ensuring **ongoing** compliancy from vendors is critical. According to the City's contract with its financial institution, the City is responsible for ensuring that *"all such agents or third party processors are (i) registered with the applicable payment card brands; and (ii) comply with all applicable data security standards, including, without limitation, the PCI Data Security Standard."*

**Recommendation #3: The City should include boilerplate terms to include in contracts with third parties the following:**

- a) Require PCI-DSS compliance when contractors are responsible for collecting credit card information.**
- b) Require the vendors to submit current PCI-DSS compliance certificates on an ongoing basis.**

---

<sup>8</sup> City staff requested certificates from the vendor after the Auditor's Office requested it.

**Not Complying with Data Security Standards Is Risky**

The City faces significant risks in not complying with PCI-DSS. According to the City's bank, the cost of a security breach could range from \$5,000 to \$50,000. The range of the fines would depend on the extent/cause of the breach. The City would have to subject itself to an investigation and pay for investigation costs. In addition, the bank could transfer onto the City any costs/fines imposed on it. Further, if the City is not PCI-DSS compliant, the fines could be higher. Finally, the City would have the additional burden of informing affected parties of the breach. Compromised data negatively affects consumers, merchants, and financial institutions and could result in negative consequences including lawsuits, insurance claims, and a violation of the public's trust.

**No Central Responsibility for Ensuring Compliance with Data Security Standards**

As mentioned before, even though ITD is responsible to ensuring completion of self assessments and network security, there are other aspects of an effective credit card security that ITD cannot oversee on a day to day basis. These include operational checks and balances such as standards for storing hard copies of credit card numbers. The exhibit below highlights the different levels of responsibilities.



**Exhibit 5: Interdepartmental Roles and Responsibilities for Ensuring PCI-DSS Compliance**

Roles & Responsibilities	ITD	Finance Department	Other City Departments	Bank	Notes and Potential Problems
Determine the need for processing credit card transactions			X		
Grant credit card processing privileges		X		X	Finance has ensured that only its designee can set up credit card accounts linked to the City's bank account. However, it is possible for departments to establish "rogue" payment accounts such as those offered by PayPal without informing Finance.
Link credit card processing to bank account		X		X	Finance has ensured that only its designee can set up credit card accounts linked to the City's bank account. However, it is possible for departments to establish "rogue" payment accounts such as those offered by PayPal without informing Finance.
Provide guidelines for securely processing credit card transactions					Finance is the custodian of the City's bank account and the credit card processing merchants linked to it. However, currently there are not guidelines in place to guide secure credit card handling.
Decide how credit card transactions will be processed			X		Departments use their own judgment in handling credit card transactions. Some departmental practices could be counter to PCI-DSS. For instance, even if they have secured terminal swiping machines, departments can record credit card numbers and expiration dates in anticipation of referring to future customer requests.
Ensure the secure processing of credit card transactions			X	X	For accounts linked to the City's bank account, the bank provides secure swiping machines. The bank also provides scanning software for scanning the network for security threats. The effectiveness of these controls are reliant on ITD and the departments actually using them.
Informs credit card accepting programs of changing standards		X		X	The City's bank would inform Finance (the custodian of the City's bank account) of changing standards. Finance would then inform citywide credit card-accepting programs.
Revokes privileges of noncompliant, abusive and fraudulent credit card processing units		X		X	Noncompliance, abuse and/or fraud would have potentially costly consequences.
Ensuring vendors that process credit card transactions or collect personally identifiable information on behalf of the City are doing so responsibly.		X			Finance is responsible for setting up contracts that ensure vendor accountability and protect the City from potential breaches. Finance's contracts require vendors to meet standards, but Finance does not necessarily verify that the vendors actually meet standards. Furthermore, Finance's contractual controls around personally identifiable information are more vague than its controls around PCI-DSS.
Initiating contracts with vendors that process credit card transactions or collect personally identifiable information on behalf of the City.		X	X		The City has processes for initiating contracts with vendors. However, there are differences in how departments hold vendors accountable to protecting personally identifiable information.
PCI-DSS Compliance Review	X				ITD has the technical expertise to identify potential network vulnerabilities. However, PCI-DSS also call for operational safeguards outside of ITD's expertise.

Source: Auditor analysis of roles and responsibilities as described during staff interviews

As Exhibit 5 shows, even though ITD plays an important role in ensuring that the City's network is PCI-DSS compliant, the operational responsibility lies with Finance and other user departments. We observed diverse methods for handling credit card transactions during our review. They ranged from online transactions hosted<sup>9</sup> by third parties, to paper forms on which customers enter their credit card information, to the "swiping" machines offered by the City's bank. We also found differing levels of controls in place at that the various departments. For example, while PRNS has some formal policies in place, Public Works' Animal Care and Services do not.

In February 2010, the City Auditor's Office issued an *Audit of Decentralized Cash Handling*. The objective of the audit was to determine if the City had an adequate and effective system of internal controls over the cash handling process including checks and credit cards. It included a recommendation that the Finance Department develop Citywide policies and procedures to require and periodically assess Payment Card Industry compliance at all distributed cash handling sites accepting credit cards. Our report also recommended that ITD and Finance require vendors providing credit card processing software and services be pre-certified for PCI-DSS compliance, and submit quarterly or annual PCI certifications of compliance to ITD and department contract managers. These recommendations have not been fully implemented to date.

Once those certifications have been obtained, the City will need to undergo another PCI-DSS compliance review. For example, since the last PCI-DSS review, two major City entities -- DOT's parking garages and Happy Hollow Park and Zoo -- have undergone major changes. ITD intends to initiate a PCI-DSS review of the two entities once an internal assessment has been completed.

Once that is completed and the Information Security Policy is done, in our opinion, it would behoove the City to initiate another comprehensive review of its PCI-DSS compliance because the City has undergone changes since the last review (including a change in the City's financial institution). Finally, the City needs to ensure that departments clearly understand what their responsibilities are for processing credit card transactions. The policy should address various categories of users (as discussed previously) such as:

- IT staff,
- Staff who have access to cardholder data,
- All city employees, and
- Vendors/contractors/Business partners.

---

<sup>9</sup> Vendors "hosting" a service are fully responsible for the hardware and software that is required for accepting credit card transactions.

**Recommendation #4:** In order to fully comply with Data Security Standards (PCI-DSS), immediately develop an Information Security Policy and include within this policy (applicable to all users who are connected to the City's network) the following minimum standards:

- a) Updated password and access protocols (see Recommendation #2);
- b) Required schedules for periodic reviews of people with access to data center (including restricting the number of people with access);
- c) Improved guidelines to departments for facilitating IT network changes during inter-departmental transfers and terminations;
- d) Training and implementation of the City's information security policy;
- e) After developing and implementing a Council-adopted Information Security Policy, initiate a citywide data security assessment to identify City's PCI-DSS status.

