SOFTWARE LICENSE AUDIT

June 27, 2019
Audit No. AUD17-05

City of West Palm Beach
Internal Auditor's Office

Beverly Mahaso, Chief Internal Auditor, Esq., CIA, CFE
Focal Point, Contract Auditors

INTENTIONALLY LEFT BLANK

Executive Summary

SOFTWARE LICENSE AUDIT - AUD17-05

JUNE 27, 2019

WEST PALM BEACH
Internal Audit

OVERVIEW

- The City's Information Technology Department is responsible for managing all City software and safeguarding networks against malicious attacks.
- Prior to 2017, each operating area within City government had the ability to purchase and install its own software.
- Currently, each Department is required to obtain ITs' approval prior to making a software/maintenance purchase, although the budgetary approval resides with each department.
- IT uses an asset management and network inventory software, LanSweeper, to identify both hardware and software on the City's network.

SUMMARY FINDINGS

1. **Licensed Software:** Business Applications may have been installed to a greater extent than permitted by licensing agreements.
2. **Non-business Use Software and Applications:** During testing and analysis, various non-standard applications appear to have been installed on City computers, including malware.
3. **Safeguarding Assets:** Through data analytics, we determined that there were 1,548 out of 2,905 devices in the Servers and Workstations data that were not seen in the prior 7 days.
4. **Inventories:** At the present time, there are no single source inventory records for both hardware and software.
5. **Software Purchase and Installation:** Departments have the ability to purchase and install software on workstations, with access to the City's network, with little or no oversight.

SUMMARY RECOMMENDATIONS

1. Controls over software installation and licensing should be improved primarily by working with the Administration and Procurement to ensure consistent compliance with the City's Technology Use Policy. Further, controls should be implemented to ensure that the City does not exceed the maximum number of users for each proprietary software product purchased.
2. The IT Department should implement and enforce controls that permit software installations only by members of ITs Support team.
3. The IT Department should take steps to implement a basic system of inventory controls, for device purchase, receipt, assignment to employees, return to inventory and disposal.
4. The IT Department should create comprehensive, timely and standard reports for both software and hardware, including standard naming conventions. In addition, an IT employee should be designated as the inventory management custodian.
5. IT should work with Administration to update the software policy to assign centralized accountability for software purchases and installation to the IT department only, which should be the sole party with administrator rights for software installation.

INTENTIONALLY LEFT BLANK

Internal Auditor's Office
P.O. Box 3366
West Palm Beach, Florida 33402
Tel: 561-822-1380
Fax: 561-822-1424

June 27, 2019

Audit Committee
City of West Palm Beach
401 Clematis Street
West Palm Beach, Florida

RE: Software License Audit, AUD17-05

Dear Audit Committee Members:

Attached is the City of West Palm Beach's Internal Auditor's Office report on the Software License audit.

We thank the management and staff of the Information Technology Department for their time, information, and cooperation during this audit.

Respectfully Submitted,

/s/ Beverly Mahaso
Chief Internal Auditor

cc: Keith James, Mayor
Jeff Green, City Administrator
Nathan Kerr, Chief Technology Officer

INTENTIONALLY LEFT BLANK

Contents

Background

The City of West Palm Beach utilizes software from a wide variety of providers for its operating units. The software may be installed on servers, workstations, laptops, and tablets. The Information Technology Department (IT) is responsible, as defined in City policy, for managing all software that is used by the City and safeguarding the City's IT network against malicious attacks. The origination of cyber-attacks varies to include attacks launched through software. Thus, the need for the City to protect itself against cyber-attacks is essential. As of June 2019, at least 24 municipalities, most recently Baltimore and Riviera Beach, have reported various cyber-attacks just this calendar year alone. Some of these municipalities took weeks or months to recover full operations, while others paid ransoms.

Prior to 2017, each operating area within the City had the ability to purchase and install their own software. Currently, each department is required to obtain IT's approval prior to purchase, although the budget for the software purchase/maintenance resides with each individual department. To ensure compliance with licensing agreements and to ensure that all software installs are effectively in use, IT utilizes an asset management and network inventory software, LanSweeper, to identify both hardware and software on the City's network. LanSweeper also retrieves and stores software licensing information. Devices and the associated software will not be detected unless they are connected to the City's network. At one point, software information including licensing information was manually entered into LanSweeper because as noted above, departments were independently purchasing and installing software without IT's knowledge or oversight. This practice created information gaps and discrepancies that are discussed in the findings.

