Software License Management

Audit Report 201920-16

December 16, 2020

Executive Summary

Software license management is a set of tools and processes that an organization uses to document and manage software licenses to ensure compliance with developers' software license agreements. Managing software licenses provides transparency into the organization's enterprise software assets, usage, and contracts. It enhances understanding of what software is being used, how it is used, where it is used, and by whom. Managing software licenses also ensures legal compliance, lowers audit risks, and reduces the controlling costs associated with software assets. Overall, managing licensed software provides a clear, consolidated view of license software products, needs, and utilization.

The Florida Department of Highway Safety and Motor Vehicles (Department) purchased an estimated $14 million of licensed software from July 2018 through December 2019. The Department manages an estimated 8,000 to 9,000 workstations, 700 tablets and smartphones, and over 1,300 servers between Department headquarters and field offices.

The purpose of this audit was to review and evaluate the efficiency and effectiveness of software license management and compliance with best practices, applicable laws, Department policy, and procedure. Our review included: software purchasing, compliance with license agreements, installation and removal of software, separation or internal transfer of members with assigned licensed software, expirations and renewals, and the monitoring of software license use. Our evaluation determined that while the Department has implemented certain controls to manage software licenses, such as recording purchased software and preventing installation without authorization, controls pertaining to managing software licenses, monitoring license agreement compliance, and reviewing local administrator privileges should be strengthened. Strengthening these key areas would achieve greater efficiency and effectiveness and could mitigate the risks associated with inefficient management of software licenses.

Our review determined enhancing controls for managing software licenses would improve accountability and compliance. We noted the Department does not currently have a process for accurately monitoring the use of software licenses after installation occurs. Desktop Support currently uses a Software Tracking Excel spreadsheet (spreadsheet) for managing software licenses, but because it is manually maintained, software names are often inconsistent, resources are limited, and the accuracy of the spreadsheet cannot be assured. Desktop Support can also use Microsoft's System Center Configuration Manager (SCCM) to aid in monitoring, but SCCM does not have

the capability to identify or scan computers that are not on an active network, and therefore software on these inactive computers could go unmonitored. We recommend ISA management implement a comprehensive enterprise-wide software license inventory program that uses automated discovery and inventory tools and metrics to improve accountability and compliance.

Our review also determined controls should be implemented to improve monitoring of software license agreement compliance. While the Department has processes and controls to record and track the software licenses purchased, issued, and installed, there is currently not an effective system to monitor and verify compliance with software license agreements. The Department determines the number and type of licenses purchased from the invoices and does not currently monitor and verify compliance with the provisions of the software license agreements. We recommend ISA, in coordination with Department divisions, implement an effective system to retain, review, and monitor the Department's compliance with software license agreements.

Further, periodically reviewing members with local administrative access privileges would improve security and accountability. The Department does not have a consistent process for monitoring members who have local administrative access privileges to ensure the list of authorized members remain appropriate. We recommend ISA implement a process to periodically review members with local administrative access privileges to ensure permission levels remain appropriate. We also recommend ISA provide written guidance to management to notify ISA of any position changes of members with local administrative access privileges.

Management concurred with the findings and recommendations and has begun implementing corrective actions.

Background and Introduction

In accordance with Chapter 282.318, Florida Statutes, (F.S.), the Department is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security, to include cybersecurity, and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity and to mitigate risks. Agencies should establish asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

Chapter 60GG-2, Florida Administrative Code, establishes the cybersecurity standards for information technology (IT) resources. State agencies must comply with these standards in the management and operation of state IT resources. The standards for

state agencies include ensuring software platforms and applications within the organization are inventoried and managed and ensuring IT resources, including software, are categorized, prioritized, and documented based on their classification, criticality, and business value.

The National Institute of Standards and Technology (NIST) specifies in its guidance on security and privacy controls for Federal Information Systems that an organization should employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components. This should include software license information, software version numbers, component owners, and for network components or devices, machine names and network addresses. NIST also specifies the organization should use software in accordance with contract agreements and copyright laws, tracking the use of software and associated documentation protected by quantity licenses to control copying and distribution.