---

### **The City Has Work to do to Fully Implement Its Identity Theft Protection Plan**

The City's 2008 Identity Theft Prevention Program (ITPP) sought to "...assist staff to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags..." The ITPP applies to utility accounts and various loan programs for individuals and sole proprietorships. As part of the City's Identity Theft Prevention Program, Senior Staff within the stakeholder departments were responsible for oversight and reporting on service provider arrangements.

In addition to credit card information, the City handles and retains substantial amounts of private personally identifiable information of residents, merchants, and employees. The City's e-government policy provides information on how the City will use personally identifiable information. According to City Policy Manual 1.7.5: "The City will make every reasonable effort to protect your privacy. It restricts access to your personal identifiable information to those employees who will respond to your request. The City does not intentionally disclose any personal information about our customers to any third parties or outside the City except as required by law or by the consent of the person providing the information. The City only collects personally identifiable information that is required to provide service."

We found that in at least one contract with a vendor, the City did not get assurance that the vendor had sufficient guidelines to protect resident information. Specifically, the vendor collects personally identifiable information through a link on the City's website; however, nothing in its contract protects the City from harm that may result from a breach of the vendor's data.

Other government agencies have suffered significant consequences from such breaches. For example, in August 2011, an online group infiltrated the Bay Area Rapid Transit (BART) website and obtained personally identifiable information of hundreds of users, and posted it on the internet. This included names, addresses, phone numbers, emails and account passwords. This information is similar to the information collected by this vendor.

In addition to resident information, City employees also handle large amounts of personal information on City employees. This includes sensitive information such as birthdates, social security numbers and dependent information. We found that a large number of employees have access to sensitive employee information. Specifically, over 400 current employees have access. And while these employees are required to establish a business purpose for having such access, employees are not provided with guidelines for how to responsibly access, use and store the information. According to guidelines by the University of Minnesota, Office of Information Technology: *"University Policy requires University private data must be stored on University-owned computers. Employees must not store University private data on personally owned computers or other personally owned electronic devices. The other documents, spreadsheets and files containing University data should also be stored on a University file server."* There are also no policies on when this access would be terminated.

**BEST PRACTICES: THE PROPOSED PERSONAL DATA PRIVACY AND SECURITY ACT OF 2009**

The Personal Data Privacy and Security Act of 2009, was a bill proposed in the United States Congress to increase protection of personally identifiable information by private companies and **government agencies**, set guidelines and restrictions on personal data sharing by data brokers, and to enhance criminal penalty for identity theft and other violations of data privacy and security. It imposes requirements for a personal data privacy and security program on business entities that maintain sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons. It further requires a business entity that is subject to data privacy and security requirements to: (1) implement a comprehensive personal data privacy and security program to ensure the privacy, security, and confidentiality of sensitive personally identifying information and to protect against breaches of and unauthorized access to such information that could create a significant risk of harm or fraud to any individual; (2) conduct risk assessments of potential security breaches; (3) adopt risk management and control policies and procedures; (4) ensure employee training and supervision for implementation of data security programs; and (5) undertake vulnerability testing and monitoring of personal data privacy and security programs. Finally, it imposes civil penalties that violate the data privacy and security requirements and grants enforcement authority for such requirements to the FTC.

The ITPP requires the City to periodically review and report on guidelines for employees responsible for handling private information and make changes based on these reports. In its 2007 Data Security Report, the Governmental Accountability Office (GAO) noted: *“Identity theft can cause substantial harm to the lives of individual citizens—potentially severe emotional or other nonmonetary harm, as well as economic harm.”* In our opinion, the City should implement the ITPP and ensure periodic reviews of the business need for this access.

**Recommendation #5: The City should expand its Identity Theft Prevention Program to include all programs that collect personally identifiable information and:**

- a) Annually review, amend and report on the status of handling private information.**
- b) Annually review the business needs of employees with access to private information and update accordingly.**
- c) Provide periodic training for all employees handling private information and/or annually highlight (through an email) and inform employees of their responsibilities on safeguarding this data.**
- d) Include boilerplate language in its contracts to protect the City from liability when personally identifiable information is collected and ensure that the contractor has controls in place to secure and protect this information.**
- e) Ensure that the ITPP guidelines are posted publicly and easily accessible by City employees.**

---

#### **Additional Written Policies and Procedures Are Needed**

ITD does not have internal formalized documented policies and procedures. We also found that the City Policy Manual does not provide any guidance on certain information technology issues. Formal, documented policies and procedures are important because they outline clear standards that can be useful even after personnel changes. Furthermore, we believe that the formal documented policies and procedures would provide consistency and standardization among the various information technology functions that rely on ITD.

Even though some departments are in charge of their own information technology functions, ITD provides basic services such as email, network access and access to various enterprise information systems such as FMS and PeopleSoft. In those instances, it would be important to ensure that there is a standardized usage policy applicable for all user departments. However, the independent information technology functions could follow their own, in some cases, more stringent policies (compliant with applicable laws and standards).

The City has established certain Citywide information technology-related policies including: Telecommuting, Remote Access, E-Government Policy, Information Security Policy and Web-based Communications Policy. However, the City lacks centralized information technology policies surrounding ITD responsibilities and chain of command, principles of least privilege (restricting access), acceptable use of computer equipment, compliance with various federal and State guidelines such as HIPPA and PCI-DSS, making use of illegal software, etc.

**Recommendation #6: We recommend that ITD develop the following written policies and procedures:**

- a) **Internal policies and procedures on day-to-day operations within ITD;**
- b) **Citywide policies on technology usage such as ITD responsibilities in enforcement, principles of least privilege, and acceptable use of computer equipment. Within these policies develop clear guidelines on which departments would be exempt and why, from some of these policies.**

## **Finding II    The Information Technology Department's Backup Process Is Inconsistent and Resource-Intensive**

### *Summary*

Disasters are events that can threaten the availability of data or network infrastructure. Power outages, hardware failures, data corruption, and hacking attacks are examples of such disasters. Backups and disaster recovery planning are intended to limit the exposure to, and ill effects from, such disasters whether they arise by circumstance, accident or malice. The current backup process for many of the City's computer systems is inconsistent and resource-intensive.

---

### **ITD Has an Informal and Undocumented Backup Process**

ITD currently maintains most departments' data in the City's Network Operating Center (NOC). In order to ensure safekeeping of stored data (including payroll data and financial data on the City's Financial Management System), ITD has developed an informal backup process. Backups are copies of data and systems that can be deployed if primary data and applications become unavailable. A good backup process would ensure that during or after an emergency when data or applications are unavailable, ITD is able to access backups to recover historical data and restore the City's ability to resume operations.

ITD has developed an undocumented backup process which relies on a combination of hard drives and tapes. Specifically, ITD saves changes to files and applications that City employees save round-the-clock. These changes are saved on hard drives in the NOC. Every other week, ITD saves full backup copies of files and applications which remain on the network for 90 days. These backups are available to ITD staff should they need to recover files and/or systems for end-users. Even as full backups remain on the network, ITD copies full backups onto tapes and sends them to storage.

