# TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

# The End-User Incident Management Process Can Be Improved

September 26, 2022

Report Number: 2022-20-053

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

# HIGHLIGHTS: The End-User Incident Management Process Can Be Improved

**Final Audit Report issued on September 26, 2022** **Report Number 2022-20-053**

## Why TIGTA Did This Audit

The Information Technology organization's User and Network Services (UNS) function is responsible for handling incident tickets involving end-users. Its Customer Service Support Directorate manages the Enterprise Service Desk, which provides an option for users to report information technology work stoppage issues, and its Enterprise Field Operations Directorate manages Deskside Operations, which works to resolve information technology incidents and fulfills requests for information technology services. During Fiscal Year 2021, 94,549 incident tickets were closed.

This audit was initiated to determine whether the Information Technology organization is effectively and efficiently managing end-user computer incidents.

## Impact on Tax Administration

An incident is an unplanned interruption to or a reduction in the quality of an information technology service. It is important to resolve incident tickets within established performance goals to minimize the level of disruption to the IRS and its ability to consistently process taxpayer returns and further tax administration.

## What TIGTA Found

Management of end-user incident tickets needs improvement. A review of 94,549 incident tickets closed during Fiscal Year 2021 and 1,567 incident tickets that remained open as of November 17, 2021, determined that meaningful cause codes, *i.e.*, codes intended to answer the question, "Why did the incident happen?", were not always selected. There were 79,644 incident tickets that had a cause code of *Not Listed*, *No List Defined*, *Other*, *General Failure*, or a cause code was not selected. In addition, a review of 35 closed incident tickets with four or more reassignments determined that the reassignments for approximately one-third of the incident tickets were inappropriate, as they were reassigned multiple times to the same wrong assignment group or were reassigned without completing required tasks. For nearly another one-third of incident tickets, a determination of whether the reassignments were appropriate could not be made because there was insufficient documentation. Furthermore, a review of 30 closed incident tickets determined that 16 tickets did not include the user's concurrence that the issue was resolved and that the ticket could be closed.

The *UNS Balanced Scorecard* and the *UNS Operational Dashboard Report* provide 21 incident management metrics that the UNS function uses to manage its incident management program. The IRS did not always meet its monthly incident management performance goals. For Fiscal Year 2021, only five of the 21 incident management metrics were met consistently for six months or more, including three metrics, *i.e.*, the *Call Handle Time* metric, the *First Level Resolution* metric, and the *UNS Percent on Time – Level 1: Priority 3* metric, that were met every month in Fiscal Year 2021. Five metrics were met from two to five months.

However, 11 incident management metrics were not met once in Fiscal Year 2021. For example, the *UNS Percent on Time – Levels 2 – 4: Priority 1* metric, which measures the timeliness of resolving Priority 1 incidents within four hours, and the *Customer Satisfaction* metric were not met. In addition, two key industry metrics are not being captured.

## What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that incident ticket handling requirements are followed (including selecting specific codes related to the issues, documenting actions taken including the reason for reassignments, and obtaining user concurrence before closing the incident ticket) and evaluate the *Agent Utilization* metric.

The IRS agreed with the recommendations. The IRS plans to include training on the new coding and documentation requirements and update the incident management documentation, and research and evaluate the *Agent Utilization* metric's application and value.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

**U.S. DEPARTMENT OF THE TREASURY**

**WASHINGTON, D.C. 20024**

September 26, 2022

**MEMORANDUM FOR:** COMMISSIONER OF INTERNAL REVENUE

**FROM:** Heather M. Hill
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – The End-User Incident Management Process Can Be Improved (Audit # 202220013)

This report presents the results of our review to determine whether the Information Technology organization is effectively and efficiently managing end-user computer incidents. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Modernizing IRS [Internal Revenue Service] Operations*.

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

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).

# Table of Contents



## Appendices

# Background

The Information Technology organization's User and Network Services (UNS) and Enterprise Operations functions are responsible for the information technology incident management process. The UNS function is responsible for handling incident tickets involving end-users, while the Enterprise Operations function is responsible for handling incident tickets involving servers.

Specifically, the UNS function collaborates with Information Technology Service Partners to make content available through an *IT4U* interactive self-help website that provides Internal Revenue Service (IRS) employees (hereafter referred to as users) with resources to help them troubleshoot and resolve common information technology issues. For example, a BOT[1] named *Winnie* provides answers to users with Windows 10 questions, and a webchat feature allows users to report issues that they are unable to resolve themselves. In addition, the UNS function's Customer Service Support Directorate manages the Enterprise Service Desk (ESD), which provides an option for users to report information technology work stoppage issues. Also, within the UNS function, the Enterprise Field Operations Directorate manages Deskside Operations.[2] Deskside Operations is comprised of service providers, *i.e.*, employees, who are available to resolve information technology incidents and fulfill requests for information technology services, *e.g.*, on-site user, walk-in center, and user training support.

The Enterprise Operations function's Information Technology Operations Command Center manages the restoration of service to users during server outages and performs root cause analyses of server incidents and problems. It aims to ensure that high-priority incidents are being handled in a timely fashion.

