SOUTH FLORIDA WATER MANAGEMENT DISTRICT

# Information Technology Resource Approval Process Audit

**Project # 15-06**

**Prepared by**
Office of the Inspector General

**J. Timothy Beirnes, CPA, Inspector General**
**Gary T. Bowen, CIA, Lead Consulting Auditor**

sfwmd.gov

**SOUTH FLORIDA WATER MANAGEMENT DISTRICT**

July 14, 2016

Governing Board Members:

Re: Information Technology
Resource Approval Process Audit
*Project Number 15-06*

This audit was performed pursuant to the Inspector General's authority set forth in Chapter 20.055, F.S. Our objective focused on the process for purchasing Information Technology hardware, software, and services; and obtaining the required approval from the IT Bureau. Gary Bowen and I prepared this report.

Sincerely,

J Timothy Beirnes

J. Timothy Beirnes, CPA
Inspector General

# TABLE OF CONTENTS

## BACKGROUND

In accordance with the Audit Plan, we conducted an audit of the Information Technology Resource Approval Process.

Prior to District divisions/bureaus purchasing information technology products (i.e., equipment software, etc.) they are required to obtain resource approval from the Information Technology Bureau. The information technology resource approval process was established so that the Information Technology Bureau can ensure products are compatible with the existing equipment and the Bureau possess the ability to support the technology products subsequent to their purchase.

District policy has recently been revised to state that "Users of District IT Resources must not buy, procure, or contractually bind the District for any IT resources, systems, or services without the approval of IT management" (Chapter 130 – Information Technology Policy Section 130.4, Paragraph 3- l). The District has implemented controls and processes to help ensure compliance to this policy. They include:

- Workflows in the SAP Procurement Module that require appropriate IT approvals for requisitions entered with IT material codes.
- Implementation of a service management application (RemedyForce*)*, which creates automatic approval workflows for hardware and software requests.
- Desktop configuration settings which limit the user's administration rights, which are required to download or install software.

Purchase requisitions originating through the SAP procurement module contain approval workflows requiring electronic approval signoffs by the IT Management Section Leader or the IT Bureau Chief. These requisitions are also subject to Procurement policies and procedures, in addition to requiring IT Bureau approval. This process also relates to the procurement of IT services such as contractors or consultants.

The IT resource purchase approval process is integrated with the RemedyForce service management application.  RemedyForce is a real-time, cloud based service and support application the Solution Center uses for incident and problem management, service requests, and software and hardware purchases and installation requests.  As IT customers (District IT users) submit requests for new hardware and /or software via RemedyForce, the application initiates automated workflows which takes the request through the review, approval, acquisition, and installation process.

Appendix I – Software Request Process flowchart depicts the approval process as it goes through the RemedyForce application.  Requests are initially reviewed for approval by the IT Asset Management Section.  Requests for new software require the approval of the Section Administrator – IT Operations, to ensure the District is able to support the software.  Requests for software that is not in stock, and exceeds $1500 in cost, must go through the SAP procurement and approval process.

Appendix II – Hardware Request Process flowchart depicts a process similar to the software approval process, but does not require the approval of the IT Operations Section Administrator.

Unauthorized software installations and downloads from the Internet, outside of the approval process, can be prevented by restricting administrative rights.  Network domain administrative rights enable users to install drivers, change system and network configuration settings, install software, and make changes in the Program Files directory of individual computers.  The IT Customer Service Section has administrative rights and is designated to perform all desktop software installations and make changes to system and network configuration settings.

## OBJECTIVE, SCOPE, AND METHODOLOGY

The audit focused on the process for purchasing IT hardware, software, and services and obtaining the required resource approval from the IT Bureau. The audit examined how well District departments are complying with the approval requirement. Additionally, the audit reviewed IT software license compliance and utilization. Some of the procedures for this audit were performed in conjunction with the previously issued Audit of Procurement Card Transactions.

To accomplish our objectives we performed the following:

- Reviewed IT resource purchase policies and procedures.
- Interviewed appropriate personnel to obtain an understanding of the approval process and their roles in it.
- Reviewed and tested the resource approval process.
- Identified key control points in the approval process and evaluated their effectiveness.
- Reviewed software copyright report for license compliance and utilization.
- Followed up on P-Card (purchase card) audit findings pertaining to potentially unauthorized IT resource purchases.

