



*Controls Should Be Strengthened to
Ensure Timely Resolution of Information
Technology Incident Tickets*

September 13, 2019

Reference Number: 2019-20-055

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500

E-mail Address / TIGTACommunications@tigta.treas.gov

Website / <http://www.treasury.gov/tigta>



To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.



HIGHLIGHTS

CONTROLS SHOULD BE STRENGTHENED TO ENSURE TIMELY RESOLUTION OF INFORMATION TECHNOLOGY INCIDENT TICKETS

Highlights

Final Report issued on September 13, 2019

Highlights of Reference Number: 2019-20-055 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The Information Technology organization's Enterprise Operations and User and Network Services functions have joint responsibility for the Incident Management program. It is important to resolve incident tickets within target resolution times to minimize the level of disruption to the IRS and its ability to consistently process taxpayer returns and further tax administration.

WHY TIGTA DID THE AUDIT

This audit was initiated to assess the effectiveness and efficiency of the processes and practices for resolving information technology incidents and reported problems for the IRS's tax administration systems.

WHAT TIGTA FOUND

Incident tickets are used to document and track any unplanned interruption or reduction in the quality of an information technology service. The IRS has taken steps to improve its controls over incident ticket management, such as identifying and implementing initiatives to foster more effective and efficient incident management operations.

On October 2, 2017, the IRS upgraded its incident management tool, the Knowledge Incident/Problem Service Asset Management (KISAM)-Service Manager (SM) module. As of July 30, 2019, all open incident tickets that were in the old KISAM-SM module have been closed.

However, TIGTA reviewed Priority 1 through Priority 4 incident tickets and found that the IRS

has not generally improved the percentage of tickets resolved and closed within their target resolution times over the last three fiscal years.

In addition, the IRS only met its monthly performance goals more than 50 percent of the time for 12 of its 25 incident management metrics in Fiscal Year 2018. Only seven of the 25 incident management goals were consistently met for 10 months or more during the fiscal year. Moreover, incident management metrics are not up to date or consistently used by employees receiving the metric reports.

Furthermore, better documentation of incident assessments and actions taken would improve incident ticket resolution efficiency. A review of 16 closed incident tickets from Fiscal Year 2018 with four or more reassignments determined that seven of the tickets may have been inefficiently worked and had either minimal or no documentation of actions performed.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer update performance goals and renegotiate specific levels of service to better reflect current resource allocations; update performance metrics to better align with overall program objectives and expanded use in daily operations; and ensure that all incident assessments and actions performed are documented in incident tickets to provide a complete historical record of all activities.

The IRS agreed with all of our recommendations. The IRS plans to complete an evaluation of the current levels of service to determine the appropriate incident management performance goals in line with the business need(s); complete an evaluation of incident management performance metrics to ensure alignment with program objectives and use in daily operations; and update the business-wide ticket guidelines to focus on the activity description and reassignments documenting an incident history.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 13, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Controls Should Be Strengthened to Ensure
Timely Resolution of Information Technology Incident Tickets
(Audit # 201820015)

This report presents the results of our review to assess the effectiveness and efficiency of the processes and practices for resolving information technology incidents and reported problems for the Internal Revenue Service's (IRS) tax administration systems. This review is included in our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenge of Achieving Program Efficiencies and Cost Savings.

Management's complete response to the draft report is included as Appendix VI.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).



*Controls Should Be Strengthened to Ensure Timely
Resolution of Information Technology Incident Tickets*

Table of Contents

Background	Page 1
Results of Review	Page 4
Incident Management Performance Levels Can Be Improved	Page 4
Recommendation 1:	Page 10
Incident Management Metrics Are Not Consistently Used or Not Used at All	Page 10
Recommendation 2:	Page 12
Better Documentation Would Improve Efficiency in Resolving Incident Tickets	Page 12
Recommendation 3:	Page 14
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 15
Appendix II – Major Contributors to This Report	Page 17
Appendix III – Report Distribution List	Page 18
Appendix IV – Incident Management Metrics Defined	Page 19
Appendix V – Glossary of Terms	Page 22
Appendix VI – Management’s Response to the Draft Report	Page 24



*Controls Should Be Strengthened to Ensure Timely
Resolution of Information Technology Incident Tickets*

Abbreviations

EOps	Enterprise Operations
ESD	Enterprise Service Desk
IRS	Internal Revenue Service
KISAM	Knowledge Incident/Problem Service Asset Management
P	Priority
SM	Service Manager
UNS	User and Network Services



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Background

The Information Technology organization's Enterprise Operations (EOps) and User and Network Services (UNS) functions have joint responsibility for the Incident Management program. The program establishes procedures to monitor information technology-related incidents and problems throughout the Internal Revenue Service's (IRS) incident management life cycle.¹ These procedures provide the necessary steps and define the standards for recording, classifying and prioritizing, investigating and diagnosing, resolving or forwarding, and closing incidents and problems.

The UNS function is the process owner for incident management and has primary responsibility for distributing, managing, and supporting the information technology hardware and client software products issued and used by IRS's end users. The incident management process begins when a customer either calls into or submits an online request for information technology products and services to the UNS function's Customer Service Support Enterprise Service Desk (ESD). The ESD was created to provide a single point of contact and a process for customers requesting products and services, such as installing or troubleshooting hardware and software, assistance with resetting and changing a password, or requesting system access. The ESD creates, assigns, and monitors tickets affecting systems as well as users, and tracks them on the Knowledge Incident/Problem Service Asset Management (KISAM)-Service Manager (SM) module. This module serves as the primary incident management tool and provides a centralized database for incident reporting, tracking, and support services.

All contacts with the ESD are categorized as either an interaction or an incident. An interaction is the documented contact between the first-level support specialist and the customer to obtain information regarding the issue, or is automatically created when the customer submits a service request online. Interactions can be escalated to an incident if the first-level support specialist is unable to resolve the issue or unable to reach the customer back, or if there are multiple contacts for the same issue. Incident tickets are used to document and track any unplanned interruption or reduction in the quality of an information technology service. For issues not resolved on the initial contact, the incident ticket is assigned to either another first-level support specialist or a service provider.