## Incident management

An incident is an unplanned interruption to or a reduction in the quality of an information technology service. A user, service desk operator, service provider, or event monitoring software program can initiate an incident ticket. A user can initiate an incident ticket by calling the ESD, initiating an *IT4U* webchat session, or using the *OS GetServices* application.[3] A service desk operator can initiate an incident ticket when a user's issue cannot be resolved on the initial call, while a service provider can initiate an incident ticket when a user needs on-site support. In addition, event monitoring software can automatically generate an incident ticket when it detects the occurrence of predefined events.

The incident management process is designed to restore service operations 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. The goal of incident management is to have a process that is predictable, stable, and consistently operating at target levels of performance.

[1] See Appendix IV for a glossary of terms.

[2] The Enterprise Field Operations Directorate also manages Telecommunications Operations.

[3] *OS GetServices* is an online application that allows users to submit requests for information technology services.

## Master Service Level Agreement (MSLA)[4]

The annual MSLA establishes the target resolution times for resolving incidents based upon the priority level of the incident ticket. The priority level is used to identify the relative importance of an incident and is based on impact and urgency. There are four priority levels for incident tickets.

- Priority 1 – A severe mission-critical work stoppage impacting multiple internal or external users, services to taxpayers, or safety or health. The target resolution time is four hours.
- Priority 2 – A potential work stoppage that could have a direct impact on services to taxpayers or if its scope is multiuser and there is no workaround. The target resolution time is eight hours.
- Priority 3 – A work stoppage for one user with no workaround. The target resolution time is two business days.
- Priority 4 – A noncritical incident in which it is not a work stoppage and there is a workaround. The target resolution time is four business days.

## Knowledge Incident/Problem Service Asset Management (KISAM) Tool[5]

The KISAM tool is a commercial off-the-shelf software tool used by the UNS and Enterprise Operations functions to track and respond to interactions, incidents, problems, and changes. The Enterprise Operations function configures and manages the KISAM tool. Within the KISAM tool, the IRS uses many of the 10 available components, including interaction management, incident management, problem management, change management, request fulfillment, knowledge management, and service catalog.[6]

- Interaction Management component – used by service desk operators to document and track initial calls.
- Incident Management component – used by users, service desk operators, and service providers to submit and manage incident tickets.
- Problem Management component – used by service providers to document the root cause of a problem, workarounds, known errors, and permanent solutions.
- Change Management component – used by service providers to support the process of requesting, managing, approving, and controlling changes that modify the organization's infrastructure.
- Request Fulfillment component – used by users, service desk operators, and service providers to manage user requests for products and services.

[4] Dated August 2020. It is a binding mutual agreement between the Information Technology organization and the business units regarding information technology responsibilities and the services that will be provided.

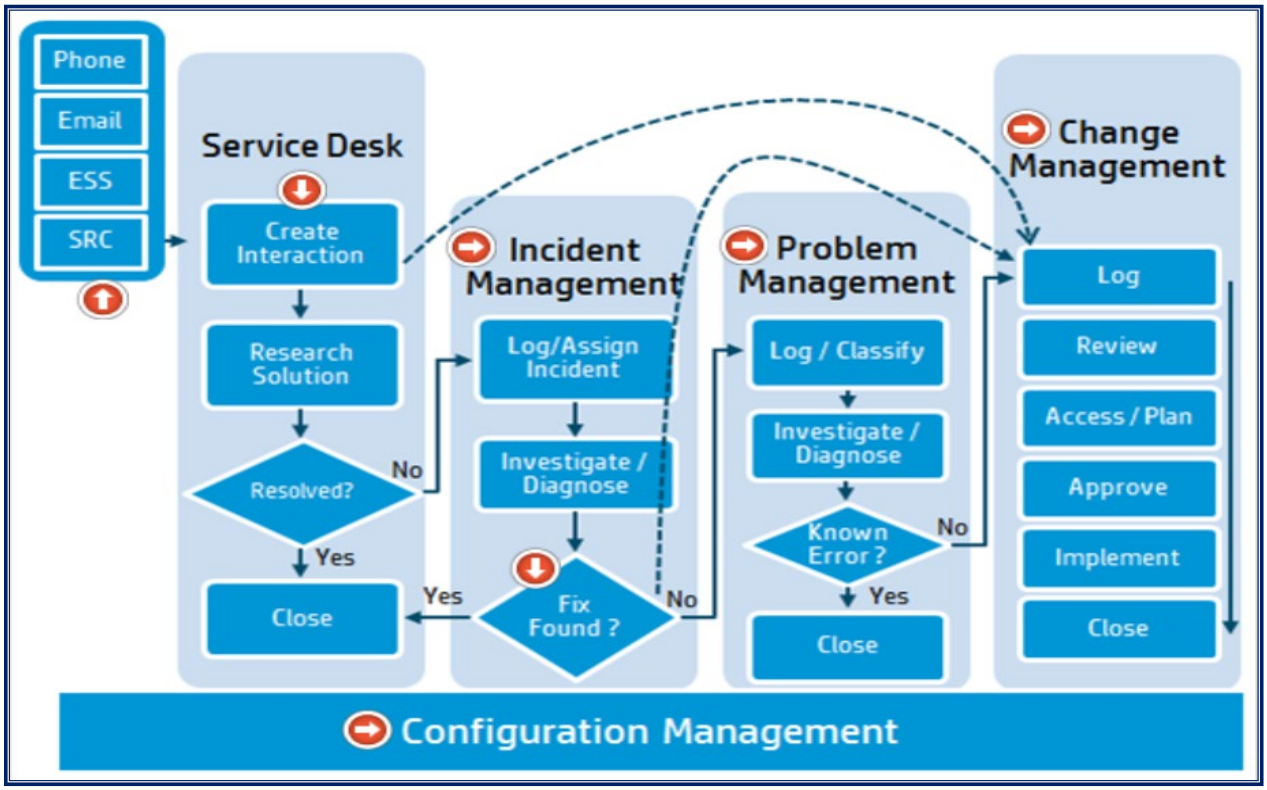
[5] The ServiceNow® IT [Information Technology] Service Management tool is scheduled to replace the KISAM tool in Fiscal Year 2023. The new tool is cloud-based and uses automated workflows, artificial intelligence, machine learning, and natural language processing agent chatbots.