Managing software licenses takes a coordinated effort between various sections within ISA and the continual communication between ISA and Department management. There are three types of software licenses purchased by the Department:

- Perpetual License- perpetual licenses typically authorize an individual to use a specific version of a software program continually with a one-time payment.

- Subscription License- subscription software typically includes the software license, software maintenance, product upgrades, and access to technical and developer support for a defined period and requires renewal.

- Server-Based License- licensed software used with computing. Typically, the end-user will install a software license server on a host computer to provide licensing services to an enterprise computing environment. This server-based software license type is infrequently purchased and has many different components. Usually, these purchases are tied to special projects.

Variance Software Approval

The Department maintains a list of software that has been approved by the Chief Information Officer (CIO) and Information Security Manager (ISM).

Purchases of new software, freeware, or open-source software must be approved by management before the purchase is initiated or installed. If the software is not on the approved list, the recipient must complete a Variance of Software Standards Request form through the Self-Service Portal and it must be approved by the recipient's Bureau Chief, the ISM, and the CIO before the purchase can occur. If the software is on the approved list, a request to install the software is sent to Desktop Support with the PO

and license key. Before an installation occurs, the recipient must provide a PO with the request.

When the request has been approved, the Client Services team receives a service ticket within the Self-Service Portal. The recipient receives an email informing them that the software was approved and will be installed on their device. The Business Manager creates a service ticket with the PO and a license key to Desktop Support to install the software.

Compliance with Software License Agreements

Currently, the Department tracks the number and type of available licenses through purchasing documentation (i.e., the PO numbers and invoices) and requires members to submit service tickets to install new software. The procedures for completing service tickets include reviews to ensure there are available licenses to fulfill the requests, either through purchases of new software licenses or transfers. However, the software license agreements are not retained for review or monitoring.

Installation and Removal of License Software

Department members must request installation of newly purchased software, open-source or freeware software, or transfer of software from one Department owned device to another through the Self-Service Portal. Only certain members in ISA have the necessary privileges to perform installations.

When members are on-boarding or off-boarding, a service ticket request is submitted. If there is a certain license software that must be installed, Desktop Support will determine if there are any available licenses for that section and will install the software based on availability by reviewing the spreadsheet. The spreadsheet is then updated to reflect the license transfer.

ISA uses two methods to assign download and installation privileges to members. ISA uses Palo Alto to restrict and assign members' rights to download software. To control members' ability to install software and assign local administrative privileges, ISA uses Microsoft Active Directory's Group Policy. ISA assigns these rights based on the members' specific business needs and these different needs are divided into groups within Palo Alto and local administrative groups within group policy.

Separation or Internal Transfer

When a member leaves a position with the Department, a supervisor must submit an offboarding service ticket through the Self-Service Portal. Once Desktop Support receives the service ticket, a staff member will pull the departing member's data off the

computer, wipe all data from the computer, and prepare the computer for the next user. This includes removing all installed software and reloading the computer with Microsoft Office 365. Desktop Support will manually update the spreadsheet to reflect each software license no longer in use by the computer and user.

ISA uses a software, Recover Keys, to scan Department computers and discover installed software and license keys as part of the software install/uninstall process or upon request. ISA also uses SCCM to generate reports of software installed on Department computers. However, SCCM cannot scan computers that are not regularly connected to the network, so utilized licenses could remain undetected. Additionally, the usefulness of the reports is limited given the nature of the data and the inconsistent naming of software by vendors.

Expiration and Renewal License Software

At the beginning of each month, the ISA Software Plan List is reviewed to identify software up for renewal or expiring in the next three months. This list was created to maintain all software purchases for the Department and to identify renewal periods. ITFP members meet to discuss questions and concerns pertaining to the list. This list is sent to the necessary division's point of contact (POC) to notify them that software they are responsible for is up for renewal.

Monitoring Software Licenses

All installation requests of a newly purchased software, and open-source or freeware software, or a transfer of software from one Department owned device to another must be submitted through the Self-Service Portal via a service ticket. The majority of the Department's members do not have local administrative access privileges, which enforces the need for service tickets for the downloading of software.