ITD has developed distinct storage processes for "mission-critical" and "day-to-day" full backups.<sup>10</sup> Through a third-party storage provider, ITD sends "mission-critical" backups to offsite storage, while ITD staff store "day-to-day" backups in a storage area within the NOC. ITD has adopted storage retention periods for different types of backups. Exhibit 6 outlines some of the storage retention periods. The storage vendor also returns tapes on a pre-determined schedule for either destruction or reuse.

---

<sup>10</sup> Mission-critical data includes files, records, and systems that support the City's payroll, personnel, financial management, and billing systems. Non-critical "day-to-day" data include emails and other files.



**Exhibit 6: Key ITD Backup Retention Schedules**

Description of Data or System to be Stored/Backed-up	# of Days Stored within the Network Operations Center	Frequency of Pickups for Offsite Storage	# of Days Stored at Offsite Facility
Departments' Files	90 Days	Not applicable	Not Applicable
Financial and HR/Payroll Records	90 Days	14 Days	5 Years
Billing/Budget Records	90 Days	30 Days	5 Years

Source: Auditor summary of ITD's retention schedules as of October 2011.

**ITD Was Not Following Its Backup Process**

As mentioned above, ITD has arranged for "mission-critical"<sup>11</sup> backups to be delivered and stored off-site to a storage facility over 100 miles away. The purpose of this arrangement is to protect the City's mission-critical data from a regional disaster affecting the greater San José area.

We reviewed the third-party storage provider's activity logs to determine whether mission-critical backups were picked up according to ITD's self-prescribed timelines. Our review found that between October 2010 and October 2011, the City's mission-critical financial, billing and HR/Payroll records were picked up only sporadically for offsite storage. ITD's schedule dictates pickups every two weeks which would have resulted in 26 pickups. However, we found that mission-critical tapes were picked up only 8 times and mission-critical finance and payroll backups were not sent offsite for safekeeping at all for a 14-plus-week period between July and October 2011.

We also found that ITD was not following its backup and onsite storage schedules for day-to-day files. Specifically, we found that ITD was not storing tapes according to the retention schedule but instead, rotating/re-recording tapes based on the tapes' capacities.

---

**Opportunities Exist to Improve the Current Back-up Process**

Tape is a typical backup medium among information technology functions, but it is not the most efficient. For one, tapes are inherently damage prone. Secondly, tape backup processes are labor intensive, requiring substantial care and discipline by staff to perform backup duties such as: ensuring tapes are loaded/unloaded

---

<sup>11</sup> We should note that the SJP, Library, Airport, and WPCP are in charge of their own mission critical data backups and storage. We did not review their backup policies and processes.

into/out of tape drives, transporting and storing tapes in/to/from their appropriate locations, labeling and filing tapes for future reference, and ensuring that tapes are appropriately destroyed when they are no longer needed.

These steps require significant staff time that grow as data storage demands grow. ITD has one FTE solely dedicated to backing up and recovering data from these tapes.

Lastly, the tapes present data security risks in that they involve multiple handlers as tapes are transported to and from various storage facilities. The data security risks for the City of San José are heightened because ITD does not encrypt its backup tapes. ITD agrees and is currently in the process of looking at ways of improving its current process through investments in newer storage technology.

**ITD’s Backup Process Should Periodically Consider End-Users’ Assessment of Mission-Criticality and Needs to be Reviewed for Compliance with the City’s Adopted Document Retention Schedules**

As stated above, the only data sent offsite are data and applications deemed by ITD as “mission-critical.” According to ITD staff, backing up and sending all data offsite would require many more tapes and staff time than does the current process. However, we believe ITD’s sole reliance on onsite backups for some backups could present problems.

To our knowledge, ITD has not consulted with various departments to determine which data/applications would be mission-critical. ITD reports that its process for backing up departmental data is based on a retention schedule it developed in 2003 following a review of the Santa Clara County Grand Jury that urged local agencies to develop ITD disaster recovery plans. In our opinion, data owners should be periodically consulted about data back-up procedures.

In addition, end-users and Citywide Council-approved document retention schedules should be consulted to determine at what point the data should be destroyed, thereby reducing the City’s data storage needs.<sup>12</sup> According to ITD, the SAN is at 83 percent of its storage capacity. In our opinion, ITD should work with individual departments to determine business needs of each department and develop a data retention/backup schedules based on these business needs and the City’s approved document retention schedules.

---

<sup>12</sup> As noted earlier, ITD’s Storage Area Network (SAN) houses about 120 terabytes of data.

**Recommendation #7: In order to ensure that the City's critical data is protected ITD should:**

- a) Ensure that backups are done and tapes are sent off-site at the pre-determined intervals;**
- b) Get end-user input to determine if the current back-up process meets individual departments' business needs and City Council-approved document retention schedules; and**
- c) Formalize, document and implement these processes.**

## **Finding III    The City Does Not Have a Disaster Recovery Plan for Information Technology**

### *Summary*

We found that ITD does not have a documented disaster recovery plan defining the processes, responsibilities or roles for accessing and deploying business systems and data in the event of a disaster. Such a plan would include guidance for recovering mission-critical financial and payroll records and provides clarity on how ITD would deploy data and applications it backs up, and who will be involved in the deployment.

---

### **ITD Supports and Maintains Mission-Critical Data and Systems**

ITD provides support that enables City departments to deliver day-to-day services. Specifically, ITD ensures that data, applications and the City's network are available for the City to continue ongoing day-to-day functions such as file storage, utility billing, traffic signaling, etc. In the event of an emergency affecting the City's network, applications or data, individual departments may need to draw on their own contingency plans in order to continue delivering services without ITD. However, some ITD-dependent functions, including mission-critical functions, rely on data stored within the City's budget, payroll, personnel, and financial management systems. These systems, requiring ITD's expertise to maintain, are applications without which the City could not operate. Some examples of these applications include the City's PeopleSoft payroll system, the City's Financial Management System (FMS), and DOT's traffic light applications.

We found that ITD's practice of functioning with few formal, documented policies and procedures also extended to its disaster recovery processes. In fact, to our knowledge none of the aforementioned ITD-dependent mission-critical functions have formal disaster recovery plans. This means that in the event of a disaster or a technical disruption affecting the network, applications or data, services would be potentially threatened. Keeping these services running and being able to quickly restore these services after an emergency is an essential part of the City's mission to "...provide quality public services, facilities and opportunities that create, sustain and enhance a safe, livable and vibrant community for its diverse residents, businesses and visitors." ITD's current untested disaster recovery process would be entirely reliant on its tape backup process working (see previous chapter).