[6] The remaining three components include scheduled maintenance, self-service ticketing, and service level management.

- Knowledge Management component – used by users, service desk operators, and service providers to search, update, and author knowledge articles that document ways to address and resolve incidents and problems.
- Information Technology Service Catalog component – provides a list of information technology services that the Information Technology organization offers to the enterprise.

The Interaction Management, Incident Management, Problem Management, and Change Management components all interact with each other when a user identifies an information technology issue. When a user calls the ESD initiating an interaction, the Interaction Management component starts the process. If the service desk operator is able to resolve the issue or provide a workaround, the issue is documented, resolved, and closed as an interaction in the Interaction Management component. If the service desk operator is unable to resolve the issue or provide only a temporary fix, *e.g.*, a workaround, it is escalated from an interaction to an incident, assigned to a service provider, and documented in the Incident Management component. If the service provider is able to resolve the incident with a known solution, the incident is closed. If the solution was not previously identified and the service provider is able to find a permanent fix, the fix is documented in a knowledge article and a change request may be submitted to the Change Management component. However, if the service provider is unable to resolve the incident, the incident is closed, documented as a problem ticket, and tracked in the Problem Management component. Figure 1 presents the relationship among the KISAM tool components.

**Figure 1: Workflow of KISAM Tool Components**




*Source: Micro Focus' Adoption Readiness Tool, Service Manager 9.60, Introduction, training document, dated 2020. ESS = Employee Self-Service and SRC = Service Request Catalog.*

# Results of Review

## Management of End-User Incident Tickets Needs Improvement

The incident management process involves five activities to help ensure that the process is predictable, stable, and consistently performed. The five activities include:

1. Recording – The service desk operator verifies the user's information, records the initial description of the incident, and links the incident ticket to any related problem tickets and known errors. If event monitoring software detects an incident, an incident ticket is automatically created in the KISAM tool.
2. Categorizing and Prioritizing – The service desk operator categorizes the incident ticket based upon the incident's description, knowledge articles, and the MSLA. The service desk operator determines the incident's priority based upon its impact and urgency. Impact is a measure of the number of users affected, and urgency is a measure of the work stoppage caused by the incident.
3. Investigating and Diagnosing – The service desk operator begins diagnosing the incident by researching the knowledge articles that could explain how to resolve the incident. If knowledge articles are not found, the incident is identified as a candidate for the knowledge database. Diagnosing the incident is considered complete once an incident ticket is associated with a knowledge article, an incident ticket is linked to another existing incident ticket for the same issue, or the incident is routed to a service provider.
4. Resolving and Dispatching – The incident may be resolved by the service desk operator or assigned, dispatched, and resolved by any of approximately 1,600 service provider assignment groups. This activity is completed once the incident is resolved.
5. Closing – An incident is closed once a permanent workaround has been identified, a service is restored, a problem ticket has been opened to research the root cause, or the user cancels the incident ticket. During the closure activity, the service desk operator or service provider reviews the incident details, obtains the user's concurrence that the incident is resolved, and then the incident ticket can be closed. The user is sent a User Satisfaction Survey.

The UNS function provided, from the KISAM tool, a data extract of incident tickets that were closed during Fiscal Year 2021 as well as incident tickets that remained open and being worked as of November 17, 2021. We used the *Assignment* field and identified 96,116 (94,549 closed and 1,567 open) incident tickets that were worked by the ESD or Deskside Operations.[7] We analyzed the closed and open incident ticket data and identified an issue with incident tickets being categorized without meaningful cause codes. The cause code on an incident ticket is intended to answer the question, "Why did the incident happen?" In addition, we analyzed closed incident tickets and identified that tickets reassigned to service providers were resulting in inefficiencies, and incident tickets were being closed without obtaining user concurrence.

[7] Telecommunication incident tickets were excluded from the review because they do not pertain to information technology services.

The effectiveness and efficiency of the incident ticket handling process is impacted when incident tickets are categorized with nonspecific cause codes, reassigned multiple times without sufficient justification, and closed without obtaining user concurrence. Inaccurate or incomplete data make it difficult for the IRS to identify trends in incident management and failure to obtain user concurrence may result in closing incident tickets prematurely or untimely.

## Meaningful cause codes were not always selected

With 185 different cause codes, service desk operators and service providers select the appropriate cause code when they categorize an incident ticket. Our analysis of the closed and open incident tickets determined that specific cause codes are not being selected. Specifically, we identified 79,644 (82.9 percent) incident tickets that had a cause code of *Not Listed*, *No List Defined*, *Other*, *General Failure*, or a cause code was not selected. Figure 2 provides a summary of our analysis.