On October 2, 2017, the IRS upgraded the KISAM-SM module from version 9.41 to version 9.52. Some upgraded and new features included: access to dashboards and reporting functionalities that provide quick statuses of incident tickets, analytic tools to search and categorize an entire pool of incident tickets for trends, and work actions that can be tracked as associated tasks to a single incident ticket, *etc.*

¹ See Appendix V for a glossary of terms.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

The goal of incident management is to restore a service operation back to normal as quickly as possible, while minimizing the impact on business operations and ensuring that the best possible levels of service quality and availability are maintained. At the IRS, incident tickets are categorized into four numeric levels, Priority (P) 1 through P4, which are determined by how quickly the issue must be resolved and the level of business disruption. While the IRS does not have an overall performance goal for each priority level, it has defined target resolution times.

- **P1 incident tickets:** A severe mission critical work stoppage or any issue related to safety or health, *e.g.*, fire and electrical, or impact on vital customer commitments of national or area-wide scope, affecting multiple internal or external customers, and impacting service to taxpayers.
 - Target Resolution Time: Within four hours.
- **P2 incident tickets:** A potential work stoppage that could have a direct impact on the service to taxpayers or if its scope is multiuser and there is no workaround. The incident could lead to a severe mission critical work stoppage if actions are not taken to resolve the incident or problem.
 - Target Resolution Time: Within eight hours.
- **P3 incident tickets:** A work stoppage for one customer with no workaround.
 - Target Resolution Time: Within two business days.
- **P4 incident tickets:** A noncritical and nonsoftware incident or problem in which it is not a work stoppage and there is a workaround.
 - Target Resolution Time: Within four business days.

The EOps function deploys and maintains an information technology infrastructure that supports the business and administrative needs of the IRS. The EOps function is the owner of incident escalation and its Information Technology Operations Command Center manages the restoration of services for its customers during outages by identifying activities to be performed and contacting key personnel to ensure that high-priority incidents are being worked in a timely manner. It helps to ensure timely escalation and resolution of high-priority incidents by continually monitoring the IRS's network 24 hours a day for P1 and P2 incidents.

This review was performed with information obtained from the Information Technology organization's EOps and UNS functions in Philadelphia, Pennsylvania, and Memphis, Tennessee, during the period July 2018 through July 2019. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and



*Controls Should Be Strengthened to Ensure Timely
Resolution of Information Technology Incident Tickets*

methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



*Controls Should Be Strengthened to Ensure Timely
Resolution of Information Technology Incident Tickets*

Results of Review

The IRS has taken steps to improve its controls over incident ticket management. In July 2018, the EOps and UNS functions implemented the “One Operation” model, a collaboration and partnership to identify and implement initiatives to enhance the overall customer experience and to foster more effective and efficient incident management operations. Some initiatives included the following:

- KISAM User Group – A collaborative effort between the KISAM owner and process owner to create a forum to identify and implement tool enhancements.
- High-Priority Change – Identifying special approvals for groups to have the ability to change incident tickets to a P1 or P2 ticket to help improve the handling of higher priority tickets.
- Information Alerts Publishing – Providing all KISAM users the capability to issue KISAM information alerts.
- Staff Phone and Ticketing Support – Adding former ESD staff, now working for the EOps function, to provide part-time support in answering calls to reduce call wait times.
- Incident Manager of Record Training – Mandatory training for all front-line and senior managers in the Information Technology organization. This training will help ensure that incident managers of record are prepared, and ESD managers have a better understanding of their roles and responsibilities during the incident escalation process.

However, the IRS can take additional steps to improve incident management performance levels and metrics reporting, as well as incident ticket resolution efficiency.

Incident Management Performance Levels Can Be Improved

Priority incident tickets are not generally resolved within target resolution times

The IRS has not generally improved the percentage of incident tickets resolved and closed within its target resolution times over the last three fiscal years. Using the *Open Time* and *Close Time* fields from the KISAM-SM module, the percentages of incident tickets resolved within their target resolution times for Fiscal Year 2018 have decreased when compared to Fiscal Year 2017 for all four priority levels. In addition, when compared to Fiscal Year 2016, the Fiscal Year 2018 percentages decreased for three of the four priority levels.

In discussions with EOps function management, they stated that assessing the effectiveness of the resolution of incident tickets is a much more complicated calculation than just using the

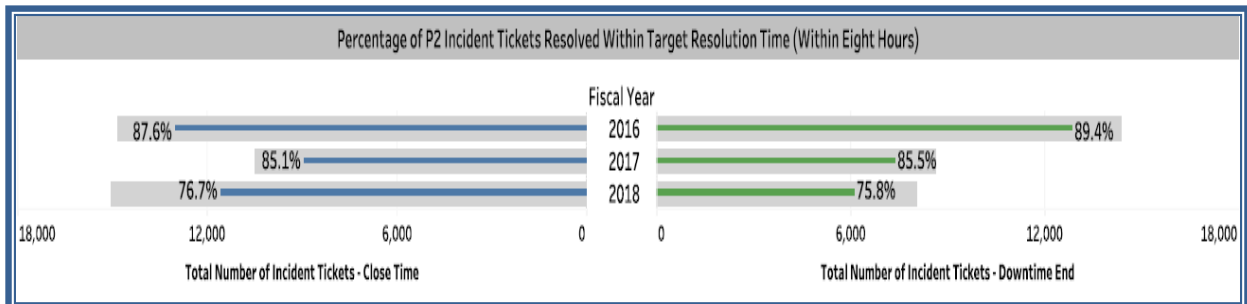
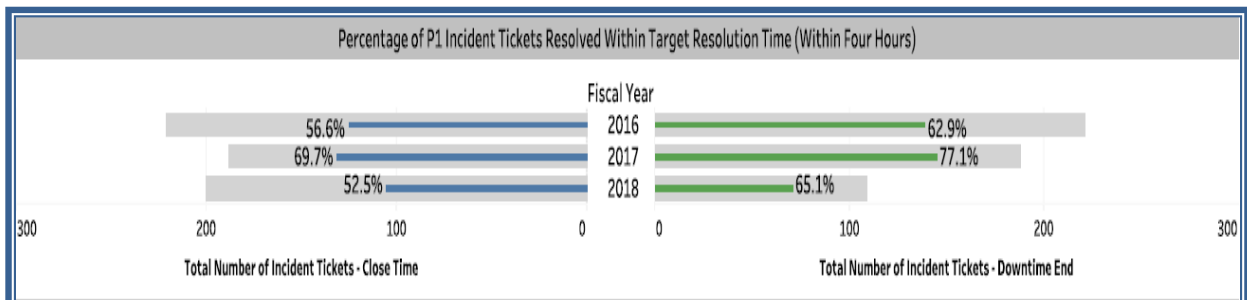


Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Open Time and *Close Time* fields from the KISAM-SM module. For example, some incident tickets are left open and monitored to ensure that their issues have been fully resolved or to identify and associate other incident tickets with similar issues, resulting in the incident tickets remaining open and not immediately closed. In these situations, a more accurate indicator to calculate the incident ticket resolution time is to use the *Downtime End* field, which provides the actual time it took for an incident to be resolved.

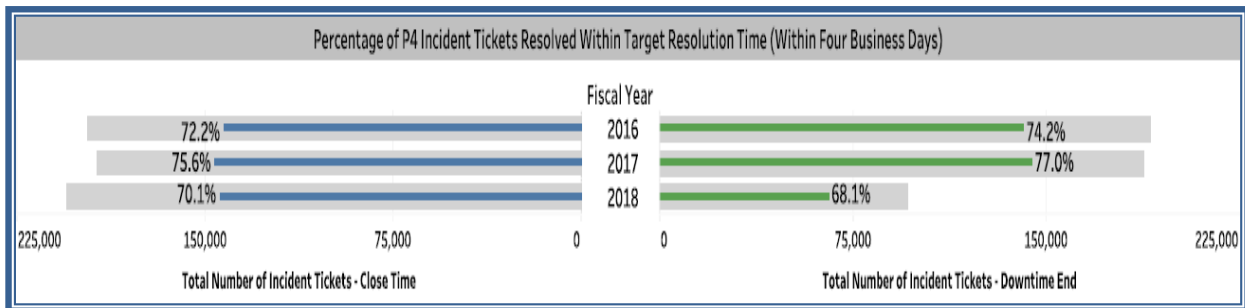
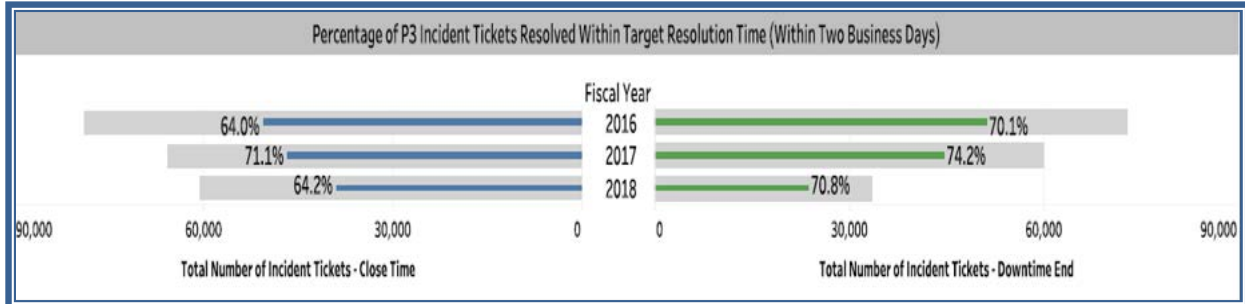
Based upon this information, we recalculated the percentage of incident tickets resolved within the target resolution times by priority level and fiscal year, using the *Open Time* and *Downtime End* fields. However, the *Downtime End* field was not always populated in the KISAM-SM module as this field is only used for incident tickets that are left open to ensure that their issues have been fully resolved or to associate other tickets with similar issues. For example, 143,132 (50.9 percent) of 281,102 incident tickets closed in Fiscal Year 2018 did not have any information in the *Downtime End* field, leaving only 137,970 incident tickets with the field populated. From incident tickets with that field populated, the percentage of incident tickets resolved within their target resolution times between Fiscal Years 2017 and 2018 have decreased for all four priority levels as in our initial assessment. However, when compared to Fiscal Year 2016, the percentages for only two of the four priority levels decreased in Fiscal Year 2018. Figure 1 provides a side-by-side comparison of the percentages of incident tickets resolved within their target resolution times by priority level and fiscal year, using the *Close Time* and *Downtime End* fields.

Figure 1: Percentage of Incident Tickets Resolved Within Target Resolution Times by Priority Level and Fiscal Year (Comparison Between Close Time and Downtime End Fields)





Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets



Source: Treasury Inspector General for Tax Administration review of incident tickets closed between October 1, 2015, and September 30, 2018, from IRS-provided data extracts of the KISAM-SM module.

In addition, EOps function management stated that depending on the customer reported issue, some incident tickets may be reclassified and escalated to a higher priority level, *e.g.*, a P2 to a P1 incident ticket, a P4 to a P2 incident ticket, *etc.* As incidents are assessed, priority levels are reviewed to ensure that they are properly categorized based upon how quickly the issue must be resolved and the level of business disruption. EOps function management also stated that when an incident ticket is escalated, the resolution time should be calculated based upon when the priority level changed. However, this information is not reflected in any incident management metric report or captured in a field in the KISAM-SM module that can be easily researched. It can only be identified through a manual review of the *Activities* section of the individual incident tickets. EOps function management further stated that they perform such reviews for P1 and P2 tickets, but when asked for any program metrics related to this issue, they were unable to provide them.