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.

## AUDIT RESULTS

### Executive Summary

We found that the IT Bureau has adequate controls and processes in place to help ensure District departments comply with the policy on acquiring IT resources. However, based on our review and testing, we found that the controls and processes to prevent unauthorized downloading or installation of software could be improved by limiting desktop administrative rights. We found that there were approximately 700 users who had been granted network domain administrative rights. This means that they were able download and install software, change configurations settings and install drivers, and thereby might be able to bypass controls limiting user installation of hardware and software.

A review of installed software for a sample of 25 users found that 6 had potentially unauthorized software installed which was not listed on the software inventory database. Further analysis of installed software was performed to determine whether the District was in compliance with copyright and licensing requirements. We concluded that the District for the most part was in compliance with copyright and licensing requirements as we found that only 8 licensing units out of 617 total were non-compliant. The analysis also revealed that a number of licenses held exceeded the actual number being used, which suggested that savings could be realized by reducing the number of unneeded licenses.

Our follow up of two potential P-Card purchase policy violations determined that one did not require IT approval, while the other was considered an isolated incident.

### Limit PC Administration Rights

A key control in the IT resource acquisition approval process is the restriction of personal computer user administrator rights. Network domain administrator rights allow users to install drivers, change system and network configuration settings, install software, and make changes in the Program Files directory. Most PC users at the District do not need administrator rights, and in fact, granting them may create a threat to IT security. Limiting administrator rights functions as a resource acquisition control by preventing users from installing software and drivers acquired outside of the approval process and requiring users to contact the IT Help Desk for new software downloads and installations, or to make other changes to their PC.

We obtained a list of all network domain users who have administrator rights and noted that there were approximately 700 users listed. Each of these users have rights to download and install software, make changes to their PC configuration settings, and install drivers. This could be done without going through the help desk, or obtaining proper approvals, and thereby possibly circumventing controls and District IT Resource policy.

**Recommendations:**

1. **Review the list of users with administrator rights and determine whether there is a legitimate need for them to retain the rights. Rescind the administrator rights as deemed appropriate.**

   **Management Response:**

   Asset Management, the Solution Center, the Chief Information Security Officer, and the Chief Information Officer reviewed the list of users with administrator rights and removed the rights from all users that did not have a specific requirement for local admin rights (i.e. install software, drivers or connect equipment). The review resulted in 505 reductions. There are software licenses that require local administrator rights such as the newest version of AutoCAD, Rockwell software, and Planar software. Local administrator rights are also needed to connect with specific field or lab equipment, for Engine/Fleet Diagnostics, and to correct a known issue with the Pump Logs at the Pump Stations.

| Local Admin Rights By User | 10/26/2015 | 5/3/2016 | Reduction |
|---|---|---|---|
| **Total** | 594 | 89 | **505** |

**Responsible Division:**
Information Technology

**Estimated Completion:**
May 2016

2. **Develop criteria and a process for granting administrator rights in limited situation**s.

   **Management Response:**
   IT developed a new process for the review/approval of requests for administrator rights. All requests are entered through a Remedy Service Request and require approval by the Chief Information Security Officer or Chief Information Officer. Local admin rights are only granted in situations where it is required for the use of software or a device. In addition, IT Asset Management will annually audit desktop software for staff with local admin rights to ensure that they are compliant.

   **Responsible Division:**
   Information Technology

   **Estimated Completion:**
   Process completed March 2016 and audit of users will occur annually in June

### Ensure Installed Desktop Software is Authorized

The IT Asset Management Section maintains an inventory of all IT assets including hardware and installed software. The IT Bureau has the capability to review and compare the software applications installed on each PC to the licenses inventory to ensure their agreement and ascertain whether all installed software is authorized and licensed. A software report from the Asset Lifecycle Manager Inventory database (a record of all authorized software installed on a particular PC) can be compared to a software report from the System Center Console Manager discovery tool (reports software actually installed on the PC). Differences between the reports may represent unauthorized software, or incomplete records which require further follow up.

We selected a sample of 25 users having administrator rights for review to determine whether the software installed on their computers was authorized and agreed with the inventory. With the assistance of IT staff, using the System Center Console Manager Discovery Tool, we were able to compare the software actually installed to the software recorded in the inventory database for the particular user's computers selected.  We found that in 17 instances, the software inventory matched the discovered software, in 2 cases there were minor differences, and in 6 cases there were major differences.