### **Some Departments Maintain Their Own Formal Disaster Recovery Plans**

The SJPD, Library, and WPCP maintain formal disaster recovery plans. One of the reasons for these departments' diligence is that they are subject to review by various outside organizations. For example, because of the sensitivity of SJPD's data, they are subject to regular reviews by Federal and State organizations such as the Federal Bureau of Investigations' Criminal Justice Information Services and the State of California Department of Justice. Similarly, the WPCP may be subject to review by federal agencies, as it is considered a "critical infrastructure" facility by the federal government.

### **Other Entities Confirm the Importance of a Formal Disaster Recovery Plan**

The importance of disaster recovery planning is confirmed by a number of authoritative entities. In 2003 the Santa Clara County Civil Grand Jury conducted a review of local agencies' technology disaster preparedness and recommended: *"all cities/towns within Santa Clara County and all county agencies/authorities/districts should have written disaster recovery plans for mission-critical computer information systems, and should regularly test and update these plans."*

The Government Finance Officers Association (GFOA)<sup>13</sup> recommends *"...every government formally establish written policies and procedures for minimizing disruptions resulting from failures in computers or other advanced technologies following a disaster."* GFOA further recommends that a disaster recovery plan *"should be evaluated annually and updated periodically, no less than once every three years"* and outlines minimum components of disaster recovery policies and procedures including: assigning disaster recovery coordinators for each agency or department to form a disaster recovery team, creating and preserving back-up data, making provisions for the alternative processing of data following a disaster, providing detailed instructions for restorations, and establishing guidelines in the immediate aftermath of a disaster.

In our opinion, the lack of a disaster recovery/business continuity plan endangers City operations, technology infrastructure and data, and defies common sense, industry standards, and the City's best interests.

### **The Age of Some Mission-Critical Systems Increases the Need for Disaster Data Recovery Plans**

In keeping with the City's stated commitment of actively managing the assets in a way that minimizes liability and loss, in 2009-10 the City's Risk Manager led a citywide team of senior staff that conducted a citywide risk assessment. The

---

<sup>13</sup> The purpose of the Government Finance Officers Association is to enhance and promote the professional management of governments for the public benefit by identifying and developing financial policies and best practices and promoting their use through education, training, facilitation of member networking, and leadership.

2009-10 risk assessment identified "business systems," "information security," and "IT infrastructure" among the City's highest risks, meaning failures in these areas were either likely and/or would present significant costs to the City.

Further, the assessment identified key Citywide enterprise systems that support mission-critical functions that are operating beyond their predicted lifespans. These enterprise systems may be more likely to fail and more difficult to restore.

FMS was identified as a vulnerable system. Restoring it after a failure could be difficult because it is beyond its recommended lifespan (see Finding V for more discussion on the aged critical systems). In our opinion, having an IT-specific disaster recovery plan is particularly important given that some of our enterprise systems are beyond life expectancies.

### **Proposed Redundant Data Center**

As mentioned before, ITD is in the process of developing a redundant data center in a different location with the intent of establishing it as a potential redundant center to the main NOC. ITD sees the redundant data center as key in its disaster recovery planning, as it is expected to fill-in during and after a localized disaster at the main NOC. ITD also envisions the future data center as a backup storage repository. According to ITD staff, the department is in the process of finding consultants to install a storage network that will physically link storage at the remote data center with the NOC. ITD plans for the system to also link both facilities to distant backup facilities via the internet. However, currently the remote data center is minimally used and houses only some departments' back-up hardware.

### **ITD Needs to Ensure That Critical Data Is Recoverable in Case of a Disaster**

In case of a natural or man-made disaster, the City will not be able to function and perform critical functions without access to data. ITD understands the need for a formal disaster recovery plan. However, as mentioned above, the department has never developed one. There have been attempts towards disaster planning, as evidenced by the attempt to create a redundant data center. In our opinion, even though end-user departments are responsible for day-to-day contingency plans, ITD is the City's "keeper" of most critical electronic data and has a key responsibility for ensuring that the City has a viable and workable disaster data recovery plan.

**Recommendation #8: ITD take the lead to develop (and test) a Disaster Data Recovery Plan and ensure that end-user business needs are included in the final plan.**

**This page was intentionally left blank**

## **Finding IV The Information Technology Department Should Improve Its Inventory Practices**

### *Summary*

Most departments fund their own computer equipment and software. There is no centralized process to capture all technology-related budget and expenditure information citywide. Furthermore, there is no centralized tracking of all technology tools. A centralized inventory would allow ITD to: a) better evaluate purchasing needs, and b) identify opportunities to redistribute and/or share equipment and software. Finally, the City should establish policies regarding decommissioning its computer equipment.

---

### **Most Departments Fund Their Own Computer Equipment and Software**

Currently each department is responsible for determining their own ITD purchasing needs and they budget for these purchases through their own department budgets. When departments want to make technology purchases, they request approval from ITD through the “technology purchases approval” process. ITD’s consideration of these requests is based largely on the items’ compatibility with ITD’s network and data security considerations. Some items may be exempted from the approval process, although some of those may still require ITD staff assistance to purchase or install. The following are purchases that are generally exempt:

- All printers, scanners, projectors, fax machines and peripherals purchased through an existing citywide purchase order under \$20,000,
- All maintenance renewals, and
- Common desktop software under \$20,000.

Any items that do not meet the above criteria will be subject to Technology Approval, which is coordinated by ITD staff in conjunction with the Budget Office. Once requests are approved, ITD’s service desk will either order the items or notify departments to proceed with an order.

### **Lack of Information About Citywide Technology Expenditures**

Even though ITD’s operating budget is around \$19 million for 2011-12, this is only a portion of what the Citywide technology expenditures are. However, there is no centralized process to capture technology-related budget and expenditure information throughout all departments. For example, the City’s personnel



records show that in September 2011, outside of ITD, 65 technology-related classifications were filled in 13 different departments. The most common information technology classifications were Information Systems Analysts, Network Engineers and Network Technicians. We found 11 of 30 Information Systems Analysts worked outside of ITD, and 33 of 58 Network Engineers and Network Technicians worked outside of ITD. Other information technology classifications throughout the City included Communications Technician, Senior Electronic Systems Technician, Systems Applications Programmer, Senior Systems Applications Programmer and Supervising Applications Analyst.

Non-personal technology expenditures are even more difficult to capture. Although there is a code for how these expenditures can be classified (detail 4051), purchases may be classified under “supplies” or other non-personal expenditures.

The 2009 Management Partners Report also expressed concerns with the lack of good tracking of technology spending. According to Management Partners, “[...] total citywide IT expenditures are not known to the City of San José. Line department IT spending is generally spread across several budget elements; there is no IT expense category that corrals all IT spending across the entire departmental budget.”

According to the Management Partners’ report, industry standards suggest that IT staffing should be between 3-5 percent of total organization staffing. ITD’s estimated staffing together with the additional 65 employees in other departments constitute a little over 2 percent of the General Fund staffing. In our opinion, the first step to identify ways to better leverage the City’s technology investments and identify cost-savings opportunities, is to better understand and accurately identify total technology budget and expenditures.

