



OFFICE OF THE COMPTROLLER
CITY OF ST. LOUIS



DARLENE GREEN
Comptroller

Internal Audit Section

1520 Market St., Suite 3005
St. Louis, Missouri 63103-2630
(314) 657-3490
Fax: (314) 552-7670

DR. KENNETH M. STONE, CPA, CGMA
Internal Audit Executive

FILE COPY

January 27, 2014

Dele Oredugba, Director
Information Technology Services Agency
City of St. Louis
City Hall
1200 Market Street, Room 100
St. Louis, MO 63103

RE: Process Review of Information Technology Services Agency - Software License Management (Project #2013-P13)

Dear Mr. Oredugba:

Enclosed is the Internal Audit Section's process review report of the Information Technology Services Agency - Software License Management as of March 31, 2013. A description of the scope of work is included in the report.

Fieldwork was completed on June 24, 2013. Management's responses to the observations and recommendations noted in the report were received on December 31, 2013, and have been incorporated into the report.

This review was made under authorization contained in Section 2, Article XV of the Charter, City of St. Louis, as revised, and has been conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

If you have any questions, please contact the Internal Audit Section at (314) 657-3490.

Respectfully,

Dr. Kenneth M. Stone, CPA, CGMA
Internal Audit Executive

Enclosure

Cc: Keith Moore, Network Systems Manager
Robbyn Wahby, Executive Assistant to the Mayor, Mayor's Office
John Zakibe, Deputy Comptroller, Comptroller's Office



CITY OF ST. LOUIS

INFORMATION TECHNOLOGY SERVICES AGENCY (ITSA)

SOFTWARE LICENSE MANAGEMENT

PROCESS REVIEW

AS OF MARCH 31, 2013

PROJECT #2013-P13

DATE ISSUED: JANUARY 29, 2014

**Prepared By:
The Internal Audit Section**



OFFICE OF THE COMPTROLLER

HONORABLE DARLENE GREEN, COMPTROLLER

**CITY OF ST. LOUIS
INFORMATION TECHNOLOGY SERVICES AGENCY (ITSA)
SOFTWARE LICENSE MANAGEMENT
PROCESS REVIEW
AS OF MARCH 31, 2013**

EXECUTIVE SUMMARY

Background

The Information Technology Services Agency's (ITSA) mission is to provide mainframe and personal computer network support and programming along with web development and maintenance.

ITSA creates, maintains, and improves enterprise-wide, integrated information technologies serving employees, businesses and residents who can access relevant government services with an emphasis on customer service.

ITSA's management of software licenses is limited to software it directly purchases and installs on the city computer systems and includes ensuring compliance with software agreements terms and conditions.

Purpose

ITSA's software license management was selected for review based on the Internal Audit Section's annual risk assessment. The purpose was to determine if ITSA's internal controls over software license management effectively and efficiently manage risks to ensure:

- Accomplishment of established objectives and goals.
- Compliance with applicable laws, regulations, policies, and procedures.
- Safeguarding of assets.
- Reliability and integrity of operational information.

Scope and Methodology

The review was confined to evaluating internal controls over ITSA's software license management including acquiring software, installing, licensing, and monitoring them. This review does not include software independently acquired and installed by city departments and other city agencies. The review procedures included:

- Inquiries of management and staff.
- Observations of relevant processes.
- Reviews for compliance with software license agreements terms and conditions.
- Limited tests of controls.

- Other procedures as considered necessary.

Exit Conference

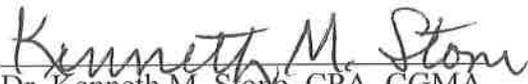
An exit conference was conducted at the ITSA conference room, on October 2, 2013. The department was represented by the Network Systems Manager. The Internal Audit Supervisor and the Auditor-in-Charge represented the Internal Audit Section.

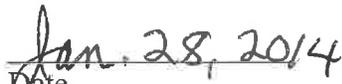
Conclusion

ITSA adequately addressed internal controls and risks related to software license management, except for the following observations:

1. Opportunity to centralize software purchases and license monitoring.
2. Opportunity to develop policy and procedures on software management.
3. Opportunity to improve internal controls over software installation and downloading.

These observations are discussed in more detail in the *Detailed Observations, Recommendations and Management's Responses* section of this report.


Dr. Kenneth M. Stone, CPA, CGMA
Internal Audit Executive


Date

**CITY OF ST. LOUIS
INFORMATION TECHNOLOGY SERVICES AGENCY (ITSA)
SOFTWARE LICENSE MANAGEMENT
PROCESS REVIEW
AS OF MARCH 31, 2013**

TABLE OF CONTENTS

Description	Page(s)
OBSERVATIONS	
Status of Prior Observations	1
Summary of Current Observations	1
DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT'S RESPONSES	2-4

OBSERVATIONS

Status of Prior Observations

The Internal Audit Section (IAS) has not performed a process review of Information Technology Services Agency (ITSA) -Software License Management recently. The last report pertaining to this area was dated January 30, 2002.