**Results of Installed Software Review**

| Finding | Number | Percent |
|---|---|---|
| Software Matched | 17 | 68% |
| Minor Differences | 2* | 8% |
| Significant Differences | 6** | 24% |
| Total Sampled | 25 | 100% |

* Minor differences include freeware installed by user.

******Significant differences include one or more purchased software installed.

Using these results as a basis for estimating compliance with IT resource policies, we concluded that the District is complying approximately 68% of the time when users have administrator rights.

It was noted that the Asset Management Section does not perform regular periodic audits of software installed on District's PCs, however, reviews are performed at the time of the maintenance renewal, prior to any software updates or upgrades, and when replacing a computer with a new one.  Implementing a plan to perform periodic audits of the installed software on the District's computers, using discovery tools already available to the IT Asset Management section, would help to ensure greater compliance with IT policy by detecting unauthorized software.

**Recommendations:**

3. **Follow up on the differences noted where discovered software did not match the inventory database.**

   **Management Response:**

   Of the 25 users audited, 17 matched the software inventory, 2 had minor differences and 6 had significant differences. Asset Management followed up with those users with discrepancies. If the software was justified, it was added to the Asset Management inventory database. If the software was not justified, it was removed from the desktop.

   **Responsible Division:**

   Information Technology

   **Completed:**
   October 2015

4. **Consider performing periodic installed software reviews to look for unauthorized software.**

   **Management Response:**

   At least once per year, Asset Management will run reports on those users with administrator privileges to compare the IT inventory to what is actually on the desktops and follow up on any discrepancies.

   **Responsible Division:**

   Information Technology

   **Completed:**

   On-going – annually in June

### Review Application Licenses

Purchased software applications usually require a license to be legally installed and operated on a users' computer.  Licenses may be purchased on a per-user or an enterprise basis. Application installations which exceed the number of licenses purchased are considered copyright violations and can lead to hefty penalties, when discovered by the software vendor. We noted that a software license audit for the period 5/1/2015 through 6/1/2015 was performed by the IT Asset Management section using Express Metrix - Am I Compliant software.  The software determines whether we are conforming to licensing requirements by comparing the software inventory to a list of software licenses owned by the District.  The number of licenses per application (license units) was compared to the number of licenses in use, to determine whether the District is compliant with licensing requirements.

The audit results are expressed in terms of license units.  The following table summarizes the results of the software license audit:

| | Count | Percent of Total |
|---|---|---|
| Non-compliant License Units | 8 | 1.3% |
| Compliant License Units | 609 | 98.7% |
| Total License Units | 617 | 100.0% |

Based on the above findings, with only 8 non-compliant license units, we concluded that IT Resource management is doing an adequate job of ensuring we are compliant with licensing requirements.

The audit results also indicated that several software applications are being under-utilized. The audit report detail shows that in a number of instances, the number of application licenses exceeds the license units actually in use.  Reviewing application usage and eliminating excess licenses, could lead to cost savings by reducing software license and maintenance fees.

**Recommendation**

5. **Review the utilization of application licenses and evaluate whether the number of licenses which exceed the usage is necessary.**

   **Management Response:**

   Asset Management will run reports every 6 months, using Express Metrix, to ensure that the number of licenses installed does not exceed the number owned.  In cases where the number of installations exceeds the licenses owned, IT will verify approval for the software and purchase sufficient licenses to remain compliant.  For those licenses that are not authorized, IT will remove the software immediately.