---

### **There Is No Centralized Tracking of Technology Inventory**

As a result of this individualized technology procurement process, there is no accurate technology inventory. ITD does not maintain and update records of technology purchases, and independent departments with their own information technology functions maintain their own inventories, and ITD is unable to track them (e.g. Airport, Library, Fire, Police, Retirement Services, and WPCP).

Recognizing the need for tracking the City’s inventory, in 2009 ITD spent nearly \$100,000 on an asset management system. However, the system cannot be used to regularly track or report on the City’s technology inventory. Asset information drops off the inventory if it is unused for more than two weeks. Further, the system does not track individual license information. If the City were better tracking its technology assets, it could more efficiently identify unused or minimally used assets, and potentially redistribute them.

An accurate asset inventory would reduce duplication and possibly increase inter-departmental sharing of hardware and software. Various departments use redundant software packages. For example, the City currently has three versions (independently purchased) of GIS software.

In addition, various departments make independent purchases of software depending on their business needs at a given time, but often, once the business need has been met, software may lie unused and/or underutilized. This problem has become bigger as a result of the staff reductions the City has endured. Because ITD does not maintain a centralized inventory, there is no process to review and share this unused software.

#### *Software Installations*

The last time ITD made a mass purchase of office productivity licenses (word processing, spreadsheets, presentations, and email) was in 2005. Based on City staffing levels at that time, ITD purchased licenses to install various Microsoft Office product licenses for over 6,500 City computers. The estimated cost for this installation was over \$1.3 million. As of September 2011, there are about 5,000 fulltime employees working for the City. We estimate there are more than 1,000 office productivity packages that are not being used (the above mentioned features of the asset management system preclude us from precisely quantifying or even locating the unused packages). These packages are probably lying dormant in unused workstations.

ITD's practice has been to install software assets at individual workstations oftentimes purchased by individual departments. In our opinion, doing centralized installations would make it easier to manage and redistribute assets like software, according to usage. Furthermore, to quickly respond to various changes in the number of staff workstations and resultant changes in software usage, the City should explore other ways to reduce its cost of maintaining and buying expensive and potentially redundant software. One potential way to do this would be by pursuing subscription-based agreements with providers of various software licenses. Subscription-based agreements allow a user to pay for a pre-determined number of applications and users only pay for those. Such agreements allow a user to either increase or decrease the number of licenses that they will pay for depending on the anticipated number of users as an annual subscription model.

A subscription format whereby the City pays a periodic fee based on use could be more efficient because the City would only need software that its employees are using. Further efficiencies could arise from ongoing updates and enhancements, and desktop support for software issues. According to an IT professional at the City & County of San Francisco, they have used a subscription model for a Portable Document Format (PDF) application. As a result, San Francisco pays less than \$10 per user per year. Further, any change in the number of employees can be reflected in the number of subscriptions. In contrast, the City of San José buys a similar software package which is installed on onsite on individual work

stations. This particular application costs about \$300 per license, and like the City's currently underutilized office productivity packages, is not redeployed when unused.

**Recommendation #9: ITD should collect, maintain and periodically update a central inventory of computer equipment and software, and should use its inventory management system and records of technology purchases to:**

- a) better evaluate purchasing needs,
- b) identify opportunities to redistribute and/or share equipment and software, and
- c) to the extent possible, ITD should pursue opportunities to centrally-install packages, rather than installing packages at individual workstations.

---

### **There Is No Centralized Policy for Decommissioning Old or Unused Computer Equipment**

Often departments send to ITD computer equipment that they no longer need or want. After collecting such equipment, we observed that ITD staff routinely remove and erase hard drives prior to surplusing them to third-party vendor that picks them up. We felt this decommissioning process was appropriate because hard drives can contain sensitive or confidential information. However, this practice is not formalized as a citywide policy, and it is up to individual departments to inform ITD of the need for getting rid of old computer equipment. As a result, various City departments leave unused computer equipment dormant in empty cubicles or store unused equipment in empty cubicles and storage spaces. Exhibit 7 shows a department with unused computer equipment.

**Exhibit 7: Unused City Computer Equipment Collecting in a Cubicle**

Source: Auditor photo (November 2011).

In our opinion, this practice is risky as many of these computers may have sensitive information such as employee social security numbers, and other information on the hard drives.

**Recommendation #10: Because computer equipment may contain personal identifiable information and other sensitive information, ITD should develop, distribute, and implement a Citywide policy for decommissioning computer equipment, and include it in the citywide surplus inventory policy.**

**This page was intentionally left blank**

## **Finding V Many of the City's Computer Systems Are Outdated and Should be Replaced**

### *Summary*

The City of San José is located in the heart of Silicon Valley, but operating with twentieth century technology. Many of the City's mission-critical applications are antiquated and many years past their life cycle. In our opinion, the City needs to review its current critical systems, determine its replacement needs and ensure that future systems are viable in dynamic environments.

---

### **The City's Outdated Computer Systems**

It will not be news to anyone who's been around City Hall for very long that some of the City's computer systems and software applications are old, archaic, and generally outdated. Not only does this affect employee productivity – the long-term viability of these systems should be reviewed. Described below are just some examples of the City's outdated systems.

*FMS:* The City's FMS which houses all of the City's financial information is based on the Cayenta Financial Management Applications Suite. It was originally installed in 1989. Because the current version of FMS, Cayenta 7.3 reached end of support, the City has had to upgrade to a new version which included a migration from the existing Sun/Unix platform to an all-Windows platform at a cost of \$48,000. To ensure on-going viability and support of these critical reports and programs, staff has embarked on a project to migrate these key reports and processes from COBOL to Crystal and alternate supported platforms. There are three ITD employees able to provide support to FMS. As mentioned above, per the City's own risk assessment, FMS is past its lifecycle. Only the City of San José uses FMS among its Bay Area city peers.

*PeopleSoft:* The current PeopleSoft system will stop receiving technical support from its manufacturer by end of 2012. The City needs to determine whether it should upgrade the system or outsource the service. It is estimated that an upgrade would cost at least \$2.5 million. The City is in the process of reviewing other options.

*Personal Computer Operating Systems:* Specifically, the most commonly used operating system (Windows XP)<sup>14</sup> in the City has been in the market for at least 10 years. Since then, several updated versions have been developed. In addition to various compatibility issues that arise when using outdate operating systems, a

---

<sup>14</sup> The asset management system also shows seventeen Windows 2000 operating systems. All support for Windows 2000 ended in July 2010.

significant security risk exists when the company ceases providing security updates, technical support and patches for the operating system. For instance, according to the timetable posted by the City's operating system vendor, general licensing of this operating system to original equipment manufacturers and terminated retail sales of the operating system ended on June 30, 2008. This time period was extended, and on April 14, 2009, the operating system was moved from "Mainstream Support" to "Extended Support." During the Extended Support Phase, the company will continue to provide security updates every month; however, free technical support, warranty claims, and design changes are no longer offered. On April 8, 2014, all support, including security updates and security-related fixes, will be terminated.