Statement of Scope

The scope of the audit was the entire population of software that is on City devices.

Statement of Objectives

The objectives of this audit were to determine whether:

1) All software was installed in accordance with the terms of the licensing agreements with regard to the permitted number of installs,

2) Identify any unused licenses, and

3) Additional objectives were added during the analysis as significant discrepancies in software, assets, and data were identified as follows:

    a. Assess the scope of the discrepancies;

b. Identify potential security weaknesses resulting from prior software purchase and installation practices.

Statement of Methodology

We utilized data analytics as well as other audit techniques to achieve the objectives. These evidence-gathering techniques included, but were not limited to:

- Interviewing IT employees,
- Process walk-throughs, and
- Tabulating and comparing software in use across multiple data sources.

The following are examples of work steps performed:

- Identify assets in the Software License Keys list that are not in the Servers/Workstations lists;
- Identify assets in the Servers/Workstations lists that are not in the "Last Seen" report;
- Compare the number of installs in the CWPB Asset Inventory and the List of Software by IP address*.
- Compare the number of installs in the Software License Keys and the List of Software by IP address**.

Software Name Harmonization
During the preliminary review of the data, inconsistent naming conventions were found. Thus, where indicated by * or **, software names were harmonized and were "fuzzy matched" to enhance comparison effectiveness.

Excluded Applications
To reduce false positives, Internet Explorer, volume licenses, and enterprise licenses were excluded from the results.

Statement of Auditing Standards

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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.

Audit Conclusions and Summary of Findings

1. **Software**- Lists and totals of installed software did not always match:
    a. Software in one list did not appear in another;

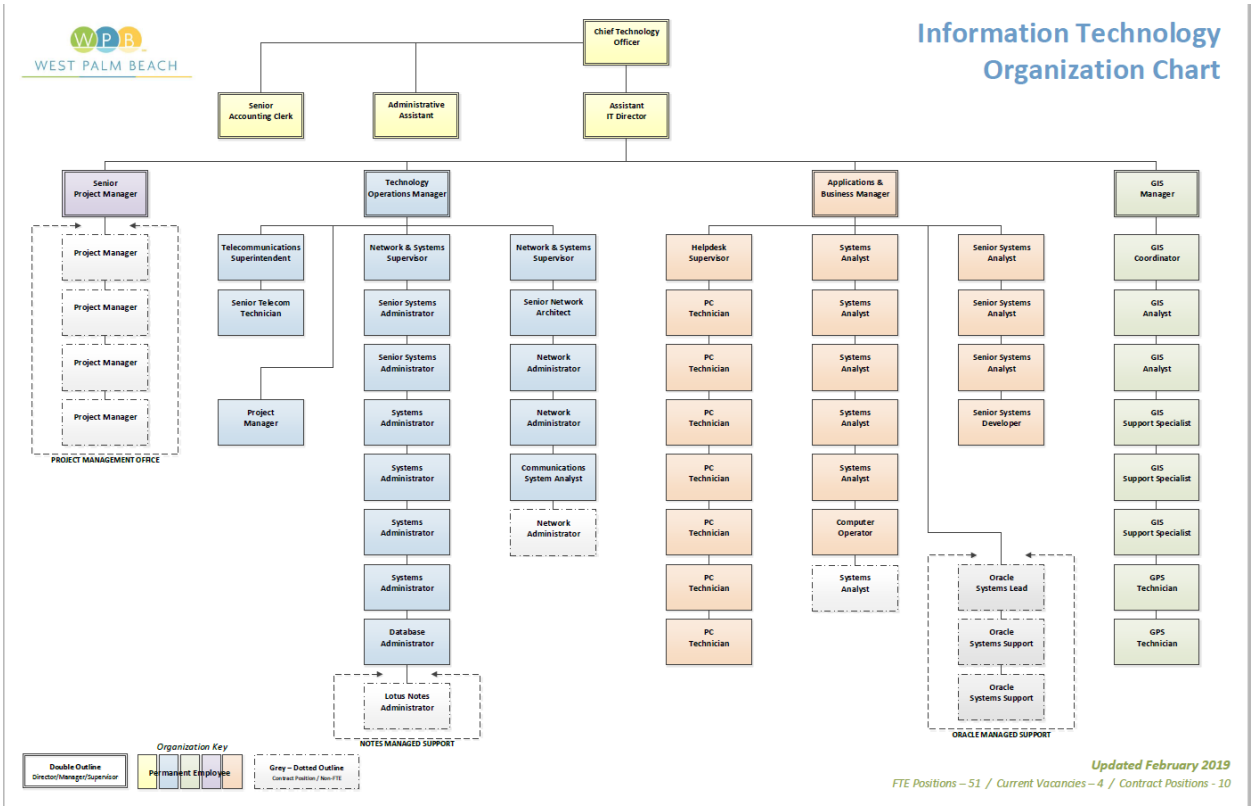
b. Total number of installs was not consistent from one list to another.