If members are on-boarding or off-boarding, the supervisor submits a service ticket. If there are certain license software that must be installed, Desktop Support will determine the availability of licenses for that section and will install the software based on accessibility by reviewing the spreadsheet. The user's name will be added or deleted depending on if the member is on-boarding or off-boarding.

When Desktop Support receives a service ticket requesting software installation, a member of Desktop Support records the information from the service ticket to the spreadsheet. This is a way to monitor who purchased the software licenses, who the licenses are assigned to, and if it is currently in use on a computer. This spreadsheet is updated daily.

ISA uses Recover Keys, a software that can scan Department computers and discover installed software and license keys. This is also helpful when licenses are lost due to a computer crashing or inadequate tracking of transfers. Currently, Recover Keys is used upon request or as a part of the install/uninstall process for software. Desktop Support typically only uses this tool on specific computers, but it has the capability to scan multiple computers at once. When time permits, Desktop Support uses this software to update their spreadsheet with the found license information.

ISA uses SCCM to generate reports of software installed on Department computers at any given time. SCCM is unable to scan computers that are not regularly connected to the network, so there is the possibility that utilized licenses would not be detected. Additionally, the inconsistent naming of the software versions causes ambiguity when determining compliance.

Findings and Recommendations

Our evaluation determined that while the Department has implemented certain controls to manage software licenses, such as recording purchased software and preventing installation without authorization, controls pertaining to managing software licenses, monitoring license agreement compliance, and reviewing local administrator privileges should be strengthened. Strengthening these key areas would achieve greater efficiency and effectiveness and could mitigate the risks associated with inefficient management of software licenses.

Managing Software Licenses

Finding No. 1: Enhancing controls for managing software licenses would improve accountability and compliance.

NIST – *Security & Privacy Controls for Federal Information Systems & Organization* specifies that organizations should employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. This should include software license information, software version numbers, component owners, and for network components or devices, machine names and network addresses.

MEGABYTE Act of 2016 requires an agency to establish a comprehensive inventory and regularly track and maintain software licenses to assist in implementing decisions throughout the software license management life cycle.

We reviewed a sample of purchased software and compared the installation status information on the Desktop Support spreadsheet to the SCCM reports which reflect the

computer names that have the selected programs installed. Out of 62 purchased software licenses reviewed, there were 17 discrepancies (27%) identified where the installation status reported by the Desktop Support spreadsheet was not supported by the installation status indicated in the SCCM reports.

- For the purchase of Adobe Acrobat Pro 2017 on PO# B2EB42, there were 3 status discrepancies identified out of 12 purchased licenses (25%);
- For the purchase of Balsamiq Mockups on PO# B1F6BE, there were 3 status discrepancies identified out of 15 (20%) purchased licenses; there was also one instance where a license was marked as installed on a Department computer, but there was no computer name recorded on the Desktop Support spreadsheet and therefore it could not be verified by the SCCM reports;
- For the purchase of Microsoft Visio Pro 2013 on PO# AC11EE, there were 9 status discrepancies out of 20 purchased licenses (45%); and
- For the purchase of Microsoft Visio Pro 2016 on PO# B1E8ED, there were 2 status discrepancies out of 4 licenses purchased (50%).

We additionally reviewed the software purchase documentation to determine the number of licenses obtained by each purchase. We compared the total number of licenses purchased against the Desktop Support spreadsheet.

During our review, we noted the following:

- For the purchase of Adobe Acrobat Pro 2017 on PO# B2EB42, the purchase order reflected 12 licenses were purchased, but the Desktop Support installation records reflected two entries as “12 of 12” for the certificate key which resulted in 13 total license entries associated with the 12 licenses purchased. While the licenses were not over-installed at the time of the review, there is greater risk of over-installing because of the duplicate entry.

Because the Desktop Support spreadsheet is maintained manually, errors are more likely. Due to some Department-owned computers not being monitored because they’re not active on the network, inconsistent naming from software vendors, and resource restraints, Desktop Support cannot assure accuracy of the spreadsheet. Additionally, SCCM does not have the capability to identify or scan when computers are not on an active network. Software on inactive devices could go undetected. The data provided by SCCM could be more useful if it was translated by a software asset management (SAM) system. Utilizing a SAM system would ensure the management of software license and enhance license compliance.