**Figure 2: Distribution of Closed and Open Incident Ticket Cause Codes**

| Cause Codes | Number of Incident Tickets | Percentage of Incident Tickets[8] |
|---|---|---|
| *Not Listed*[9] | *61,158* | 63.6% |
| *No List Defined* | *7,847* | 8.2% |
| *Other* | *5,213* | 5.4% |
| *General Failure* | *4,038* | 4.2% |
| *Configuration Error* | *3,957* | 4.1% |
| *Monitor* | *1,648* | 1.7% |
| No Cause Code Selected[10] | *1,388* | 1.4% |
| Remaining Cause Codes[11] | *10,867* | 11.3% |
| Total | *96,116* | 99.9% |

*Source: Treasury Inspector General for Tax Administration's (TIGTA) review of incident tickets closed during Fiscal Year 2021 and incident tickets that remained open as of November 17, 2021, from the KISAM tool.*

According to a KISAM tool knowledge article, *Cause Code Definitions (Oct. 2019)*, a cause code is mandatory for all incident tickets. In addition, UNS function training material, *KISAM (Sept. 2021)*, states that the cause code of *Not Listed* or *Other* should not be used because they do not provide useful information. While not specifically identified, we believe that *General Failure* also does not provide useful information.

[8] The percentages do not add up to 100 percent due to rounding.

[9] *Not Listed* and *No List Defined* are cause codes that mean an appropriate cause code was not available. UNS function management stated that *Not Listed* and *No List Defined* have the same meaning.

[10] The IRS did not make a cause code tool available until November 2020. These incident tickets potentially include tickets closed prior to the availability of the cause code tool and open tickets still being worked.

[11] The remaining 179 cause codes each represents a small percentage of the total cause code population. They are collectively reported here to provide perspective and context.

## Incident ticket reassignments were not always justified or appropriately reassigned

An incident ticket is reassigned when an incident cannot be resolved by a particular service provider or has been incorrectly assigned. An incident ticket with multiple reassignments is an indicator of potential workflow inefficiencies, resulting from the improper assignment of the ticket. Figure 3 provides the number of closed and open incident tickets by frequency of reassignments.

**Figure 3: Closed and Open Incident Tickets by Frequency of Reassignments**

| Number of Reassignments | Number of Incident Tickets |
|---|---|
| 0 Reassignment | 76,695 |
| 1 Reassignment | 10,899 |
| 2 Reassignments | 6,470 |
| 3 Reassignments | 1,168 |
| 4 Reassignments | 545 |
| 5 Reassignments | 160 |
| 6 Reassignments | 83 |
| 7 Reassignments | 37 |
| 8 Reassignments | 38 |
| 9 Reassignments | 7 |
| 10 or More Reassignments | 14 |
| Total | 96,116 |

*Source: TIGTA's review of incident tickets closed during Fiscal Year 2021 and incident tickets that remained open as of November 17, 2021, from the KISAM tool.*

To obtain a perspective of the reassignments and sufficiency of documentation, we selected and reviewed a judgmental sample[12] of 35 closed incident tickets, each having four or more reassignments. We reviewed the actions documented in the *Activities* section of the incident tickets and determined that 28 of the 35 incident tickets contained at least one reassignment that did not have a documented justification. The remaining seven incident tickets included justifications for the reassignments.

Further analysis of the 35 closed incident tickets selected for review determined that the reassignments for approximately one-third of the tickets were inappropriate, as they were reassigned multiple times to the same wrong assignment group or were reassigned without completing required tasks. For nearly another one-third of incident tickets, we were unable to make a determination whether the reassignments were appropriate because there was insufficient documentation. Reassignments for the remaining 13 incident tickets appeared appropriate.

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

In Fiscal Year 2019, we reported a similar finding.[13] We recommended that all incident assessments and actions performed are documented in incident tickets to provide a complete historical record of all activities, including a description as to why the ticket was reassigned and what actions, if any, needed to be taken. In response to the report, the Information Technology organization updated UNS and Enterprise Operations functions incident ticket guidelines.

Internal Revenue Manual 2.148.2, *IT [Information Technology] Support Services Management, Incident Management Process*,[14] states that when an incident ticket is reassigned, it should be updated to provide a written justification indicating why the ticket needs to be reassigned and what actions the service provider needs to perform.

## User concurrence was not obtained

We reviewed a second judgmental sample of 30 closed incident tickets to determine whether service desk operators and service providers properly obtained user concurrence prior to closing the incident tickets. Of the 30 closed incident tickets, 14 tickets included the user's concurrence that the issue was resolved and that the ticket could be closed. Sixteen closed incident tickets did not contain the user's concurrence.

Internal Revenue Manual 2.148.2 states that service providers are responsible for working with the users, documenting steps taken to resolve the incident tickets, escalating incident tickets to management as needed, and closing the incident tickets. The manual also states that during the incident ticket closure process, service desk operators and service providers must confirm with the user that the incident has been resolved or the service has been restored.