As a result, we further analyzed 38 closed P1 incident tickets that were not resolved within their target resolution time for Fiscal Year 2018 to identify if there was a change in priority level. We determined that 19 incident tickets did not have a change in priority level. Of the remaining 19, only three incident tickets were resolved within four hours from the recorded time the priority level changed, marginally increasing the percentage of incident tickets resolved within their target resolution times from 65.1 to 67.9 percent.

Another concern are the 4,937 incident tickets that remained open as of October 1, 2018. These tickets are for P3 (1,679) and P4 (3,258) incidents and are beyond their target resolution times of two and four business days, respectively. In addition, 1,412 (28.6 percent) of these incident



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

tickets were created and opened in the old KISAM-SM module prior to October 2, 2017. Seven of these incident tickets were created as far back as Fiscal Year 2013. Both EOps function and UNS function management are aware that these incident tickets remain open in the old KISAM-SM module. Management stated that they are in the process of conducting a verification to ensure that all open incident tickets in the old KISAM-SM module were input into the new module, and closing them when the issues have been addressed. The UNS function plans to complete the verification before the old KISAM-SM module is retired on September 30, 2019.

Many of these old incident tickets have been open well in excess of a year and may no longer need to be worked because the employee has left the IRS, the equipment is no longer in operation, or the originally reported incident is no longer an issue. Conducting a verification to ensure that all of the old incident tickets are migrated to the new KISAM-SM module may be an inefficient use of resources considering the original need may no longer be there. For those viable incident tickets on the old KISAM-SM module, we believe that an additional reminder to all affected employees to resubmit an incident ticket in the new KISAM-SM module would suffice. As of May 29, 2019, 1,213 incident tickets were still open in the old KISAM-SM module, the remainder being either an open ticket in the new KISAM-SM module or already resolved and closed.

Management Action: On July 9, 2019, the Director, Customer Service Support, sent an e-mail to managers with employees having currently open incident tickets in the old KISAM-SM module. The Director requested that all open incident tickets in the old KISAM-SM module be reviewed and appropriate actions taken, *i.e.*, close the open incident ticket and if necessary, open a ticket in the new KISAM-SM module, no later than July 15, 2019. To aid in this effort, the Director provided a newly developed dashboard in the old KISAM-SM module that can display multiple reports, including a report that provides a listing of all open incident tickets by group. The Director also requested Assistant Chief Information Officers to certify that his or her respective organization has taken appropriate actions to ensure a successful “clean-up” effort for the old KISAM-SM module and that any remaining open incident tickets can be part of a mass closure. As of July 30, 2019, all incident tickets that were open in the old KISAM-SM module have been closed.

Other performance goals are not being met

The IRS did not always meet its monthly incident management performance goals. We reviewed the incident management metrics captured from three main IRS reports,² the *EOps ITOCC [Information Technology Operations Command Center] Metrics Dashboard*, the *UNS Balanced Scorecard*, and the *UNS Operational Dashboard*. We compiled the incident management metrics from these three reports and identified 25 monthly performance goals that the IRS uses

² We did not review a fourth report, the monthly *Enterprise Services Performance Report*, because it does not provide performance goals.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

to manage its Incident Management program. See Appendix IV for an explanation of the incident management metrics.

For Fiscal Year 2018, the IRS only met its monthly performance goals more than 50 percent of the time for 12 of its 25 incident management metrics. Only seven of the 25 incident management goals were consistently met for 10 months or more during the fiscal year. Figure 2 provides a summary of the number of months in Fiscal Year 2018 that the IRS met/did not meet its performance goals.

Figure 2: Number of Months in Fiscal Year 2018 the IRS Met/Did Not Meet Monthly Performance Goals by Incident Management Metric

	Function	Incident Management Metric	Performance Goal	Months Performance Goal Met	Months Performance Goal Not Met	Not Applicable ³
1	UNS	<i>Call Abandonment</i>	13 percent or less	0	12	0
2	UNS	<i>Call Handle Time</i>	25 minutes or less	12	0	0
3	UNS	<i>Customer Satisfaction</i>	85 percent	1	11	0
4	UNS	<i>Customers per Deskside Technician</i>	200	12	0	0
5	UNS	<i>End User Systems and Services Percent on Time – Priority 3</i>	90 percent	10	2	0
6	UNS	<i>First Level Resolution</i>	60 percent	12	0	0
7	UNS	<i>Mean Time to Resolve – Priority 1</i>	4 hours	3	8	1
8	UNS	<i>Mean Time to Resolve – Priority 2</i>	8 hours	0	12	0
9	UNS	<i>Overage Tickets – Level 1</i>	10 percent or less	7	5	0
10	UNS	<i>Overage Tickets – Levels 2 - 4</i>	10 percent or less	1	11	0
11	UNS	<i>Overage Tickets – Overall</i>	10 percent	1	11	0
12	EOPs	<i>Percentage of Assessment Calls With Duration Under 30 Minutes</i>	95 percent	6	6	0
13	EOPs	<i>Percentage of Assessment Calls Within One Hour of Incident Open</i>	70 percent	12	0	0
14	EOPs	<i>Percent of Technical Service Restoration Team Calls Within One Hour of Assessment Call</i>	90 percent	10	2	0
15	UNS	<i>Request Fulfillment (20 work days)</i>	93 percent	1	11	0

³ Months for which there were no incidents reported for the metric category or there were no incidents to be measured.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

	Function	Incident Management Metric	Performance Goal	Months Performance Goal Met	Months Performance Goal Not Met	Not Applicable ³
16	UNS	<i>Resolution Timeliness</i>	87 percent	7	5	0
17	UNS	<i>Speed of Answer (Service Desk)</i>	8 minutes	0	12	0
18	UNS	<i>UNS Percent on Time – Level 1: Priority 1</i>	88 percent	3	5	4
19	UNS	<i>UNS Percent on Time – Level 1: Priority 2</i>	85 percent	7	5	0
20	UNS	<i>UNS Percent on Time – Level 1: Priority 3</i>	87 percent	12	0	0
21	UNS	<i>UNS Percent on Time – Level 1: Priority 4</i>	87 percent	6	6	0
22	UNS	<i>UNS Percent on Time – Levels 2 - 4: Priority 1</i>	88 percent	3	7	2
23	UNS	<i>UNS Percent on Time – Levels 2 - 4: Priority 2</i>	85 percent	2	10	0
24	UNS	<i>UNS Percent on Time – Levels 2 - 4: Priority 3</i>	87 percent	0	12	0
25	UNS	<i>UNS Percent on Time – Levels 2 - 4: Priority 4</i>	87 percent	0	12	0

Source: Treasury Inspector General for Tax Administration review of incident management metrics from the EOps ITOCC [Information Technology Operations Command Center] Metrics Dashboard, UNS Balanced Scorecard, and UNS Operational Dashboard between October 1, 2017, and September 30, 2018.

