

Fort Worth



1964 • 1993 • 2011

Mayor

Betsy Price

Council Members

Sal Espino, District 2

W. B. Zimmerman, District 3

Danny Scarth, District 4

Gyna Bivens, District 5

Jungus Jordan, District 6

Dennis Shingleton, District 7

Kelly Allen Gray, District 8

Ann Zadeh, District 9

Software License Compliance Audit

October 24, 2014



**City of Fort Worth
Department of Internal Audit**

1000 Throckmorton Street
Fort Worth, Texas 76102

Audit Staff

Patrice Randle, City Auditor

Terry Holderman, Assistant City Auditor

Carol Dickey, IT Auditor



The Software License Compliance Audit was included in the Department of Internal Audit's Fiscal Year 2014 Annual Audit Plan, as a carryover from the prior year.

Audit Objectives

The objectives of this audit were to determine whether:

- controls are in place to prevent software licensing infractions;
- employees are in compliance with the City's Copyrighted Software Policy; and,
- personally-owned software installed on City IT assets was properly approved and documented.

Audit Scope

Our audit covered the period July 1, 2012 through June 30, 2013

Opportunities for Improvement

Conduct routine software license procurement audits for City departments

Update policies and procedures

Incorporate on-going employee training and awareness

Apply software updates to the IT asset management system

Executive Summary

As a carryover from the FY2013 Annual Audit Plan, the Department of Internal Audit conducted a Software License Compliance Audit. Our audit covered the period from July 1, 2012 through June 30, 2013.

Based on the work performed, we concluded that continuous monitoring has been established in the Information Technology Solutions (ITS) Department to prevent software licensing infractions. In addition, we determined that ITS is consistent with removing unauthorized copies of downloaded software from city-issued personal computers.

The City of Fort Worth has licensing agreements with enterprise software vendors such as Microsoft, Adobe and McAfee which require annual software license audits. Based on the results of these audits, vendors will notify ITS if additional license purchases are needed to comply with license agreements.

The Department of Internal Audit concluded that the City of Fort Worth's Administrative Regulation (AR) D-6, Copyrighted Software Policy, was established in 2000 with a review date scheduled in 2005. However, as of this audit, no review had been conducted.

According to City policy, personally-owned software is discouraged for City business, and approval (with justification) must be submitted in writing by department management. However, ITS does not have a process in place to maintain records of personally-owned software installed on City computers, and the current policy is inconsistent regarding what is and what is not allowed.

These findings are discussed in further detail within the [Detailed Audit Findings](#) section of this report.

We feel that management's implementation of its planned course of action (as noted in this report) will adequately address the audit recommendations made within this report.



Table of Contents

Background.....	1
Objectives	3
Scope.....	3
Methodology	3
Audit Results.....	4
Overall Evaluation	4
Detailed Audit Findings.....	5
Acknowledgements.....	10



Background

It is the responsibility of each City of Fort Worth (CFW) employee to ensure commercial software acquired by the CFW is used in accordance with software licensing agreements. ITS is responsible for keeping a record of software licenses purchased through the City's procurement process.

CFW Administrative Regulation D-6, Copyrighted Software Policy, is a city-wide regulation and set of procedures regarding the use and reproduction of copyrighted computer software. The policy establishes responsibility for administering procedures pertaining to the procurement process and installation of copyrighted computer software on city-owned or city-operated equipment.

During the planning phase of the audit, the Department of Internal Audit researched several software alliance groups to gain an understanding of software license compliance. One prominent advocate alliance group, Business Software Alliance (BSA), established a mission to stop software piracy and educate computer users about software copyright laws. The CFW uses software applications developed by well-known software companies (such as Microsoft, Adobe, McAfee and Oracle) who are members of the BSA global advocacy team.

BSA considers a software licensing infraction as the copying, distribution, or downloading of unauthorized copies of software. According to BSA's article "Don't Risk Your Business"¹ specific examples of copyrighted software infractions include the following:

- **Unlicensed Software** – Any software product that has been installed on a personal computer when the license agreement does not allow or support that installation or a license agreement has not been established with the copyright owner
- **Under-licensed Software** – Software that has been installed on more personal computers than the license agreement allows. For example, if the license allows for installation on 20 personal computers but the software has been installed on 30 personal computers, this is considered an under-licensed infraction.
- **Miss-licensed Software** – Software being used for purposes not permitted under the license agreement. For example, software licensed for academic use but used for commercial purposes represents a miss-licensed infraction.
- **Pirated Software** – Software that has been deliberately copied on a significant scale to defraud the copyright owners through illegal distribution, either by using CDs or Internet download sites

Copyrighted software infractions can result in both civil and criminal penalties on individuals and organizations. In 2012, an owner of rogue websites was found to be illegally selling software that was stolen from BSA companies Adobe and Microsoft which resulted in 57 months

¹ Source: Business Software Alliance. Web. October 1, 2013



in prison and was ordered to pay \$400,000 in restitution.² In 2013, CityNet of West Virginia agreed to pay \$106,000 to settle claims of unlicensed software use.³ In October 2013, an article published in TCU360 (Texas Christian University student newspaper) reported student copyright infringement cases were down by 88 cases, while emphasizing copyright law very heavily favors copyright holders.⁴

² Source: Business Software Alliance. Web. February 29, 2012

³ Source: Business Software Alliance. Web. May 31, 2013

⁴ Source: TCU360. Web. October 23, 2013



Objectives

The objectives of this audit were to determine whether:

- controls are in place to prevent software licensing infractions;
- employees are in compliance with the City's Copyrighted Software Policy; and,
- personally-owned software installed on City IT assets was properly approved and documented.