*The City's budget system:* This is a collection of modules that automate many of the processes used by the City Manager's Budget Office and City departments to develop the annual budget and publish the numerous budget documents. These systems were developed by internal City staff using Oracle database and tools. There are six key modules including the Automated Budget System (ABS), Capital Automated Budget System (CABS), Proposal Database System (PDS), Mid-year/Annual Report System, Ordinance system, and Fees and Charges System. ITD is evaluating alternatives for the platform hosting the budget applications. The current product will reach end of support in FY 2011-12. According to ITD staff, there is currently only one employee that is able to support this system.

### **Management Partners and the IT Master Plan Also Expressed Concerns About Old IT Systems**

More than a decade ago (as early as 2000), the IT Master Plan expressed concerns about IT infrastructure. According to the Plan, IT investment had not been a priority, and most departments did not have an adequate level of technical support to realize the full potential of the installed systems. Because of this, ITD staff often spent their time reacting to problems rather than being an enabler of improved business functions and services. According to the Plan, the City would have to be willing to make appropriate investments in IT support staff, technical and end user training, and computing and communication systems. Failure to invest appropriately would hinder the City's ability to deploy and support new means of service delivery using existing and emerging technologies.

Management Partners repeated some of these concerns about IT expenditures. Specifically, that IT expenditures should closely correlate with the size of the enterprise they support, (i.e. the total number of city employees). San José fell well below the average expenditures of peer cities and committed the lowest percentage of total IT expenditures to non-compensation budget elements. Further, the report stated that in addition to large redundant business applications, several non-redundant software packages were running on old computer operating systems. Some were small applications, but the core financial software package, utility billing system, and components of the online permit system were also running under older operating systems. Finally, Management

Partners recommended that keeping business systems within a few years of the current state-of-the-art can be an important component in ensuring services reliability.

### **Problem Supporting Outdated Computer Systems and Hardware**

In addition, the City can find itself with major support problems when the few employees with the requisite skills leave the organization during a time when these skills are also increasingly rare outside of the City. Transitioning to systems that are more commonly understood by IT professionals would mitigate the City's risk of a system "crashing" and ITD being unable to "bring it up again".

Furthermore, in practice and **when funds are available**, ITD approves the replacement of old personal computers if they are experiencing problems and the cost of replacement is less than the cost of having a technician spend time fixing them, or if problems with a personal computer are preventing the end user from being able to perform their job functions. However, ITD's decision process is not documented and is informal, and depends on whether the department has sufficient funds. In addition, the City does not have a formal, written policy or guidance on the replacement of its old computer equipment.

According to the ITD CIO, technicians oftentimes may attempt to repair old computers. The employee's time in fixing the equipment is oftentimes more than the cost of purchasing new items. For example, it costs about \$450 to replace a desktop. The average ITD technician costs over \$50 per hour. In essence, buying a new desktop would be more cost-effective if repairs require more than 9 hours of ITD staff time. In our opinion, ITD should develop parameters on the cost of replacement versus repair of certain ITD equipment.

The City's level of funding for technology continues to remain extremely limited. As cited earlier, ITD staffing is a little over 2 percent of total organization staffing whereas the industry standard recommends 3-5 percent. As critical systems age, many require substantial investments simply to maintain existing functionality. While consolidation of resources, tools, and investments will mitigate some of the effect of funding gaps, consolidation itself is not a substitute for reasonable technology investments in a more efficient, secure, and flexible organization. In our opinion, given budgetary constraints, the City needs to take a risk-based approach to reviewing the age of its critical computer systems and determine a replacement schedule for those that are deemed "high-risk".

**Recommendation #11: Review the life expectancies of critical computer systems and determine a replacement schedule and budget for the highest-priority systems and hardware.**



**This page was intentionally left blank**

# Conclusion

Our review of IT general controls identified several weaknesses in passwords and access controls. The City has not implemented top priority recommendations from a 2008 information security audit to ensure compliance with payment card industry data security standards (PCI-DSS) and should follow up on its Identity Theft Protection Program guidelines. In addition, IT should improve its backup, disaster recovery and inventory practices. Finally many of the City's computer systems are outdated and should be replaced.

## RECOMMENDATIONS

Recommendation #1: To ensure changes to the City's network and mission-critical enterprise systems are tightly controlled, ITD should immediately change the password to its shared administrative account, ensure that administrative log-ins to the City's network are traceable, and strictly limit administrative log-in privileges to those who absolutely need such privileges. Furthermore, we recommend that the ITD CIO annually review and approve the memberships of shared accounts that can access the City's network and enterprise systems, and if necessary make changes based on current business needs.

Recommendation #2: To improve password and access controls over the City's network and data, ITD should:

- a) Establish minimum length and complexity requirements for users' passwords, automatic periodic expiration schedules, and "lock-outs" when users reach a pre-determined number of consecutive unsuccessful login attempts.
- b) While granting access to additional server drives, etc., ITD should by default, terminate transferring employees' access to the drives of the departments they are departing, or explore a system through which employees' access levels are tied to their employment status as recorded in the City's personnel system.
- c) Develop a review process requiring departments to periodically review the users with access to their departmental drives.

Recommendation #3: The City should include boilerplate terms to include in contracts with third parties the following:

- a) Require PCI-DSS compliance when contractors are responsible for collecting credit card information.
- b) Require the vendors to submit current PCI-DSS compliance certificates on an ongoing basis.

## Information Technology General Controls

---

Recommendation #4: In order to fully comply with Data Security Standards (PCI-DSS), immediately develop an Information Security Policy and include within this policy (applicable to all users who are connected to the City's network) the following minimum standards:

- a) Updated password and access protocols (see Recommendation #2);
- b) Required schedules for periodic reviews of people with access to data center (including restricting the number of people with access);
- c) Improved guidelines to departments for facilitating IT network changes during inter-departmental transfers and terminations;
- d) Training and implementation of the City's information security policy;
- e) After developing and implementing a Council-adopted Information Security Policy, initiate a citywide data security assessment to identify City's PCI-DSS status.

Recommendation #5: The City should expand its Identity Theft Prevention Program to include all programs that collect personally identifiable information and:

- a) Annually review, amend and report on the status of handling private information.
- b) Annually review the business needs of employees with access to private information and update accordingly.
- c) Provide periodic training for all employees handling private information and/or annually highlight (through an email) and inform employees of their responsibilities on safeguarding this data.
- d) Include boilerplate language in its contracts to protect the City from liability when personally identifiable information is collected and ensure that the contractor has controls in place to secure and protect this information.
- e) Ensure that the ITTP guidelines are posted publicly and easily accessible by City employees.

Recommendation #6: We recommend that ITD develop the following written policies and procedures:

- a) Internal policies and procedures on day-to-day operations within ITD;
- b) Citywide policies on technology usage such as ITD responsibilities in enforcement, principles of least privilege, and acceptable use of computer equipment. Within these policies develop clear guidelines on which departments would be exempt and why, from some of these policies.