UNS function management attributed the issues we identified related to the use of meaningless cause codes, inappropriate incident ticket reassignments, and premature closure of incident tickets to staffing shortages and the Coronavirus Disease 2019 pandemic-related increases in demand. Management stated that during Fiscal Year 2021, they were presented with extraordinary challenges due to the pandemic. Because the majority of employees worked remotely, the UNS function experienced higher call volumes without corresponding staff increases. Management also stated that they are working to improve these ticket handling practices through new knowledge articles reinforcing documentation requirements and addressing them with personnel through additional training.

**Recommendation 1:** The Chief Information Officer should ensure that incident ticket handling requirements are followed including selecting specific codes related to the issues, documenting actions taken including the reason for reassignments, and obtaining user concurrence before closing the incident ticket.

**Management's Response:** The IRS agreed with this recommendation. The IRS will include training on the new coding and documentation requirements and update the incident management documentation.

[13] TIGTA, Report No. 2019-20-055, *Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets* (Sept. 2019).

[14] Dated May 11, 2020.

## Incident Management Performance Goals Are Not Being Met

We reviewed 21 incident management metrics from the *UNS Balanced Scorecard* and the *UNS Operational Dashboard Report* that the UNS function uses to manage its incident management program. For Fiscal Year 2021, only five of the 21 incident management metrics were met consistently for six months or more, including three metrics, *i.e.*, Metric 2, *Call Handle Time*, which measures the average time it takes a service desk operator to complete an inbound service call; Metric 5, *First Level Resolution*, which measures the percentage of interactions closed by the ESD; and Metric 16, *UNS Percent on Time – Level 1: Priority 3*, which measures the timeliness of resolution for Priority 3 interactions and incidents worked by the ESD, that were met every month in Fiscal Year 2021. Five metrics were met from two to five months. However, 11 incident management metrics were not met once in Fiscal Year 2021.

A similar finding was reported in the TIGTA report mentioned previously. We recommended that incident management performance goals be updated and specific levels of service be renegotiated to better reflect current resource allocations. In response to the report, the UNS function evaluated its incident management performance metrics, determined they were aligned with program objectives, and did not update the performance goals. Figure 4 provides a summary of the number of months in Fiscal Year 2021 that the UNS function met or did not meet its incident management performance goals. Appendix II provides definitions of the incident management metrics.

**Figure 4: Fiscal Year 2021 UNS Function Incident Management Performance**

| | Incident Management Metric (Source of Performance Goal) | Performance Goal | Months Performance Goal Met | Months Performance Goal Not Met | Not Applicable[15] |
|---|---|---|---|---|---|
| 1 | *Call Abandonment (UNS Function Executives)* | 13% or less | 2 | 10 | 0 |
| 2 | *Call Handle Time (UNS Function Executives)* | 25 minutes or less | 12 | 0 | 0 |
| 3 | *Customer Satisfaction (UNS Function Executives)* | 85% | 0 | 12 | 0 |
| 4 | *Customer per Deskside Technician (UNS Function Executives)* | 200 customers | 0 | 12 | 0 |
| 5 | *First Level Resolution (UNS Function Executives)* | 60% | 12 | 0 | 0 |
| 6 | *Mean Time to Resolve – Priority 1 (MSLA)* | 4 hours | 0 | 8 | 4 |
| 7 | *Mean Time to Resolve – Priority 2 (MSLA)* | 8 hours | 0 | 12 | 0 |
| 8 | *Overage Tickets – Priority Level 1*[16] *(UNS Function Executives)* | 10% or less | 5 | 7 | 0 |

[15] Months for which there were no incidents reported for the metric.

[16] Level 1 refers to incident tickets worked by ESD personnel.

| | Incident Management Metric (Source of Performance Goal) | Performance Goal | Months Performance Goal Met | Months Performance Goal Not Met | Not Applicable[15] |
|---|---|---|---|---|---|
| 9 | *Overage Tickets – Priority Levels 2–4*[17] *(UNS Function Executives)* | 10% or less | 0 | 12 | 0 |
| 10 | *Overage Tickets – Overall (UNS Function Executives)* | 10% | 0 | 12 | 0 |
| 11 | *Request Fulfillment (20 business days) (UNS Function Executives)* | 93% | 0 | 12 | 0 |
| 12 | *Resolution Timeliness (UNS Function Executives)* | 87% | 7 | 5 | 0 |
| 13 | *Speed of Answer (Service Desk) (UNS Function Executives)* | Less than 8 minutes | 0 | 12 | 0 |
| 14 | *UNS Percent on Time – Level 1: Priority 1 (MSLA)* | 88% | 2 | 1 | 9 |
| 15 | *UNS Percent on Time – Level 1: Priority 2 (MSLA)* | 85% | 11 | 1 | 0 |
| 16 | *UNS Percent on Time – Level 1: Priority 3 (MSLA)* | 87% | 12 | 0 | 0 |
| 17 | *UNS Percent on Time – Level 1: Priority 4 (MSLA)* | 87% | 5 | 7 | 0 |
| 18 | *UNS Percent on Time – Levels 2–4: Priority 1 (MSLA)* | 88% | 0 | 8 | 4 |
| 19 | *UNS Percent on Time – Levels 2–4: Priority 2 (MSLA)* | 85% | 0 | 12 | 0 |
| 20 | *UNS Percent on Time – Levels 2–4: Priority 3 (MSLA)* | 87% | 0 | 12 | 0 |
| 21 | *UNS Percent on Time – Levels 2–4: Priority 4 (MSLA)* | 87% | 5 | 7 | 0 |