2. **Computer Assets**- Lists of computer assets did not always match:
    a. Computers (servers and workstations) in one list did not appear in another.
3. **Potential Workstation Vulnerability**- Historically, departments had great latitude in determining which software to purchase and install on their workstations. This can lead to:
    a. Installation of malware and other questionable applications;
    b. Inconsistent and weak security standards; and
    c. Violations of licensing agreements.

Noteworthy Accomplishments

We acknowledge IT's efforts to manage software and licensing. Considering that prior to 2017, there was no policy to prevent departments from purchasing and installing software, IT has implemented a process whereby they scan City devices periodically to identify software and licenses. Further, IT also scans individual machines when installing new software. Finally, we commend IT for proactively taking corrective action as findings were identified.

IT Organization Chart



Opportunities for Improvement

1. Licensed Software

Condition

Our review determined that business applications may have been installed to a greater extent than permitted by license agreements. We performed data analytics to match installed software applications extracted with LanSweeper to the permitted number of licenses in the Software License Key file provided by IT. Deficiencies in the data files included blank department names and/or IP addresses, unmatched application names, errors and/or omissions. Consequently, there were several gaps in the data results when we attempted to match applications.

In addition, it appears that both the Software License Key File and the data file of installed software may not have been fully updated due to purchases made without IT guidance. In an effort to better understand the data results, we divided software applications into three groups: Adobe, Microsoft and Other, and found the following:

- Of the 1,082 distinct Microsoft applications in the Software License Key file, 949 (88%) were not found in the data file of installed software,
- Of the 418 distinct Adobe applications in the Software License Key file, 330 (79%) were not found in the data file of installed software,
- Of the 24 distinct Other applications in the Software License Key file, 19 (79%) were not found in the data file of installed software, and
- 411 out of 104,740 applications identified by LanSweeper did not have a domain identified.

As a result of these discrepancies, it may be challenging for IT to manage software and ensure that only licensed software is installed on City devices. We acknowledge IT's on-going efforts to address this long-standing situation by sweeping machines for software and licensing information periodically and on an individual basis.

Criteria

Management is responsible for the design of the entity's information system and related control activities to achieve objectives and respond to risks. Business software requires licensing agreements and non-compliance with those agreements could result in significant penalties.

Cause

Prior to the issuance of the City's Technology Use Policy (Policy 1-28) in April 2017, controls governing software purchases and installation were historically weak or non-existent. Therefore, departments and individuals were able to purchase, download, and install software without obtaining IT support or oversight, and IT was not receiving updates about software purchases or installations. Further, manual entries to the system may have contributed to this issue.

Effect

Due to the historically weak controls over software purchases, IT was not able to effectively manage the City's software licenses. As a result, the City may be in violation of license agreements, which could expose the City to financial penalties. In the past, the City has owed money due to unlicensed software. This may be a recurring problem until all software licenses are accounted for through the IT department. In addition to unlicensed users, there may also be licenses that are no longer utilized and should be deactivated, which could reduce costs.

An additional risk is incurred when departments purchase software that does not interface with the City's existing ERP system, and therefore cannot be utilized to its full capability. This could result in additional costs to develop interfaces that may have been avoided if IT had been consulted before committing to a certain product.

Recommendation 1

Controls over software installation and licensing should be improved by:

(1) Working with the Administration and Procurement to ensure compliance with the City's Technology Use policy (Section H5) regarding IT pre-approval of software purchases. This should include advance approvals by the requesting Department Director, prior to submittal to IT for approval;

(2) Implementing controls that will permit software installation only by members of the IT Support team, particularly when a paid license is required;

(3) Scheduling periodic software scans to compare the number of actual installations with valid license agreements;

(4) Ensuring that the software license key is updated on a periodic basis to reflect new and/or deactivated license agreements; and

(5) Implementing controls that will ensure the City does not exceed the maximum number of users for each proprietary software product purchased.