Scope

Our audit scope covered the period July 1, 2012 through June 20, 2013.

There was an audit scope limitation in that the Department of Internal Audit could not determine whether procured software is used in accordance with software license agreements. IT software assets are tracked in the asset management system. However, during partial software audits conducted by ITS, random software assets disappeared from the asset listing report for unknown reasons. Although ITS has informed the vendor, the vendor (FrontRange) has not been able to duplicate the error. In addition, the Department of Internal Audit did not analyze software maintenance costs associated with software licenses.

Methodology

To achieve the audit objectives, the Department of Internal Audit performed the following steps:

- Reviewed CFW Administration Regulations
 - Copyrighted Software Policy (AR D-6)
 - Information Technology Security (AR D-5)
 - Information Technology Electronic Communications Resources Use (AR D-7)
 - CFW Financial Management Policies, Directives, Practices and Procedures (AR C-12)
- Interviewed ITS personnel
- Determined primary functionality of IT Asset Management Discovery software
- Reviewed ITS' enterprise and departmental software audit results
- Reviewed purchase orders supporting software purchased by the CFW through ITS



Audit Results

The Department of Internal Audit concluded that ITS conducts annual enterprise software audits to ensure software license compliance, and has an action plan in place to remove illegal software from City IT assets.

City departments have the responsibility of maintaining records of personally-owned software installed on CFW IT assets. Since the personally-owned software is not purchased through the CFW’s procurement process, ITS does not keep an inventory or records of such software and has no way of knowing if departments are in compliance. However, the City’s asset management system (ITAM Discovery) is used to scan personal computers and has the capability of detecting software that was or was not procured through the ITS process. An established schedule for departmental software audits does not exist. Instead, specific departmental software audits are performed by adhoc request or if unusual internet activity is detected on the CFW network.

The City’s policy for “Copyrighted Software” is eight years overdue for a review, which could result in City employees not understanding the risks that could implicate them and/or the City. Also, the current policy is inconsistent regarding what is and what is not allowed. For example, section 6.1 stipulates only commercial software that has been purchased through the City procurement process should be allowed on CFW IT assets. However, within section 6.10, personally-owned software is discouraged, but can be installed if there is business need for it.

ITAM/Discovery was purchased by the CFW to track IT hardware and software assets. During this audit, ITS staff indicated that ITAM/Discovery sporadically and systematically removes software assets from reports, but self-corrects during the next full audit scan of personal computers. ITS has reported the problem to the software developer and the vendor’s recommendation is for the CFW to upgrade ITAM/Discovery to the latest software version. The CFW is currently running on version 9.2. Version 9.4 is the vendor’s most current version.

Overall Evaluation

High	Medium	Low
	No established schedule for departmental-procured software license audits	
	Outdated policies	
		Asset management system not current on software maintenance



Detailed Audit Findings

1. There is no established schedule for departmental procured software license audits.

An established schedule for departmental-procured software license audits does not exist. Instead, software audits for departments are typically performed when the department requests an audit or when ITS detects unusual internet activity of software downloads.

ITS uses a software product called ITAM/Discovery to track CFW IT assets. When a software audit is initiated, Discovery is capable of scanning personal computer hard drives and reporting on software installed on the computers. The scan results are then reviewed by ITS staff. If software license infractions are found, ITS contacts department management and either removes the software or requires the department to purchase additional licenses.

According to section 6.4 of Administration Regulation D-6, on at least an annual basis, an inventory of all software on each individual PC will be audited against the organization's license agreement records to ensure that no illegal copies of commercial software are installed on any equipment. The Regulation further states that any illegal copies of software discovered in the audit will be deleted from the computer system only after disciplinary action has been taken by the affected Department Director.

Without scheduled software audits for city-wide departments, the risk of using unauthorized copies of software products could result in both civil and criminal penalties against the City and/or employees.

Recommendation 1A:

The Director of Information Technology Solutions should incorporate a formal schedule to perform departmental software audits on City computers to ensure compliance with software license agreements.

Auditee's Response:

Concur. Expanding the current software audits being done to include the department-procured software would strengthen City processes. A schedule and process will be developed after the policy and procedures update is complete and will reflect new technology/software upgrades and capabilities.

Target Implementation Date: June 1, 2015

Responsibility: Assistant Director - Services



Recommendation 1B:

The Director of Information Technology Solutions should develop a continuous monitoring report in the ITAM/Discovery system to 1) report software license infractions; 2) communicate infractions (in writing) to department management; and 3) conduct routine follow up audits to ensure repeated offenses have not occurred.