Recommendation #7: In order to ensure that the City's critical data is protected ITD should:

- a) Ensure that backups are done and tapes are sent off-site at the pre-determined intervals;
- b) Get end-user input to determine if the current back-up process meets individual departments' business needs and City Council-approved document retention schedules; and
- c) Formalize, document and implement these processes.

Recommendation #8: ITD take the lead to develop (and test) a Disaster Data Recovery Plan and ensure that end-user business needs are included in the final plan.

Recommendation #9: ITD should collect, maintain and periodically update a central inventory of computer equipment and software, and should use its inventory management system and records of technology purchases to:

- a) better evaluate purchasing needs,
- b) identify opportunities to redistribute and/or share equipment and software, and
- c) to the extent possible, ITD should pursue opportunities to centrally-install packages, rather than installing packages at individual workstations.

Recommendation #10: Because computer equipment may contain personal identifiable information and other sensitive information, ITD should develop, distribute, and implement a Citywide policy for decommissioning computer equipment, and include it in the citywide surplus inventory policy.

Recommendation #11: Review the life expectancies of critical computer systems and determine a replacement schedule and budget for the highest-priority systems and hardware.

**This page was intentionally left blank**

# Memorandum

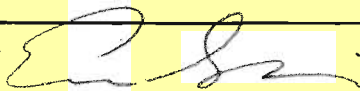
**TO:** SHARON ERICKSON  
CITY AUDITOR

**FROM:** Vijay Sammeta

**SUBJECT: RESPONSE TO THE AUDIT  
ON INFORMATION TECHNOLOGY  
GENERAL CONTROLS**

**DATE:** January 17, 2012

Approved



Date

1/17/12

The Information Technology Department (ITD) has reviewed the Audit on Information Technology General Controls and is in overall agreement with the recommendations identified in the report. Many elements of the recommendations are already being addressed by ITD in the form of policy and procedural changes or through the phased Citywide IT consolidation effort. However, the City employs a highly distributed model of IT support which will necessitate a joint endeavor with Council, Council Appointees and the City Administration to draft, mandate and enforce recommended policy changes. Further, a Citywide Information Security Policy is currently being drafted by ITD and the City's Information Security Consultant. Following coordination with the City Attorney's Office, this policy is expected to be submitted for Council approval by April, 2012.

As the Auditor's Report noted, many of the City's technology investments are outdated with keys systems such as HR/Payroll and the City's budgeting system being implemented more than a decade ago. The oldest enterprise application is the financial management system (FMS), which is over 25 years old. While upgrades have occurred since implementation, those systems are no longer reflective of the needs of the City and present increasing risks to sustain operations. As a result, the "Capital of Silicon Valley" finds itself with ineffective and/or antiquated technology running its core business. Considerable funding is required to replace or modernize current systems, reverse the City's multi-year trend of underinvestment in technology and begin to mitigate risks as outlined in the Audit Report.

The following are the ITD responses to each recommendation in the Audit Report.

## RECOMMENDATIONS AND RESPONSE

***Recommendation #1: To ensure changes to the City's network and mission critical enterprise systems are tightly controlled, ITD should immediately change the password to its shared administrative account, ensure that administrative log-ins to the City's network are traceable, and strictly limit administrative log-in privileges to those who absolutely need such privileges. Furthermore, we recommend that the ITD CIO annually review and approve the memberships***

*of shared accounts that can access the City's network and enterprise systems, and if necessary make changes based on current business needs.*

**ITD Response to Recommendation #1:** ITD is in general agreement with the recommendation to tighten password controls. The Department has already begun changing passwords for shared accounts with privileged access to key systems. In addition, the Chief Information Officer (CIO) will be providing guidelines in a forthcoming Information Security Policy for departments to evaluate risk associated with shared administrative accounts.

Further, ITD has auditing software in place to track account changes to all Active Directory network accounts, including shared and administrative log-ins. The Department will perform scheduled reviews of logs to identify potential misuse. ITD will formalize a policy to review shared accounts with departments that requires periodic reauthorization by the CIO.

***Recommendation #2: To improve password and access controls over the City's network and data, ITD should:***

***A) Establish minimum length and complexity requirements for user's passwords, automatic periodic expiration schedules, and "lock-outs" when users reach a pre-determined number of consecutive unsuccessful login attempts.***

***B) While granting access to additional server drives, etc., ITD should by default, terminate transferring employees' access to the drives of the departments they are departing, or explore a system through which employees' access levels are tied to their employment status as recorded in the City's personnel system.***

***C) Develop a review process requiring departments to periodically review the users with access to their departmental drives.***

**ITD Response to Recommendation #2:** ITD agrees with this recommendation. The Department is currently working on the introduction of additional password complexity and is developing a process to tie account access to the HR/Payroll system to disable or transfer accounts in a more timely fashion. ITD also agrees with Section C, and will work with the City Administration to develop a policy requiring departments to periodically review approved access to individual department drives.

***Recommendation #3: The City should include boilerplate terms to include in contracts with third parties the following:***

***A) Require PCI-DSS compliance when contractors are responsible for collecting credit card information.***

***B) Require the vendors to submit current PCI-DSS compliance certificates on an ongoing basis.***

**ITD Response to Recommendation #3:** ITD agrees with this recommendation and will work with its PCI Audit firm, Finance and the City Attorney's Office to develop appropriate PCI language for the City's standard contract templates.

***Recommendation #4: In order to fully comply with Data Security Standards (PCI-DSS) immediately develop an Information Security Policy and include within this policy (applicable to all users who are connected to the City's network) the following minimum standards:***

- A) Updated password and access protocols (see Recommendation #2)***
- B) Required schedules for periodic reviews of people with access to data center (including restricting the number of people with access)***
- C) Improved guidelines to departments for facilitating IT network changes during inter-departmental transfers and terminations***
- D) Training and implementation of the City's information security policy***
- E) After developing and implementing a Council-adopted Information Security Policy, initiate a citywide data security assessment to identify City's PCI-DSS status.***

**ITD Response to Recommendation #4:** ITD agrees with this recommendation and has already taken steps to address most of the elements described above. In addition, ITD is working with its Information Security Consultant to formalize an Information Security Policy. Section A was addressed in Recommendation #2. Periodic access review for the Data Center as described in Section B is already performed, but a schedule will be formalized that requires approval by the CIO. Improved guidelines for departments in facilitating network changes will be documented in the forthcoming Information Security Policy and implemented in the HR/Payroll system as recommended in Section C. ITD is in agreement with Sections D and E; a training and implementation program will be developed and another Citywide information security audit will be performed following Council adoption of an Information Security Policy.