Summary of Current Observations

ITSA adequately addressed internal controls and risks relating to software license management, except for the following observations:

1. Opportunity to centralize software purchases and license monitoring.
2. Opportunity to develop policy and procedures on software management.
3. Opportunity to improve internal controls over software installation and downloading.

These observations are discussed in more detail in the *Detailed Observations, Recommendations and Management's Responses* section of this report.

DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANGEMENT'S RESPONSES

1. Opportunity To Centralize Software Purchases And License Monitoring

The purchase of computer software by the City is not centralized. ITSA purchases and manages software for mainframe, web development, network support, and computer software used city-wide. However, City departments may acquire software that is unique to them, without coordinating the purchase or software license management with ITSA. In addition, departments do not inform ITSA if they are complying with the licensing requirements for the acquired software. Consequently, ITSA has no oversight over the licensing requirements of the software purchased by the City departments.

Software is protected by copyright laws written to protect the author's work product. When commercial software is purchased, the underlying software code is not purchased, only the right to use it in accordance with the software license. Under federal law in the United States, each software license violation carries a potential fine of up to \$150,000 per software title copied illegally.

Centralized control over software purchases and license management assists in ensuring that software is properly installed and is compatible with current City hardware, software and operating systems. In addition, centralized software management assists in ensuring that the software is legally licensed for the intended use and for the proper number of users. Properly licensed software protects the City from potential fines for non-compliance with the licensing requirements.

Recommendation

It is recommended that ITSA work with the Board of Estimate & Apportionment to:

1. Define, implement and communicate to all department heads a City-wide software purchase and software license management policy. The policy should require ITSA to:
 - a) Approve, install and support all City software.
 - b) Maintain a complete list of all installed software and related license requirements.
 - c) Maintain and manage all software licenses
2. Perform regular checks comparing licenses to installed software to ensure compliance.
3. Monitor and remove obsolete and unlicensed software from City computers using automatic tools.
4. Conduct an annual inventory of software licenses with respective usage to comply with licensing requirements.

1. Continued...

Management's Response

While we agree completely with the concept and benefits of a centralized and manageable software licensing system for the entire City, and will work hard to make it happen, there are several political aspects and layer of management, outside the control of ITSA that are integral to a successful implementation.

2. Opportunity To Develop Policy And Procedures On Software Management

ITSA has not developed a citywide policy and procedures on software purchase, installation, and licensing by the City departments (software management).

A citywide written policies and procedures on software management will ensure that:

1. Software purchases and licensing by City departments are centralized.
2. Policy and procedures are communicated to all City departments.
3. City employees and departments are in compliance with the centralized software management policy.
4. Department heads and employees are aware of the consequences of not complying with the software management policy.
5. City departments are in consultation with ITSA prior to acquiring software.

The consideration to develop and implement a centralized software management policy for citywide use has not gained universal acceptance.

Lack of an approved centralized standard written software management policy and procedures may result in software being used without adequate licensing. This may expose the City open to lawsuits and fines.

Recommendation

It is recommended that ITSA's management develop and implement a citywide standard software management policies and procedures. Such policies and procedures:

1. Should be approved by the appointing authority and dated.
2. Formally communicated to all City employees and require written acknowledgement of employees and supervisors; similar to the requirement for acknowledging the City's ethical code.
3. Reviewed and updated periodically
4. Centralize acquisition, installation and licensing of software by ITSA.
5. Require disciplinary action for violation and non-compliance with them.

Management's Response

We agree there is a need for policies and procedures regarding software management and will actively work to develop those.

3. Opportunity To Improve Internal Controls Over Software Downloads and Installations

ITSA has not fully implemented a system of internal controls that would prevent employees from downloading and installing unauthorized software programs on their computers. ITSA has installed a software program that would prevent such installations and downloads, however, it requires additional configuration to be fully operational.

A sound information technology system should have internal controls in place that would not only detect but prevent downloads and installations of unauthorized software programs.

Unauthorized software programs may not be supported by ITSA and may:

1. Contain spyware capable of capturing confidential information.
2. Expose the City's system to viruses that will spread not only to other computers but infect the citywide computer system.
3. Conflict with the existing applications or change crucial configuration information.
4. Conflict with the currently installed software that may cause the computer and /or the City's systems to crash.
5. Subject the City to potential penalties for non-compliance with software license requirements.

Recommendation

It is recommended that ITSA perform the additional configurations to the make the installed software program operational to prevent unauthorized software downloads and installations.

Management's Response

While the statement that ITSA has installed a software program to prevent unauthorized installations and downloads is not entirely accurate, the intent and essence of this item are correct. The technologies involved in this area consist of a variety of systems. However, it is correct to say that ITSA has been working toward this goal and that we agree it is of high importance. It should be noted, however, that ITSA does not have the central authority necessary to prohibit and/or limit administrative access to all computers in the City. Also, a number of computer systems exist entirely outside the control of ITSA and are not administered by us at all.