Auditee's Response:

Concur. By leveraging automation and moving to continuous monitoring, there will be less need for scheduled audits. This will require significant resources in that it will require a software upgrade as well as implementation of a new module: License Manager and new procedures such as entering software contracts into the system to make continuous monitoring an achievable goal.

Target Implementation Date: December 1, 2015

Responsibility: Assistant Director – Services

2. CFW policies and procedures governing software license compliance are outdated.

Administration Regulation D-6, Copyrighted Software Policy, was established on June 15, 2000. The next review date was scheduled for June 15, 2005. However, as of audit fieldwork, the policy had not been updated. As a result, City employees may not understand the risks that could implicate them and/or the City.

Information technology devices are constantly changing. As a result, employees are more equipped with mobile devices to work from home or from remote locations. Additionally, with the constant change of technology, employees have easier access to the internet which increases the opportunity for software infractions.

Written policies and procedures provide instruction to help ensure that employees are aware of company practices, and ensure that each employee's application of the policy is consistent. Well-defined, updated policies that are scheduled for regular review allow employees to become more aware of U.S. Copyright law, and reduce the risk of software licensing infractions and virus or hacker attempts on the CFW network.

Recommendation 2A:

The Information Technology Solutions Director should update the City's Copyrighted Software Policy to include new policy directives for software licensing and usage on city-owned computers. The updated policies should address new devices such as mobile tablets or smart phones with specific guidelines on downloading software from the internet or from other media devices outside of the CFW network.



Auditee's Response:

Concur.

Target Implementation Date: December 1, 2015

Responsibility: Assistant Director – Operations

Recommendation 2B:

The Information Technology Solutions Director, in conjunction with the Chief Financial Officer, should consider requiring city-procured software be coded to specific account numbers and the software procurements be systematically routed to ITS for approval.

Auditee's Response:

Concur. Current processes such as the M&C [Mayor and Council] process requiring ITS approval as well as increased levels of security and permissions required for software installation ensure IT Solutions is aware of software purchases in most cases. IT Solutions Director will meet with Chief Financial Officer to consider ways to ensure IT Solutions is aware of software purchases.

Target Implementation Date: January 15, 2015

Responsibility: IT Solutions Director

Recommendation 2C:

The Information Technology Solutions Director should incorporate regular training sessions designed to educate employees on the Copyrighted Software Policy and possible penalties associated with using unlicensed copies of software on city computers. Written acknowledgement that the employee has read and understood the policy after completing the training class should be required. The signed acknowledgement should be filed in the employee's HR file.

Auditee's Response:

Concur with expanding existing training to include education regarding copyrighted software. Will consider written acknowledgement recommendation.

Target Implementation Date: July 1, 2015

Responsibility: Assistant Director - Operations



Recommendation 2D:

The Information Technology Solutions Director should design a communications plan to periodically inform City employees of the Copyrighted Software Policy (along with other information technology policies) via means such as new employee orientation, publications in The RoundUp, department director group emails, reminders printed on paychecks, etc.

Auditee's Response:

Concur. Currently IT Solutions routinely and regularly communicates plans, security information, and other technology updates through a variety of mechanisms including new employee orientation, The RoundUp, presentations for example at: Council, Department Heads, and Quarterly Manager Meetings, Annual Business Plan, IT Strategy, Technology Users' Group, targeted emails, etc. A more structured communications plan could strengthen communications by identifying specific areas to target.

Target Implementation Date: January 15, 2015

Responsibility: IT Solutions Director

3. IT Asset Management/Discovery is not current on software maintenance.

ITS implemented ITAM/Discovery to track hardware and software inventory. During the course of this audit, the Department of Internal Audit determined that ITAM/Discovery is not current on software maintenance.

ITS staff indicated that when partial audit scans on personal computers are performed using ITAM/Discovery system, some software records disappear from the report. The problem resolves itself during the next full audit scan and software records reappear. The vendor, FrontRange, has not been able to duplicate the problem and has recommended a software upgrade. The CFW is currently on version 9.2 of ITAM/Discovery software. However, version 9.4 is the vendor's most current version.

Timely upgrades and software patches help ensure optimal system performance and help ensure compliance with the terms and conditions of the software agreement. An advantage of upgrading software is to fix software "bugs." In addition, running an outdated system may cause the CFW to be out of compliance with maintenance and support agreements.

Section 2 (c) of the terms and conditions of FrontRange maintenance and support stipulate that "Support is available for the current and immediately preceding version of the Licensed Software and for any version released within eighteen months of the date of the Support request, provided that Customer and FrontRange are parties to a current M&S agreement."



Recommendation 3:

The Information Technology Solutions Director should oversee the upgrade of ITAM/Discovery to the latest version and/or apply software patches in a timely manner.

Auditee's Response:

Concur and will include implementation of License Manager.

Target Implementation Date: December 1, 2015

Responsibility: Assistant Director - Services



Acknowledgements

The Department of Internal Audit would like to thank the Information Technology Solutions Department for their cooperation and assistance during this audit.