*Source: TIGTA's review of incident management metrics from the UNS Balanced Scorecards and UNS Operational Dashboard Reports between October 1, 2020, and September 30, 2021.*

It is important to resolve incident tickets within established performance goals to minimize the level of disruption to the IRS and its ability to consistently process taxpayer returns and further tax administration. By failing to meet its established incident management performance goals, there may be an increased level of disruption to users. For example, Metric 18, *UNS Percent on Time – Levels 2–4: Priority 1*, measures the timeliness of service providers resolving Priority 1 incidents within four hours. While the goal is 88 percent of Priority 1 incident tickets being resolved within four hours, the UNS function did not achieve the performance goal in any of the eight months in Fiscal Year 2021 for which there were incidents reported for the metric. In addition, the UNS function did not achieve the Metric 3, *Customer Satisfaction*, performance goal of 85 percent during any month in Fiscal Year 2021. The user satisfaction results are based upon the responses to three survey questions that are sent to every user after the UNS function resolves an incident ticket. The survey questions include reviews on the overall level of service

[17] Levels 2–4 refer to incident tickets worked by UNS function assignment groups other than the ESD.

provided, the speed of the response received, and the level of communication. The user can answer the survey questions on a scale from 1 to 5, with 1 being very unsatisfied and 5 being very satisfied. When responding to the survey questions, users also have the option to provide comments, which the UNS function keeps track of and categorizes them as either compliments or complaints. The sum of the satisfied and very satisfied responses (4 and 5, respectively) for the month reported is divided by the total monthly valid responses to calculate the monthly user satisfaction percentage.

## Two key industry metrics are not being captured

The UNS function does not capture two key industry metrics established by the Service Desk Institute, a worldwide professional organization for the information technology service and support industry. Without capturing these key industry metrics, the IRS may not have a complete measure of its incident management program. We compared the key industry metrics to metrics captured and measured by the UNS function and found that the *Cost per Contact* and *Agent Utilization* metrics are not captured. *Cost per Contact* measures how efficiently the service desk is conducting its business by taking the annual operating expense and dividing it by the annual contact volume. *Agent Utilization* is the average time that an agent spends handling both inbound and outbound contacts per month, divided by the total number of hours worked in a given month. This metric measures labor efficiency.

The Government Accountability Office's *Standards for Internal Control in the Federal Government* [18] states that "management should use quality information to achieve the entity's objectives," and the information should be "appropriate, current, complete, accurate, accessible, and provided on a timely basis." The MSLA establishes the performance goals for 10 of the 21 incident management metrics, *as previously annotated in Figure 4*. The UNS function's Service Planning and Improvement Directorate provides the data for the metrics and analytics within the UNS function. The remaining 11 performance goals are established by UNS function executives and documented in the Service Planning and Improvement Directorate's data dictionary.[19] In addition, the Service Desk Institute identifies seven key performance indicators for service desks. The key performance indicators include: 1) *Cost per Contact,* 2) *User Satisfaction,* 3) *Agent Utilization,* 4) *First Contact Resolution Rate,* 5) *First Level 1 Resolution Rate,* 6) *Agent Satisfaction,* and 7) *Agent Service Desk Performance*.

UNS function management stated that they did not meet their performance goals in Fiscal Year 2021 due to the impact of the Coronavirus Disease 2019 pandemic. The pandemic caused employees to have to work remotely, leading to an increase in call volume without an increase in staffing to answer the calls and work the incidents. UNS function management also stated that the Enterprise Field Operations Directorate tried to provide its services remotely, but when this was unsuccessful, its personnel had to schedule a time to resolve the incident in person, at the user's convenience. Booking appointments around the user's schedule led to many incident tickets not meeting target resolution times.

UNS function management acknowledged that they do not capture the *Cost per Contact* and *Agent Utilization* metrics. Management stated that they do not capture the *Cost per Contact* metric because the IRS does not maintain a cost accounting system that would easily provide

[18] Dated September 2014.

[19] A data dictionary includes attributes such as data type, size, allowed values, default values, and constraints.

the data needed and that collecting the data manually exceeded the value provided in measuring the metric. While the UNS function does not specifically capture the *Agent Utilization* metric, UNS function management stated that other productivity metrics are being captured in the *UNS Balanced Scorecard* and the *UNS Operational Dashboard Report* that include, for example, Metric 13 *Speed of Answer (Service Desk)* and Metric 2 *Call Handle Time*. Management also stated that other productivity metrics are captured but not in these two reports. Examples include the *Service Level (Phone)* metric, which measures the percentage of calls service desk operators answer within five minutes, by calculating the total number of incoming calls answered and abandoned within five minutes divided by total calls, and the *Productivity* metric, which measures the productivity of service desk operators, by calculating the total number of calls answered divided by the total log on time. UNS function management further stated that they plan to evaluate whether the *Agent Utilization* metric will add any additional value to their current productivity metrics.

It is important to have realistic performance goals and capture key industry metrics. Without them, the IRS cannot truly measure performance against program objectives, effectiveness, and efficiency.

**Recommendation 2:** The Chief Information Officer should evaluate the *Agent Utilization* metric for inclusion in the incident management program.

**Management's Response:** The IRS agreed with this recommendation. The IRS will research the *Agent Utilization* metric and evaluate the application and value to the incident management program.