The Department does not consistently monitor what software is being utilized; however, ISA has implemented a new service product that has the capability of replacing the Service Manager Portal to capture this data regularly.

Recommendation

We recommend ISA management implement a comprehensive enterprise-wide software license inventory program that uses automated discovery and inventory tools and metrics to improve accountability and compliance.

Management Response

ISA management concurs with this finding, however sufficient funding and skilled resources to implement and maintain a toolset are not available to the Division. ISA will continue to review and refine our manual processes as well as draft a legislative budget request proposal for consideration during the next budget cycle.

License Agreement Compliance

Finding No. 2: Controls should be implemented to improve monitoring of software license agreement compliance.

NIST specifies organizations should use software in accordance with contract agreements and copyright laws and track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

While the Department has processes and controls to record and track the software licenses purchased, issued, and installed, there is currently not an effective system to monitor and verify compliance with software license agreements. The Department determines the number and type of licenses purchased from invoices and does not currently monitor and verify compliance with the provisions of the software license agreements. Further, software license agreements are not retained for review or monitoring.

ITFP staff have begun discussions with Desktop Support to perform spot checks for compliance but given the available tools and COVID-19 disruptions, those plans have been delayed.

Reviewing software license agreements and monitoring the Department's compliance with the agreements are necessary to decrease the Department's risks associated with noncompliance. These risks include software audits (which can require a large amount of Department resources), potential fines, business interruptions, and adverse public image.

Recommendation

We recommend ISA, in coordination with Department divisions, implement an effective system to retain, review, and monitor the Department's compliance with software license agreements.

Management Response

ISA management concurs with this finding and will share this recommendation with the General Counsel's office and the Division of Administrative Services in order to develop a plan to best accomplish this. The Florida Highway Patrol and the Division of Motorist Services would also be engaged during the planning process. ISA will begin the planning process by June 30, 2021.

Local Administrative Access Privilege Controls

Finding No. 3: Periodically reviewing members with local administrative access privileges would improve security and accountability.

ISA's *Information Security Policy Manual* states that the Department should ensure that information resources are protected from computer threats, including, but not limited to viruses, malware, and other threats of malicious software designed to compromise system integrity.

To have the capability to install software on a Department device, a member must be approved by an Enterprise Security Management (ESM) member and added to a local administrative group list via Microsoft Active Directory's Group Policy. When members separate from the Department, their access is turned off through Active Directory and they are then removed from the group.

However, when members with local administrative access privileges transfer to another area within the Department, there is no process to notify ESM of the transfer, so that ESM can evaluate whether local administrative access privileges remain appropriate for the member's new position. The member remains on the group list unless the member or their supervisor notifies ISA to change their access.

During our review, we noted at least one member listed with local administrative access privilege who changed positions within the Department since they were originally approved for the group. When we inquired as to the process for determining whether local administrative access privileges remained appropriate for the member's new position, ISA management indicated there was not a process in place to monitor or evaluate the list of authorized members.

The Department does not have a consistent monitoring process for members who have local administrative access privileges to ensure the list of authorized members remain appropriate. Without adequate monitoring, the Department may not have reasonable assurance that the list of members with local administrative access privileges authorized to install software remains appropriate.

Recommendations

We recommend ISA implement a process to periodically review members with local administrative access privileges to ensure permission levels remain appropriate.

We also recommend ISA provide written guidance to management to notify ISA of any position changes of members with local administrative access privileges.

Management Response

ISA management concurs with this finding and intends to implement a biannual review process to ensure local admin permission levels remain appropriate by June 30, 2021. In addition, the Access Management team within ISA will review its practices and policies to address how position changes of members with local administrative access privileges. Once these updates are made, ISA will provide written guidance within the Access Management Processes document. This will also be completed by June 30, 2021.

Purpose, Scope, and Methodology

The purpose of this audit was to review and evaluate the efficiency and effectiveness of software license management and compliance with best practices, applicable laws, Department policy, and procedure.

The scope of this audit included Information Systems Administration license software management practices from July 2018 through December 2019.