The Government Accountability Office’s *Standards for Internal Control in the Federal Government*⁴ provides that “Quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis.... Management uses the quality information to make informed decisions and evaluate the entity’s performance in achieving key objectives and addressing risks.”

EOps function and UNS function management stated that there are several reasons why they did not meet monthly performance goals. Resources are limited and, as a result, they have adjusted resource allocations continuously to meet as many service level agreements as possible. For example, when employees answer and work customer calls at the ESD, those same employees will be unable to work incident tickets, which results in delays in resolving tickets. Conversely, when employees are tasked with working incident tickets, those same employees will be unable to answer and work telephone calls at the ESD. As a result, the call abandonment rate will be higher.

⁴ Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Management also stated that the monthly performance goals are based upon negotiations between the Information Technology organization and business functions to provide specific levels of service. However, existing performance goals were based on more than twice the current staffing level, and are not realistic. These goals were established in Calendar Year 2013 and, while reviewed annually, have never been updated. Furthermore, during the KISAM-SM module upgrade, customers still with open incident tickets in the old KISAM-SM module were asked to recreate the same ticket in the new KISAM-SM module. This resulted in first-level support specialists and service providers not timely going back into the old KISAM-SM module and closing the incident tickets when the issues had been resolved.

It is important to resolve incident tickets within target resolution times to minimize the level of disruption to the IRS and its ability to consistently process taxpayer returns and further tax administration. It is also important to establish realistic monthly performance goals that are reflective of resources available for the Incident Management program. Without realistic performance goals, the IRS cannot truly measure against program objectives, effectiveness, and efficiency.

Recommendation

Recommendation 1: The Chief Information Officer should update incident management performance goals and renegotiate specific levels of service to better reflect current resource allocations.

Management's Response: The IRS agreed with this recommendation. The IRS will complete an evaluation of the current levels of service to determine the appropriate incident management performance goals in line with the business need(s).

Incident Management Metrics Are Not Consistently Used or Not Used at All

Based on the results of our analysis of incident management data, we sent a survey to employees who management identified as receiving one or more of the metric reports. We sent the survey to 69 employees (12 EOps function and 57 UNS function employees) and asked each employee to identify the report(s) received, the incident management metric(s) reviewed, and how the metric(s), if any, are used to manage their respective program or function. Of the 57 employees (7 EOps function and 50 UNS function employees) who responded, we made the following observations:



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

E Ops Function Employees

- 3 employees responded that they do not use the EOps function incident management report because they no longer work in the program or functional area.⁵
- 3 employees responded that they just do not use the report.
- 1 employee responded that the metrics in the incident management report are “descriptive,” *e.g.*, identify surges in work on a particular day and time, but does not believe the metrics provide the necessary information to make timely decisions to be effective.

UNS Function Employees

- 6 employees responded that they do not use UNS function incident management reports because they no longer work in the program or functional area.⁶
- 8 employees responded that they just do not use the reports.
- 36 employees responded that they use one or both of the reports.
 - 15 employees responded that they do not review the report(s) for specific metrics, but rather reviewed the report(s) overall on the “effectiveness of operations.”
 - 21 employees responded that they reviewed specific metrics in the report(s) to determine the effectiveness of the day-to-day operations for planning and decisionmaking. Some of the incident management metrics the employees cited using included: *Call Handle Time, Customer Satisfaction, First Level Resolution, Overage Tickets, Request Fulfillment (20 work days), Speed of Answer (Service Desk), UNS Percentage on Time, etc.* For example, one employee stated that the *Request Fulfillment (20 work days)* metric provides an overall monthly view of the organization’s progress against service level agreement requirements. This metric also provides the needed information to adjust and/or focus team resources in the areas that require more attention, *e.g.*, P1, P2, P3, and/or P4 incident tickets. When one or more of the metrics are not meeting performance goals, attention and resources can be directed towards the area not meeting the goal.

Internal Revenue Manual 2.148.2, *IT Support Services Management, Incident Management Process*, dated March 30, 2016, provides that the process owner is accountable to ensure that a process is fit for purpose. The process owner is responsible for the sponsorship, design, change management, and continual improvement of the process and its metrics. In turn, the process manager is responsible for the planning and coordination of all activities required to carry out, monitor, and report on the process. It also provides that management will regularly review

⁵ This is the *E Ops ITOCC [Information Technology Operations Command Center] Metrics Dashboard* report.

⁶ These are the *UNS Balanced Scorecard* and the *UNS Operational Dashboard* reports.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

quantifiable data related to different aspects of the incident management process in order to make informed decisions and take appropriate corrective action, if necessary.

While a number of employees receiving EOPs function or UNS function report(s) used some metrics to determine the effectiveness of the day-to-day operations for planning and decisionmaking, the majority of the others found that the report(s) only provided an overall assessment on the effectiveness of the Incident Management program or did not use them. Given that the incident management metrics were established in Calendar Year 2013 and never updated, it is important that metrics are established or updated so that they are reflective and usable by employees to help better manage the Incident Management program. Without usable metrics, the IRS cannot achieve program objectives, effectiveness, and efficiency.

Recommendation

Recommendation 2: The Chief Information Officer should update incident management performance metrics to better align with overall program objectives and expanded use in daily operations.