Any exceptions should be determined by IT on a case-by-case basis and supported by a valid business reason.

Management Response 1

We agree with the recommendations. There is already compliance and agreement with Finance and Procurement to route technology related items to IT for approval if the submitter fails to do so. In addition, Local Administrator Rights are now only given to System Administrators within the IT Department, with a few minor exceptions, minimizing the possibility of illegal software being installed. IT is also implementing a software solution that will allow us to have better control on concurrent users for licensed software. This solution also allows for centralized management of software updates and software key updates.

Target Implementation Date: 4th Quarter of 2019 to schedule/plan regular software scans and ensuring local admin rights are available to IT staff only.

2. Non Business Use Software and Applications

Condition

During testing and analysis of software, various non-standard applications were detected on staff computers. Further research indicated that malware and other questionable applications appear to have been installed on some user computers. At least 3 definite malware applications were identified and 4 other applications did not have discernable business benefits. We brought this to the attention of IT, and the new IT management responded quickly to our concerns. There is a risk that there may be additional questionable applications that were not identified because they were outside the scope of this review.

The threat of malware should not be taken lightly. Smaller organizations are at higher risks due to inadequate defensive protection. Over 10 billion malware attacks were detected in 2018. In 2019, a collection of 2.7 billion identity records, consisting of 774 million unique email addresses and 21 million unique passwords, were posted on the web for sale. The average cost of a data breach in the USA will be over $150 million by 2020, with the global annual cost forecasted to be $2.1 trillion.

Criteria

Management is responsible for being vigilant and designing control activities for security management of the information system, including access by internal and external sources. Malware and other unauthorized third-party applications provide avenues for hackers to make unauthorized changes to IT systems, exploit vulnerabilities, or bring down entire IT networks. ISO (International Organization for Standardization) standards discuss controls related to software installation as follows:

- Rules governing the installation of software by users should be established and implemented.
- The organization should define and enforce strict policy on which types of software users may install.
- Networks should be managed and controlled to protect information in systems and applications.
- Detection, prevention, and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Cause

Prior to the issuance of the City's Technology Use Policy (Policy 1-28) in April 2017, controls governing software purchases and/or installation were historically weak or non-existent. Therefore, departments and individuals were able to purchase, download, and install software without obtaining IT support or oversight.

Effect

Based on information from the ISO, "Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity, or other information security incidents or to violations of intellectual property."

Further, serious risks to the City's ability to achieve validity, completeness, accuracy, and confidentiality of transaction processing and secure data storage may be possible. Unauthorized or fraudulent changes from malware could include the creation of false vendor accounts or employee accounts, which could then be leveraged to create false payments, thereby undermining the City's financial stability and security.

Recommendation 2

The IT Department should:

(1) Implement/enforce controls that permit software installation only by members of the IT Support team,

(2) Create a policy that requires departments and individuals to purchase and install software only through the IT Support team,

(3) Require regular software scans to identify malware and other suspicious applications, and

(4) Implement malware detection software throughout the IT environment.

Any exceptions should be determined by IT on a case-by-case basis and supported by a valid business reason.

Management Response 2

We agree with the above recommendations in principle. Local Administrator Rights are now only given to System Administrators within the IT Department, with a few minor exceptions, minimizing the possibility of illegal software being installed. The IT Department has also recently upgraded its security monitoring application, SPAM filter and will be implementing additional security monitoring tools in the next fiscal year.

Target Implementation Date: 4th Quarter of 2019 to schedule/plan regular software scans and formalize the recommended policy.

3. Safeguarding Assets

Condition

The City utilizes many types of computerized devices in its day to day operations, including workstation PCs, laptops, tablets, and telecommunication devices, to list a few. Many of these devices have a fairly short life cycle due to the ever improving level of technology and are upgraded periodically. Our objective was to link the devices listed in the Servers and Workstations dataset with the corresponding assets in the "Last Seen Data File" provided by IT.

Data analytics were used to compare all computer devices in the Servers and Workstations data with the assets in the Last Seen data. We found that at the time of our review, 1,548 devices out of 2,905 devices in the Servers and Workstations data, were not in the Last Seen data (past 7 calendar days).