The methodology included:

- Reviewing applicable statutes, rules, manuals, and procedures;
- Interviewing Department members and determine the methods through which software licenses are recorded and tracked and to determine if the controls are adequate;
- Determining whether there is an effective system in place to monitor and verify compliance with software license agreements;

- Reviewing controls over license software installation and removal and determining if controls are adequate to prevent open-source or freeware software from being installed without authorization and to ensure software installations are appropriately licensed to the Department;
- Determining how licenses are handled during separation of employment or internal transfers and evaluate whether adequate controls are in place;
- Determining how software license expirations and renewals periods are tracked and determining if the processes are adequate;
- Selecting a sample of purchased licensed software and determining if the Department's usage is compliant with the license agreements; and
- Identifying and determining the extent of monitoring and quality assurance activities regarding software licenses and compliance with licensing agreements.

Distribution, Statement of Accordance, and Project Team

Distribution

Terry L. Rhodes, Executive Director
Jennifer Langston, Chief of Staff
Boyd Dickerson-Walden, Chief Information Officer
Scott Bean, Chief of Service Operations
Scott Morgan, Information Security Officer
Michelle Morris, Manager of IT Financial & Planning Services
Jerome Brady, IT Business Consultant Manager

Melinda M. Miguel, Chief Inspector General
Sherrill F. Norman, Auditor General

Statement of Accordance

Section 20.055, Florida Statutes, requires the Florida Department of Highway Safety and Motor Vehicles' Inspector General to review, evaluate, and report on policies, plans, procedures, accounting, financial, and other operations of the Department and to recommend improvements. This audit engagement was conducted in accordance with applicable *International Standards for the Professional Practice of Internal Auditing* published by the Institute of Internal Auditors and *Principles and Standards for Offices of Inspector General* published by the Association of Inspectors General.

Project Team

Engagement conducted by:
Kim Butler, Auditor
Bethany Vickerman, Auditor

Under the supervision of:
Erin Mook, Audit Director

Approved by:

Mike Stacy, Inspector General

ATTACHMENT - Management Response

FLHSMV
FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES

Terry L. Rhodes
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

MEMORANDUM

DATE: December 16, 2020
TO: Erin Mook, Audit Director
FROM: Clayton Boyd Dickerson-Walden, Chief Information Officer
SUBJECT: Software License Management Audit (201920-16)

The following is our response to the findings and recommendations presented in the report.

Finding 1: ***Managing Software Licenses***

Enhancing controls for managing software licenses would improve accountability and compliance.

Recommendation

We recommend ISA management implement a comprehensive enterprise-wide software license inventory program that uses automated discovery and inventory tools and metrics to improve accountability and compliance.

Management Response

ISA management concurs with this finding, however, sufficient funding and skilled resources to implement and maintain a toolset are not available to the Division. ISA will continue to review and refine our manual processes as well as draft an LBR proposal for consideration during the next budget cycle.

Finding 2: ***License Agreement Compliance***

Controls should be implemented to improve monitoring of software license agreement compliance.

Recommendation

We recommend ISA, in coordination with Department divisions, implement an effective system to retain, review, and monitor the Department's compliance with software license agreements.

Management Response

ISA management concurs with this finding and will share this recommendation with the General Counsel's office and the Division of Administrative Services in order to develop a plan to best accomplish this. The Florida Highway Patrol and the Division of Motorist Services would also be engaged during the planning process. ISA will beginning the planning process by June 30, 2021.

Finding 3: ***Local Administrative Access Privilege Controls***

Periodically reviewing members with local administrative access privileges would improve security and accountability.

Recommendations

We recommend ISA implement a process to periodically review members with local administrative access privileges to ensure permission levels remain appropriate.

We also recommend ISA provide written guidance to management to notify ISA of any position changes of members with local administrative access privileges.

Management Response

ISA management concurs with this finding and intends to implement a biannual review process to ensure local admin permission levels remain appropriate by June 30, 2021. In addition, the Access Management team within ISA will review its practices and policies to address how position changes of members with local administrative access privliedges. Once these updates are made, ISA will provide written guidance within the Access Management Processes document. This will also be completed by June 30, 2021.