Management's Response: The IRS agreed with this recommendation. The IRS will complete an evaluation of incident management performance metrics to ensure alignment with program objectives and use in daily operations.

Better Documentation Would Improve Efficiency in Resolving Incident Tickets

Incident ticket resolution efficiency would improve with better documentation of incident assessments and actions taken to potentially help reduce the number of ticket reassignments. In addition, we believe that incident tickets with multiple reassignments provide indications of potential workflow inefficiencies, resulting from improper routing of the tickets. Figure 3 provides the number of incident tickets by frequency of reassignments and fiscal year.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Figure 3: Number of Incident Tickets by Frequency of Reassignments for Fiscal Years 2016 through 2018

Frequency of Reassignments	Fiscal Year ⁷		
	2016	2017	2018
0 Reassignment	233,804 (80.2 percent)	219,753 (81.3 percent)	221,818 (78.9 percent)
1 Reassignment	37,768 (13.0 percent)	32,980 (12.2 percent)	40,708 (14.5 percent)
2 Reassignments	11,038 (3.8 percent)	10,133 (3.8 percent)	13,519 (4.8 percent)
3 Reassignments	3,442 (1.2 percent)	2,724 (1.0 percent)	2,982 (1.1 percent)
4 Reassignments	3,112 (1.1 percent)	2,880 (1.1 percent)	1,246 (0.4 percent)
5 Reassignments	964 (0.3 percent)	626 (0.2 percent)	419 (0.1 percent)
6 Reassignments	654 (0.2 percent)	545 (0.2 percent)	222 (0.1 percent)
7 Reassignments	365 (0.1 percent)	267 (0.1 percent)	90 (< 0.1 percent)
8 Reassignments	185 (0.1 percent)	131 (< 0.1 percent)	47 (< 0.1 percent)
9 Reassignments	129 (< 0.1 percent)	93 (< 0.1 percent)	25 (< 0.1 percent)
10 and More Reassignments ⁸	167 (0.1 percent)	128 (< 0.1 percent)	26 (< 0.1 percent)
Total	291,628 (100 percent)	270,260 (100 percent)	281,102 (100 percent)

Source: Treasury Inspector General for Tax Administration review of incident tickets between October 1, 2015, and September 30, 2018, from IRS-provided data extracts of the KISAM-SM module.

To obtain a perspective of the extent of reassignments and sufficiency of documentation, we obtained and reviewed a judgmental sample⁹ of 16 closed incident tickets with four or more reassignments during Fiscal Year 2018. Based on our analysis of the documented actions performed in the *Activities* section of the incident tickets, we determined that seven of the 16 tickets may have had inefficiencies in working the incident between first-level support specialists and service providers. For example, one incident ticket was reassigned to various

⁷ The percentages do not equal 100 percent due to rounding.

⁸ The highest number of reassignments on one incident ticket for Fiscal Years 2016 through 2018 were 32, 29, and 25 reassignments, respectively.

⁹ A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

service providers 16 times, while another incident ticket was mostly reassigned back and forth between two service providers 12 times, including one reassignment back to a first-level support specialist. In both cases, documentation of the actions performed or reasons provided for the reassignment were minimal, if documented at all. Without proper and sufficient documentation of actions performed, we were unable to determine whether the large number of reassignments was due to inefficiencies in the workflow process or were actually necessary to resolve the incident.

The *Customer Service: Ticket Management Student Guide*, dated August 2, 2007, provides that an incident ticket should be assigned to the primary service provider responsible for providing service support. If assistance is required from another service provider to complete the request, that service provider should be identified, and the incident ticket should be reassigned to the most appropriate service provider that can resolve the incident or assist with the resolution. When reassigning an incident ticket, an accurate description should be updated in the *Activities* section as to why the ticket is reassigned and what, if any, actions have been taken prior to the reassignment. In addition, the UNS function's *Support Services Management User Guide*, dated July 31, 2016, provides that the first-level support specialist and each service provider involved with handling incidents must perform an investigation and diagnosis to determine the resolution of the incident. All actions performed by the service provider should be documented in the incident ticket so that a complete historical record of all activities is maintained at all times.

Incident tickets with a large number of reassignments may have resulted from poor documentation by first-level support specialists and service providers. A UNS function management official acknowledged that the lack of documentation of incident actions by personnel is an issue. The official stated that if the actions performed are not documented, the service provider will have to send the ticket back to the first-level support specialist or prior service provider for more details. Without proper documentation of actions performed, the next first-level support specialist or service provider working on the incident ticket may not know what work was performed or what still may be needed to resolve the issue. This can lead to multiple reassignments and inefficiency in working incident tickets.

Recommendation

Recommendation 3: The Chief Information Officer should ensure that all incident assessments and actions performed are documented in incident tickets to provide a complete historical record of all activities. This includes an updated description in the *Activities* section as to why the ticket is reassigned and what, if any, actions have been taken prior to the reassignment.

Management's Response: The IRS agreed with this recommendation. The IRS will update the business-wide ticket guidelines to focus on the activity description and reassignments documenting an incident history.



*Controls Should Be Strengthened to Ensure Timely
Resolution of Information Technology Incident Tickets*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness and efficiency of the processes and practices for resolving information technology incidents and reported problems for the IRS's tax administration systems.¹ To accomplish our objective, we:

- I. Evaluated the effectiveness and efficiency of the IRS's processes and practices for resolving incident tickets.
 - A. Identified and reviewed the IRS's policies, procedures, guidance, goals, and metrics for resolving information technology incidents and reported problems for the IRS's tax administration systems.
 - B. Conducted a walkthrough with ESD and Information Technology Operations Command Center personnel to determine the processes in place for resolving incident tickets. This included the recording, categorizing and prioritizing, investigating and diagnosing, resolving or escalating to a service provider, and closing of the ticket.
 - C. Assessed the IRS's processes and practices for resolving incident tickets.
 1. Obtained KISAM-SM data extracts of production incident tickets that were closed during Fiscal Years 2016 through 2018 and incident tickets that were still open at the time the data extracts were pulled.
 2. Evaluated the reliability of the KISAM-SM data extracts to help ensure that the data were reasonably complete and accurate. We verified the criteria used to create the reports, verified that all fields requested were received, and verified that the record counts equaled to what was expected. We determined that the data to be reliable for the purposes of this review.
 3. Analyzed the data extracts of closed and open incident tickets by fiscal year to determine the effectiveness and efficiency of the IRS's processes and practices for resolving incident tickets.
 - a. Determined whether incident tickets were resolved within the specified time frames based upon priority level.
 - b. Determined the frequency of incident tickets reassigned from the original service provider, and selected and reviewed a judgmental sample² of 16 incident

¹ See Appendix V for a glossary of terms.