While we acknowledge that some of these machines are likely used by employees who may be on vacation, are not used frequently, are virtual machines, or some other valid business reason, there remains a significant number of machines that are not, but should be accounted for, particularly when considering that the City has about 1,600 to 1,700 employees. If any hardware is set to be retired then that process should occur and IT should have the related software deactivated to ensure that the City is not paying for software that is not used. It should also be noted that laptops, tablets, and phones were not included in this analysis as they may not consistently connect to the City's network.

Criteria

Management is responsible for establishing physical control to secure and safeguard vulnerable assets. Management should periodically count and compare such assets to control records. There should be a methodology for ensuring that all computer devices are located, users identified, and properly accounted for.

Cause

An offline device may not be identified when device detection sweeps are conducted. Inaccurate or untimely inventories may also be the cause. Further, devices may also have been misplaced, misappropriated, in storage, or otherwise unaccounted for.

Effect

There are several concerns that arise when assets are not properly safeguarded and/or accounted for. For example:

- Proper inventories and asset valuations cannot be made.
- Loss of assets can lead to increased expenses when the devices are replaced.
- Incorrect depreciation expense on the City's financial statements may be recognized.
- The City may also record incorrect asset disposal revenue.

Recommendation 3

The IT department should create and enforce a policy with the associated procedures for the following: (1) device purchases; (2) the receipt of devices in inventory; (3) the transfer of devices to employees; (4) the return of devices from employees to inventory; and (5) the disposal of devices at the end of their useful lives.

Management Response 3

We agree that the above recommendations are best practice. While providing reports for this audit the focus was on a software inventory, not an inventory of devices. The discrepancies found in the provided information may be attributed to the extensive use of a virtual desktop environment, laptops assigned to field workers, staff on vacation and workstations that may have been retired before an asset management system was implemented to track surplus. The IT Department has implemented a new asset management system that will be tracking software and hardware as they are received and retired.

Target Implementation Date: 4th Quarter of 2019 to implement a policy.

4. Inventories

Condition

At present, there are no single-source inventory reports for software and hardware. Different reports provide different items and different counts.

Criteria

Management is responsible for establishing physical control to secure and safeguard vulnerable assets. Management should periodically count and compare such assets to control records. There should be a methodology for ensuring that all computer devices are located, users identified, and properly accounted for. In addition, a register should be maintained of all proprietary software and information assets.

Cause

There is no one party that has overall accountability for the inventory reports with standard naming conventions.

Effect

It is incredibly challenging and cumbersome to determine to a useful degree of certainty whether the City complies with its software licensing agreements.

Recommendation 4

The IT department should:

a) Enforce its policy related to control software maintenance including licensing terms and conditions;

b) Create comprehensive, timely, and standard set of reports for both software and hardware, including standard naming conventions. Where possible, these reports should be automatically generated rather than manually generated to reduce errors; and

c) Designate an IT employee as the inventory management custodian.

Management Response 4

We agree. The IT Department does have an internal policy to control software maintenance and there is a designated staff member that has assumed asset management duties. We agree that reports should be standardized which will be easier to do now that new software and hardware are being entered into our asset management system.

Target Implementation Date: 4th Quarter of 2019 to standardize reporting within LanSweeper and SolarWinds.

5. Software Purchases and Installation

Condition

Departments have the ability to purchase and install software on workstations, with access to the City's network, with little or no oversight.

Criteria

Adequate controls should be in place to ensure that software purchases are in alignment with City and departmental objectives. Further, procedures should be in place to ensure that the City is in compliance with all third-party license requirements and that intellectual property rights and restrictions are respected**.**

Cause

Software installation controls are not centralized or consistent with best practices for ensuring security.

Effect

Without strong controls, possible avenues for the introduction of malware and security weaknesses into the entire City system are created. Further, potential purchasing efficiencies are not realized. In addition, software installations may be incompatible with existing business applications and thus be of limited use over time, leading to less than optimal use.

Recommendation 5

IT should work with Administration to update the software policy to assign centralized accountability for software purchase and installation to the IT department only, which should be the sole party with administrator rights for software installation. Any exceptions should be made on a case-by-case basis with a valid business reason.

Management Response 5

There is already compliance and agreement with Finance and Procurement to route technology related items to IT for approval if the submitter fails to do so. Local Administrator Rights are now only given to System Administrators within the IT Department, with a few minor exceptions, minimizing the possibility of illegal/unknown software being installed.

Target Implementation Date: 4th Quarter of 2019 to formalize official policy as suggested.