# Appendix I

## Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the Information Technology organization is effectively and efficiently managing end-user computer incidents. To accomplish our objective, we:

- Reviewed the Government Accountability Office's *Standards for Internal Control in the Federal Government*, and IRS policies, procedures, and guidance for managing end-user incident tickets as well as service desk industry standards and best practices regarding incident ticket processes, performance goals, and metrics. We observed UNS function personnel demonstrating the incident management processes of using the KISAM tool.
- Assessed whether planned corrective actions were implemented to resolve previously reported conditions by reviewing documentation supporting the closure of the corrective actions.
- Performed data analytics to identify problematic trends with TIGTA's Applied Research and Technology Directorate's assistance by running queries against a data extract of 94,549 incident tickets closed during Fiscal Year 2021 and 1,567 incident tickets that remained opened as of November 17, 2021.
- Evaluated the effectiveness of resolving incident tickets by reviewing a judgmental sample[1] of 35 closed incident tickets from a population of 884 tickets having four or more reassignments, and assessed the incident ticket closure process by reviewing a second judgmental sample of 30 closed incident tickets from a population of 94,549 incident tickets. We selected judgmental samples because we did not plan to project the results to the populations.
- Assessed the UNS function's performance metrics and goals for completeness, and determined whether the UNS function is achieving its performance goals by comparing its performance goals to performance metric reports.

### Performance of This Review

This review was performed with information obtained from the Information Technology organization's UNS and Enterprise Operations functions located at the New Carrollton Federal Building in Lanham, Maryland, during the period October 2021 through July 2022. 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.

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

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Carol Taylor, Audit Manager; Allen Henry, Lead Auditor; Lauren Ferraro, Auditor; and Laura Christoffersen, Information Technology Specialist.

## Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the KISAM tool. We evaluated the data by 1) tracing select incident tickets from the data extract to the KISAM tool, 2) reviewing KISAM tool product documentation, and 3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

## 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* and IRS policies, procedures, and guidance regarding incident ticket recording, prioritizing, diagnosing, resolving, and closing; the MSLA; UNS function performance reports; and the service desk industry standards from the Service Desk Institute. We evaluated these controls by interviewing Information Technology organization personnel concerning the procedures and processes for incident management and reporting of incident metrics, analyzing a data extract from the KISAM tool, reviewing judgmental samples of closed incident tickets, and reviewing supporting documentation.

# Appendix II

## Definitions of Incident Management Metrics

| Incident Management Metric | Performance Goal | Metric Defined |
|---|---|---|
| *Call Abandonment* | 13% or less | Measures the percentage of all calls in the ESD queue that are disconnected by the customer before reaching a service desk operator. |
| *Call Handle Time* | 25 minutes or less | Measures the average amount of time it takes a service desk operator to complete an inbound service call. It includes talk time, hold time, wrap time, voice message, and other. |
| *Customer Satisfaction* | 85% | Measures the monthly and fiscal year-to-date results of three survey questions for interactions, incidents, and requests worked by the UNS function. |
| *Customers per Deskside Technician* | 200 customers | Measures how many customers are supported per service provider. |
| *First Level Resolution* | 60% | Measures the percentage of interactions closed by the ESD. It includes closed non-escalated interactions and ESD worked incidents and requests. |
| *Mean Time to Resolve – Priority 1* | 4 hours | Measures the average time it takes the UNS function to resolve Priority 1 interactions and incidents. |
| *Mean Time to Resolve – Priority 2* | 8 hours | Measures the average time it takes the UNS function to resolve Priority 2 interactions and incidents. |
| *Overage Tickets – Priority Level 1* | 10% or less | Measures the average daily percentage of ESD non-escalated interactions and assigned incidents, and requests open more than 30 calendar days. |
| *Overage Tickets – Priority Levels 2–4* | 10% or less | Measures the average daily percentage of all non-escalated interactions, and UNS function (assignment groups other than the ESD) incidents and requests open more than 30 calendar days. |
| *Overage Tickets – Overall* | 10% | Measures the average daily percentage of all non-escalated interactions, and UNS function incidents and requests open more than 30 calendar days. |
| *Request Fulfillment (20 business days)* | 93% | Measures the resolution timeliness of requests. |
| *Resolution Timeliness* | 87% | Measures the ability of the UNS function to resolve interactions and incidents for Priority 1 – 4 incident tickets closed during the month. |
| *Speed of Answer (Service Desk)* | Less than 8 minutes | Measures the average amount of time a customer waits in the Service Desk queue before reaching a service desk operator. |
| *UNS Percent on Time – Level 1: Priority 1* | 88% | Measures the timeliness of resolution for Priority 1 interactions and incidents worked by the ESD. |

| Incident Management Metric | Performance Goal | Metric Defined |
|---|---|---|
| *UNS Percent on Time – Level 1: Priority 2* | 85% | Measures the timeliness of resolution for Priority 2 interactions and incidents worked by the ESD. |
| *UNS Percent on Time – Level 1: Priority 3* | 87% | Measures the timeliness of resolution for Priority 3 interactions and incidents worked by the ESD. |
| *UNS Percent on Time – Level 1: Priority 4* | 87% | Measures the timeliness of resolution for Priority 4 interactions and incidents worked by the ESD. |
| *UNS Percent on Time – Levels 2–4: Priority 1* | 88% | Measures the timeliness of resolution of Priority 1 incidents resolved at the second level (UNS function assignment groups other than the ESD). |
| *UNS Percent on Time – Levels 2–4: Priority 2* | 85% | Measures the timeliness of resolution of Priority 2 incidents resolved at the second level (UNS function assignment groups other than the ESD). |
| *UNS Percent on Time – Levels 2–4: Priority 3* | 87% | Measures the timeliness of resolution of Priority 3 incidents resolved at the second level (UNS function assignment groups other than the ESD). |
| *UNS Percent on Time – Levels 2–4: Priority 4* | 87% | Measures the timeliness of resolution of Priority 4 incidents resolved at the second level (UNS function assignment groups other than the ESD). |