² A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

tickets closed in Fiscal Year 2018 to determine if the number of reassignments was appropriate and properly documented. We selected a judgmental sample because we did not plan to project to the population.

- II. Determined whether the IRS is accurately capturing and reporting incident management metrics and effectively managing the Incident Management program.
 - A. Determined whether the IRS is accurately capturing and reporting incident management metrics.
 - 1. Identified and obtained the IRS's incident management metrics and goals for Fiscal Years 2016 through 2018.
 - 2. Interviewed Information Technology organization personnel responsible for working incident tickets to determine how the IRS calculates the metrics, including the types of raw data used in the calculation.
 - 3. Assessed whether the metrics provide a fair measurement of the program.
 - B. Determined whether the IRS is effectively using its metrics to manage the Incident Management program and meet its performance goals.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the Government Accountability Office's *Standards for Internal Control in the Federal Government*,³ Internal Revenue Manual 2.148.2, *IT Support Services Management, Incident Management Process*, dated March 30, 2016, as well as various IRS policies, procedures, and processes for managing the Incident Management program, reporting of incident management metrics, and the system used to record incident tickets, *e.g.*, the KISAM-SM module. We evaluated these controls by interviewing Information Technology organization personnel concerning the procedures and processes for incident management and reporting of incident metrics, analyzing KISAM-SM data extracts, reviewing a judgmental sample of incident tickets, and reviewing supporting documentation.

³ Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).



*Controls Should Be Strengthened to Ensure Timely
Resolution of Information Technology Incident Tickets*

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information
Technology Services)
Bryce Kisler, Director
Louis Lee, Audit Manager
Jason Rosenberg, Lead Auditor
Charlene Elliston, Senior Auditor



*Controls Should Be Strengthened to Ensure Timely
Resolution of Information Technology Incident Tickets*

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User and Network Services
Director, Enterprise Audit Management



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Appendix IV

Incident Management Metrics Defined

Incident Management Metric	Description
<i>Call Abandonment</i>	Measures the percentage of all calls in the ESD queue that are disconnected by the customer before reaching a first-level support specialist.
<i>Call Handle Time</i>	Measures the average amount of time it takes an ESD first-level support specialist to complete an inbound service call, including talk time, hold time, wrap-up time, voice messaging, and other.
<i>Customer Satisfaction</i>	Measures the monthly and fiscal year-to-date results of three survey questions using a scale of 1 to 5 (1 = very dissatisfied to 5 = very satisfied).
<i>Customers Per Deskside Technician</i>	Measures how many customers one deskside technician would support.
<i>End User Systems and Services Percent on Time – Priority 3</i>	Measures the timeliness of resolution against the standards contained in the master service level agreement. It includes both interactions and UNS function-worked incidents closed within a specified time period.
<i>First-Level Resolution</i>	Measures the percentage of information technology interactions closed at the first level, <i>i.e.</i> , by the ESD. It includes closed non-escalated interactions plus ESD-worked incidents and request tasks with a break out of telephone and non-telephone.
<i>Mean Time to Resolve – Priority 1</i>	Measures the average time it takes the UNS function to resolve P1 interactions and incidents.
<i>Mean Time to Resolve – Priority 2</i>	Measures the average time it takes the UNS function to resolve P2 interactions and incidents.
<i>Overage Tickets – Level 1</i>	The average daily percentage of all non-escalated interactions and all ESD-assigned incidents and request tasks open more than 30 days.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Incident Management Metric	Description
<i>Overage Tickets – Levels 2 – 4</i>	The average daily percentage of all non-escalated interactions and all other UNS function groups, except the ESD, assigned incidents, and request tasks open more than 30 days. ¹
<i>Overage Tickets – Overall</i>	The average daily percentage of all non-escalated interactions and all UNS function groups, including the ESD, assigned incidents, and request tasks open more than 30 days.
<i>Percentage of Assessment Calls With Duration Under 30 Minutes</i>	The percentage of the total number of assessment calls completed from start to finish in under 30 minutes.
<i>Percentage of Assessment Calls Within One Hour of Incident Open</i>	The average time elapsed between assessment call request and assessment call start.
<i>Percent of Technical Service Restoration Team Calls Within One Hour of Assessment Call</i>	The percentage of calls that are started within 60 minutes of the end of an assessment call that requested the Technical Service Restoration Team. ²
<i>Request Fulfillment (20 work days)</i>	Measures the timeliness of requests resolution against the historical standards contained in the master service level agreement.
<i>Resolution Timeliness</i>	Measures the overall ability of the UNS function to resolve all P1 through P4 interactions and UNS function-assigned incidents in accordance with the master service level agreement.
<i>Speed of Answer (Service Desk)</i>	Measures the average amount of time a customer waits in the queue before reaching an ESD first-level support specialist.

¹ The IRS was unable to further define the difference between Levels 2 through 4. A UNS management official stated that there is no reporting or general work difference between these levels.

² See Appendix V for a glossary of terms.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Incident Management Metric	Description
<i>UNS Percent on Time – Level 1</i>	Measures the timeliness of resolution for P1 through P4 incidents worked by the ESD against the standards contained in the master service level agreement. It includes both interactions and ESD-worked incidents.
<i>UNS Percent on Time – Levels 2 Through 4</i>	Measures the timeliness of resolution for P1 through P4 incidents closed by UNS function assignment groups other than the ESD.