***Recommendation #5: The City should expand its Identity Theft Prevention Program to include all programs that collect personally identifiable information and:***

- A) Annually review, amend and report on the status of handling private information,***
- B) Annually review the business needs of employees with access to private information and update accordingly.***
- C) Provide periodic training for all employees handling private information and/or annually highlight (through an email) and inform employees of their responsibilities on safeguarding this data.***
- D) Include boilerplate language in its contracts to protect the City from liability when personally identifiable information is collected and ensure that the contractor has controls in place to secure and protect this information.***
- E) Ensure that the ITPP guidelines are posted publicly and easily accessible by City employees.***

**ITD Response to Recommendation #5:** ITD is in general agreement with this recommendation; however, personally identifiable information (PII) is not necessarily connected with technology. In many cases, the information is collected in other manners such as verbally or in writing. For this reason, the CIO will advise the City Manager to direct Sections A and B above to all departments that have responsibility for collecting PII. Training for the handling of PII as outlined in Section C will be incorporated in information security training. ITD will work with Finance and the City Attorney's Office on language related to PII as recommended in



Section D. ITD agrees with Section E and will incorporate the language into the Information Security Policy.

***Recommendation #6: We recommend that ITD develop the following written policies and procedures:***

- A) Internal policies and procedures on day-to-day operations within ITD;***
- B) Citywide policies on technology usage such as ITD responsibilities in enforcement, principles of least privilege, and acceptable use of computer equipment. Within these policies develop clear guidelines on which departments would be exempt and why, from some of these policies.***

**ITD Response to Recommendation #6:** ITD is in agreement with Recommendation #6. Staff will formalize and document policies and procedures on day-to-day operations where they do not exist as specified in Section A. With respect to Section B, ITD will work with the City Administration to review existing policies on acceptable use and develop new policies where necessary. Those that relate to information security will be incorporated into the Council-adopted Information Security Policy.

***Recommendation #7: In order to ensure that the City's critical data is protected ITD should:***

- A) Ensure that backups are done and tapes are sent off-site at the pre-determined intervals;***
- B) Get end-user input to determine if the current back-up process meets individual departments' business needs and City Council-approved document retention schedules; and***
- C) Formalize, document and implement these processes.***

**ITD Response to Recommendation #7:** ITD is in agreement with Recommendation #7. To address Sections A and B, ITD will perform an operational "ground up" review to link back-ups with retention schedules as well as disaster recovery and business continuity planning. Department management will devise a traceable system to ensure that staff is following back-up schedules and procedures. With respect to Section C, ITD is creating templates for departmental data owners to identify their disaster recovery/business continuity planning requirements which will drive a more formal IT process.

***Recommendation #8: ITD take the lead to develop (and test) a Disaster Data Recovery Plan and ensure that end-user business needs are included in the final plan.***

**ITD Response to Recommendation #8:** ITD agrees that it could take the lead in developing a Disaster Recovery Plan. However, technology is only a tool in disaster recovery planning efforts that support business objectives, downtime and data loss. Business processes such as legal requirements, retention periods, recovery point objectives, and recovery time objectives must all be defined by the business owners for each system. ITD will take the lead in the design and/or redesign of the technology in support of those key business objectives. It should also be noted that disaster recovery infrastructure, planning and execution will likely require substantial resources to execute as this type of planning effort should have occurred during the initial acquisition and implementation phases of each system.

In order for ITD to begin development of a Citywide Disaster Recovery Plan, the CIO will advise the City Manager to direct each department to take responsibility for the first phase of disaster recovery. Examples of the information each department will be required to provide includes:

- Identifying critical systems
- Identifying functionality and workflows within the system in support of critical operations
- Developing thresholds for recovery point objectives (how much data can be lost between backups) and recovery time objectives (how much time can elapse between the beginning of a system outage and the critical threshold for continuity of operations)
- Identifying manual transactions that will occur during a potential outage
- Reconciling manual transactions once the system returns to operation
- Testing critical workflows/functionality once system recovery is achieved
- Reconciling retention schedules for data being backed up.

Once these factors are identified, ITD can design or redesign systems in support of disaster recovery objectives.

***Recommendation #9: ITD should collect, maintain and periodically update a central inventory of computer equipment and software, and should use its inventory management system and records of technology purchases to: a) better evaluate purchasing needs, b) identify opportunities to redistribute and/or share equipment and software, and c) to the extent possible, ITD should pursue opportunities to centrally-install packages, rather than installing packages at individual workstations.***

**ITD Response to Recommendation #9:** ITD is in partial agreement with this recommendation. With reference to Section A, evaluation of costly technology purchases, standards and economies of scale are already addressed through the current technology approval process. Whenever funding is available for equipment replacement, the current asset management system will allow ITD to create a prioritized list for planning purposes. Producing the list on an ongoing basis, with the exception of budgetary planning, would only represent a snapshot in time of infrastructure backlog without actionable recourse. Section B addresses opportunities to redistribute and/or share equipment. With the relatively low cost of assets and a variety of funding sources to track, the redistribution of assets becomes too costly from a labor perspective. For example, a new PC is currently \$456 and redistributing devalued older equipment would not be advantageous. However, ITD will develop guidelines for surplus versus re-use (e.g. spares, loaners, test equipment, etc.) to be included in the policy for decommissioning and surplus of computer equipment. ITD is in agreement with Section C and is currently pursuing software centralization and subscriptions as a way to manage expansion and contraction of the user base.

***Recommendation #10: Because computer equipment may contain personal identifiable information and other sensitive information, ITD should develop, distribute, and implement a***

***Citywide policy for decommissioning computer equipment, and include it in the citywide surplus inventory policy.***

**ITD Response to Recommendation #10:** ITD is in agreement with this recommendation and will work with the City Administration to develop a Citywide policy for decommissioning and surplus of computer equipment. The picture provided in the Auditor's Report was taken from a special-funded department and demonstrates the differing practices among departments in the retention and re-use of IT equipment.

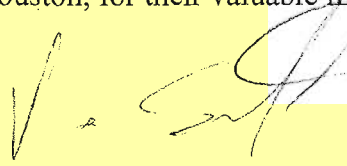
***Recommendation #11: Review the life expectancies of critical computer systems and determine a replacement schedule and budget for the highest-priority systems and hardware.***

**ITD Response to Recommendation #11:** ITD is in agreement with this recommendation. Although funding is not currently available, the department will review the life expectancy of current systems and provide a replacement schedule and budget to the City Administration.

## **CONCLUSION**

ITD has already begun remediation efforts for many of the recommendations outlined in the Auditor's Report as the issues became evident through the iterative audit process. In some cases, there are immediate corrections that may be made. In others, it may require a re-evaluation of current processes and investment in technology to reduce the complexity of the environment, reliance on manual intervention by staff, and minimize the City's IT security risk profile.

The Information Technology Department would like to thank the City Auditor and staff, specifically Gitanjali Mandrekar and Michael Houston, for their valuable insight and recommendations to improve IT controls.



Vijay Sammeta  
Acting Chief Information Officer

For questions, please contact VIJAY SAMMETA, ACTING CIO at 535-3566.