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

# Appendix III

## Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 2, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer
Digitally signed by B3CCB Date: 2022.09.02 20:52:15 -04'00'

SUBJECT: Response to Draft Report – The End-User Incident Management Process Can Be Improved (Audit #202220013)

Thank you for the opportunity to review and comment on the draft audit report. We have taken several actions to improve how we provide IRS employees the technology support they need, and we remain committed to continuously improving internal control procedures, consistent with IRS policies and guidelines.

We also appreciate TIGTA's acknowledgment of the extraordinary challenges we faced throughout the pandemic. We supported a hybrid workplace throughout Fiscal Year 2021 with many employees working remotely. This dynamic resulted in an increased demand for IT support, and we took several actions to resolve issues expeditiously. We will continue to review and update incident management guidelines and reinforce documentation requirements. We agree with your recommendations and have provided a detailed corrective action plan.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Tanya Chiaravalle, Customer Service Support Director, at (240) 613-4255.

Attachment

Attachment

**TIGTA Audit # 202220013, *The End-User Incident Management Process Can Be Improved***

**Recommendation #1:** The Chief Information Officer should ensure that incident ticket handling requirements are followed including selecting specific codes related to the issues, documenting actions taken including the reason for reassignments, and obtaining user concurrence before closing the incident ticket.

**CORRECTIVE ACTION #1**: We agree with this recommendation. The IRS will include training on the new coding and documentation requirements and update the incident management documentation.

**IMPLEMENTATION DATE:** June 15, 2023

**RESPONSIBLE OFFICIAL(S):** Associate Chief Information Officer, User and Network Services

**CORRECTIVE ACTION MONITORING PLAN:**
IRS will monitor this corrective action as part of our internal management system of controls.

**Recommendation #2:** The Chief Information Officer should evaluate the *Agent Utilization* metric for inclusion in the incident management program.

**CORRECTIVE ACTION #1**: We agree with the recommendation. The IRS will research an Agent Utilization metric and evaluate the application/value to the incident management program.

**IMPLEMENTATION DATE:** January 15, 2023

**RESPONSIBLE OFFICIAL(S):** Associate Chief Information Officer, User and Network Services

**CORRECTIVE ACTION MONITORING PLAN:**
IRS will monitor this corrective action as part of our internal management system of controls.

# Appendix IV

## Glossary of Terms

| Term | Definition |
|---|---|
| Artificial Intelligence | The ability of a digital computer to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience. |
| Automated Workflow | Shifts the performance of a series of activities needed to complete a task from humans to software programs. |
| BOT | A software program that can execute commands, reply to messages, or perform routine tasks such as online searches, either automatically or with minimal human intervention. |
| Chatbot | A computer program that simulates and processes human conversation, either written or spoken, allowing humans to interact with digital devices as if they were communicating with a real person. It can be as simple as rudimentary programs that answer a simple query with a single-line response, or as sophisticated as digital assistants that learn and evolve to deliver increasing levels of personalization as they gather and process information. |
| Cloud-Based | A computing model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing resources, *e.g.*, network, servers, storage, applications, and services, which can be rapidly provisioned and released with minimal management effort or service provider interaction. |
| Commercial Off-the-Shelf | Prepackaged, vendor-supplied software that is used with little or no modification to provide all or part of a development solution. |
| Configuration Management | Establishes proper control over approved project documentation, hardware, and software, and assures changes are authorized, controlled, and tracked. |
| Fiscal Year | Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30. |
| Impact | A measure of the effect of an incident, problem, or change on business processes. Impact is used to assign priorities to incident tickets. |
| Knowledge Article | Online documentation that answers a frequently asked question or provides instructions for solving a problem that users encounter. |
| Machine Learning | The use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy. |
| Metric | Something that is measured and reported to help manage a process, information technology service, or activity. |

| Term | Definition |
| --- | --- |
| Natural Language Processing | The ability of a computer program to understand human language as it is spoken and written. It is a component of artificial intelligence. |
| Urgency | A measure of how long it will be until an incident, problem, or change has a significant impact on business processes. Urgency is used to assign priorities to incident tickets. |
| Webchat | An Internet service that allows for the exchange of written messages with someone else who is using the service at the same time. |

# Appendix V

## Abbreviations

| | |
|---|---|
| ESD | Enterprise Service Desk |
| IRS | Internal Revenue Service |
| KISAM | Knowledge Incident/Problem Service Asset Management |
| MSLA | Master Service Level Agreement |
| TIGTA | Treasury Inspector General for Tax Administration |
| UNS | User and Network Services |


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

(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.