Source: IM [Incident Management] Data Dictionary Cards; UNS Operational Dashboard – Data Dictionary Compilation, dated October 5, 2018; and UNS Balanced Scorecard – Data Dictionary Compilation, dated October 19, 2018.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Appendix V

Glossary of Terms

Term	Definition
Assessment Call	Designed to assist in incident resolution when a resolution cannot be determined after 30 minutes or more of an incident record creation.
Calendar Year	The 12-consecutive-month period ending on December 31.
Change Management	The transition of a changed or new product through development to deployment into the current production environment with minimum disruption to users. This can occur in a number of ways including, but not limited to: 1) implementation of a change to a product baseline, 2) establishing a new product baseline, or 3) a change to a service level agreement.
First-Level Support Specialist	The initial customer contact and is responsible for recording, classifying and prioritizing, investigating and diagnosing, resolving or forwarding, and closing incidents as well as monitoring their progress.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins October 1 and ends on September 30.
Government Accountability Office	The audit, evaluation, and investigative arm of Congress that provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions.
Hardware	The physical parts of a computer and related devices; it includes motherboards, hard drives, monitors, keyboards, mice, printers, and scanners.
Incident Management Life Cycle	The various stages in the life of an information technology service or incident. The expanded incident management life cycle includes detection, diagnosis, repair, recovery, and restoration.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Term	Definition
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Knowledge Incident/Problem Service Asset Management	A system that maintains the complete inventory of information technology and non-information technology organizational assets, and computer hardware and software. It is also the reporting tool for problem management with all IRS-developed applications and shares information with the ESD.
Metric	Something that is measured and reported to help manage a process, information technology service, or activity.
Password	A secret word or code used to serve as a security measure against unauthorized access to data. It may be used to log on to a computer, network, or website or to activate newly installed software in the computer.
Retire	Withdrawal or permanent removal of an application, information technology service, <i>etc.</i> , from use in a live environment.
Service Level Agreement	A document that describes the minimum performance criteria a provider promises to meet while delivering a service, typically also setting out the remedial action and any penalties that will take effect if performance falls below the promised standard.
Service Manager	An application for reporting and managing problems with all applications developed by the IRS.
Service Provider	Provides information technology services to internal and external customers.
Software	A general term that describes computer programs and consists of lines of code written by computer programmers that have been compiled into a computer program.
Technical Service Restoration Team	A team of subject matter experts that analyzes and resolves system outages or develops and implements a workaround for escalated incidents.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Appendix VI

Management's Response to the Draft Report



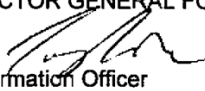
CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

AUG 20 2019

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:

Nancy A. Sieger 
Acting Chief Information Officer

SUBJECT:

Draft Audit Report – Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets (Audit #201820015) (e-trak # 2019-14446)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss our concerns. We are pleased that your report acknowledged the steps the Internal Revenue Service (IRS) has taken to improve our incident management program. We agree it's important to resolve incidents quickly to minimize any disruption to the tax operations. As your report highlights, over the last three years our percentage of P1 tickets addressed within our established target of four hours has been 62.9% or higher, 75.8% or higher for the P2 tickets are within the target of eight hours, 70.1% of the P3 tickets are within the target of two business days, and 68.1% or better of the P4s are with the target of four business days. While these resolutions percentages have varied, we believe we have made progress and will continue to do so.

Your report highlights the focused efforts our teams are making to close all the open tickets in the legacy ticketing system. Due to these efforts we are pleased to confirm that we have zero remaining open tickets in KISAM-SM model 9.41.

With thousands of IRS employees who depend on Information Technology, we continue to focus on how best to resolve incidents impacting employees quickly and efficiently. For example, we have a successful practice of standing up walk-in centers to help employees in large sites when there is a larger number of impacted employees. We acknowledge that resource constraints have impacted our ability to meet IRS performance goals for targeted ticket resolution times. We are working on improvements to better service our customers, including hiring additional support personnel to answer calls and provide hands-on support, as well as providing alternative avenues to support our customers. We believe these efforts will help IRS better meet our performance objectives.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

2

IRS recognizes the importance of constant improvements and agrees with all three of your recommendations in the audit report. For example, we agree with

recommendation three to ensure all incidents are fully documented. This best practice is especially helpful in the very small number of incidents that are reassigned. As figure three from the report highlights, roughly 80% of incidents are not reassigned and less than 3% of the incidents are reassigned three or more times.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Candace Joines at (901) 546-2958.

Attachment



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Attachment

Draft Audit Report – Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets (Audit #201820015)

RECOMMENDATION #1: The Chief Information Officer should update incident management performance goals and renegotiate specific levels of service to better reflect current resource allocations.

CORRECTIVE ACTION #1: We agree with this recommendation. IRS will complete an evaluation of the current levels of service to determine the appropriate incident management performance goals in line with the business need(s).

IMPLEMENTATION DATE: February 15, 2021

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

RECOMMENDATION #2: The Chief Information Officer should update incident management performance metrics to better align with overall program objectives and expanded use in daily operations.

CORRECTIVE ACTION #2: We agree with this recommendation. The IRS will complete an evaluation of incident management performance metrics to ensure alignment with program objectives and use in daily operations.

IMPLEMENTATION DATE: April 15, 2021

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

RECOMMENDATION #3: The Chief Information Officer should ensure that all incident assessments and actions performed are documented in incident tickets to provide a complete historical record of all activities. This includes an updated description in the Activities section as to why the ticket is reassigned and what, if any, actions have been taken prior to the reassignment.

CORRECTIVE ACTION #3: We agree with this recommendation. The IRS will update the business-wide ticket guidelines to focus on the activity description and reassignments documenting an incident history.



Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets

Attachment

Draft Audit Report – Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets (Audit #201820015)

IMPLEMENTATION DATE: September 15, 2021

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User and Network Services

CORRECTIVE ACTION MONITORING PLAN: We will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.