   **Responsible Division:**

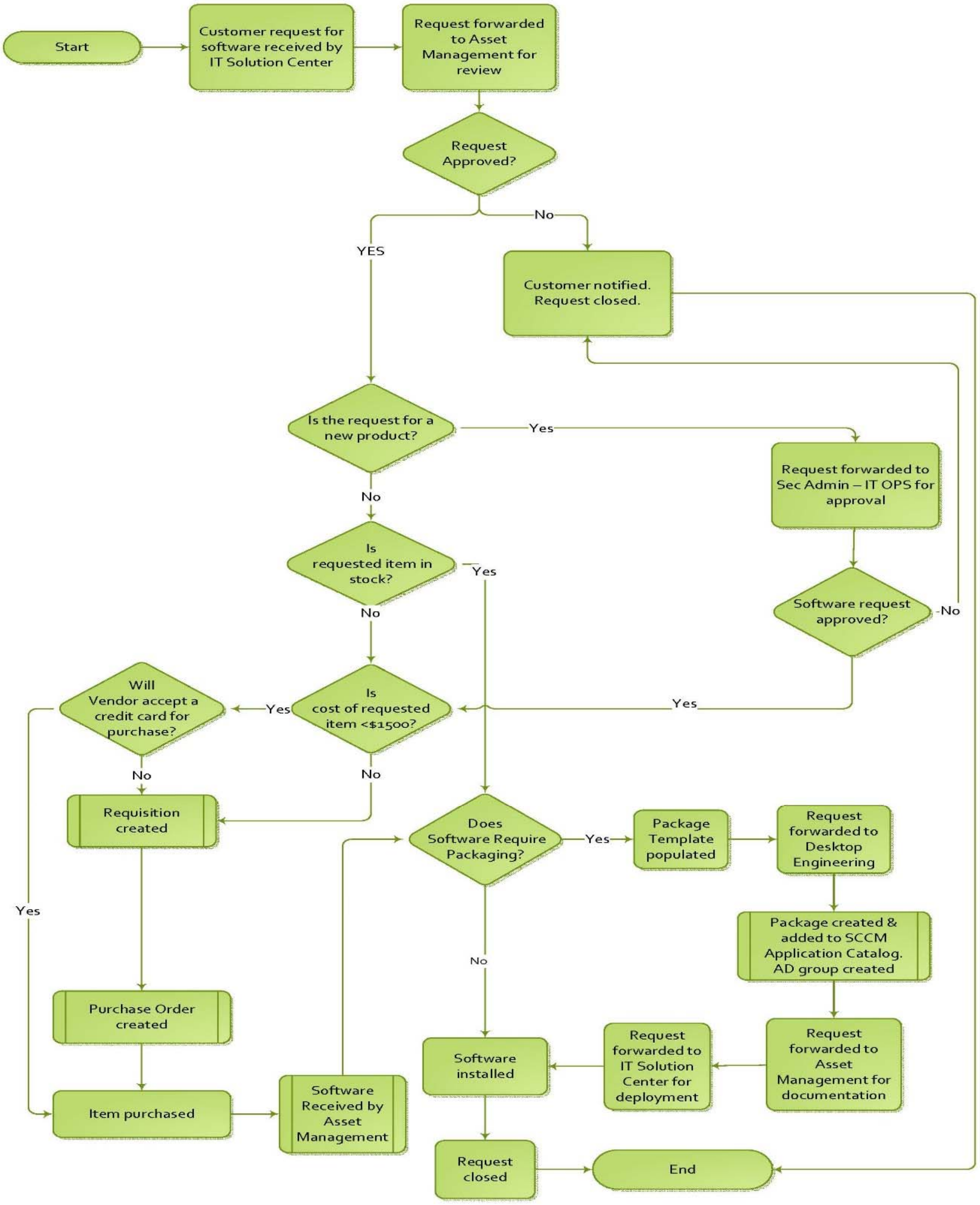
   Information Technology

   **Estimated Completion:**

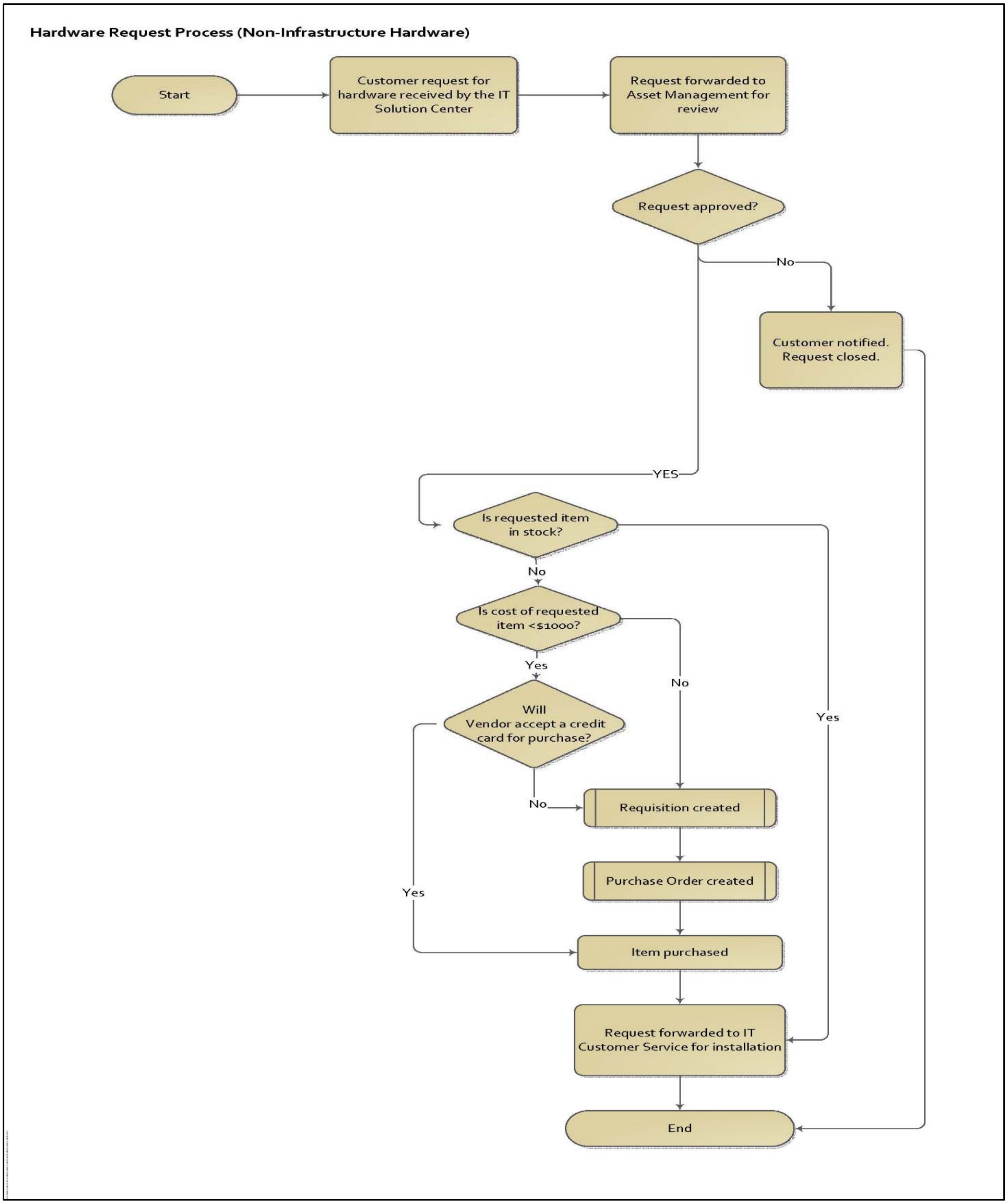
   On-going every six months in October and March

# APPENDIX I

Software Request Process


Start
Customer request for software received by IT Solution Center
Request forwarded to Asset Management for review
Request Approved?
No
YES
Customer notified. Request closed.
Is the request for a new product?
Yes
Request forwarded to Sec Admin – IT OPS for approval
No
Is requested item in stock?
Yes
Software request approved?
No
No
Will Vendor accept a credit card for purchase?
Yes
Is cost of requested item <$1500?
Yes
No
No
Requisition created
Does Software Require Packaging?
Yes
Package Template populated
Request forwarded to Desktop Engineering
Yes
No
Package created & added to SCCM Application Catalog. AD group created
Purchase Order created
Software installed
Request forwarded to IT Solution Center for deployment
Request forwarded to Asset Management for documentation
Item purchased
Software Received by Asset Management
Request closed
End

# APPENDIX II



Hardware Request Process (Non-Infrastructure Hardware)

Start
Customer request for hardware received by the IT Solution Center
Request forwarded to Asset Management for review
Request approved?
No
Customer notified. Request closed.
YES
Is requested item in stock?
No
Is cost of requested item <$1000?
Yes
No
Yes
Will Vendor accept a credit card for purchase?
No
Requisition created
Purchase Order created
Yes
Item purchased
Request forwarded to IT Customer Service for installation
End