



Professional Services  
Standard Operating Procedures (SOP)

## **Managed Services Incident Management**

This document is classified as World Wide Technology (WWT) – CONFIDENTIAL. It may not be reproduced or redistributed in any format, written or electronic, without all parties' express written consent.

---

SOP Owner: Area Director  
SOP Authors: Julie Somerville and Leslie Okere  
SOP Operations: [PS\\_DEL\\_Operations@wwt.com](mailto:PS_DEL_Operations@wwt.com)  
Current Version Number: V1.2

## Table of Contents

1	Introduction .....	4
1.1	Outcomes .....	4
1.2	Target Audience .....	4
2	Scope .....	4
3	Out of Scope .....	4
4	Business Rules .....	5
5	Roles and Responsibilities .....	6
6	Incident Management Process.....	9
6.1	Incident Detection or Identification.....	9
6.2	Incident Registration.....	9
6.3	Incident Classification and Categorization.....	14
6.4	Incident Diagnosis.....	16
6.5	Incident Resolution .....	18
6.6	Incident Closure .....	18
7	Periodic Incident Review .....	19
8	Incident Record Management.....	20
9	Incident Record Escalations .....	23
9.1	Tier 2 Requires Command Center SA Tier 3 or 4 Support:.....	23
9.2	The Command Center Requires Tier 2 or Tier 3: .....	23
10	MI Management.....	23
10.1	Identifying an MI.....	23
10.2	MI Key Characteristics.....	24
10.3	Handling a MI .....	24
10.4	Root Cause Analysis .....	25
10.5	MI Review .....	25
11	References.....	25
12	Definitions .....	26
13	Version Control .....	33
	Appendix A: Incident Process Flow .....	27
	Appendix B: Major Incident Process Flow .....	28
	Appendix C: ServiceNow Field Definitions for New Call and Incident .....	29

## List of Tables

Table 1: Business Rules .....	5
Table 2: ServiceNow Impact Classifications .....	14
Table 3: ServiceNow Urgency Classifications.....	14
Table 4: Priority Level Classification Matrix.....	15
Table 5: Priority Level Response and Target Resolutions .....	15
Table 6: Incident Categories and Subcategories.....	16
Table 7: Key Metrics - Process and Quality Management .....	19
Table 8: Table of References.....	26
Table 9: Table of Definitions .....	26

## List of Figures

Figure 1: MS NOW New Call Record .....	10
Figure 2: MS ServiceNow Calls Awaiting Triage queue.....	10
Figure 3: MS ServiceNow Customer Service Portal ( <a href="https://wwtms.service-now.com/sp">https://wwtms.service-now.com/sp</a> ) .....	11
Figure 4: MS ServiceNow Self Service Report an Issue form. ....	<b>Error! Bookmark not defined.</b>
Figure 5: MS ServiceNow Incident Queue .....	12
Figure 6: MS ServiceNow Create New Incident .....	13
Figure 7: ServiceNow New Incident Form.....	13
Figure 8: MS ServiceNow Incident in progress and field updates .....	17
Figure 9: MS ServiceNow Incident Resolved.....	18
Figure 10: MS ServiceNow Management Dashboard – Overview – Calls Awaiting Triage.....	20
Figure 11: MS ServiceNow Navigation Access – Calls Awaiting Triage .....	21
Figure 12: MS ServiceNow Management Dashboard – Incident Details – Unassigned Incidents .....	22
Figure 13: MS ServiceNow Navigation Access – Open – Unassigned .....	22

## 1 Introduction

The purpose of this document is to provide a vivid description of the WWT Managed Services (MS) Incident Management process.

This document addresses the following:

- Specify a complete, precise, and correct manner of the characteristics of the process.
- Ensure a consistent, repeatable process that enables MS to offer a high-quality service to our customers.
- Provide an understanding of the process performed across MS.
- Provide a reference point for process queries and discussion.
- The focus of Incident Management is on reducing the duration and consequences of a service outage from a business and customer perspective rather than finding the root cause.

This process description is a living document and serves as a model towards which the organization will evolve.

### 1.1 Outcomes

The successful implementation of this process will result in the following:

- Recorded and classified incidents.
- Prioritized and analyzed incidents.
- Resolved and closed incidents.
- Escalate incidents that do not progress according to agreed service levels.
- Communicate information regarding the status and progress of incidents to interested parties.
- Manage and report Major Incidents (MI).

### 1.2 Target Audience

Staff working for or on behalf of MS and individuals responsible for:

- Delivering services efficiently and at an acceptable cost.
- Delivering services within prescribed service levels.
- MS Staff maintaining user satisfaction with our services.

## 2 Scope

This document covers the MS Incident and MI Management policy and process. It includes sections on the creation, management, and closure of incident records.

## 3 Out of Scope

The following examples identify what is out of Scope for Incident Management:

- Externally hosted services where a specific support agreement with WWT MS does not exist.
- Defects identified during the development and testing of WWT MS products.
- Issues identified with the functionality of 3rd Party applications that are not under WWT MS Service Offering.

## 4 Business Rules

The following attributes are fundamental to the success of Incident Management. The governance herein defines management expectations for the practical implementation of these rules.

**Table 1: Business Rules**

Category	#	Statements
<b>1.0 General</b>	1.1	MS must have a single Incident Management process defined.
	1.2	There shall be a single accountable process owner.
	1.3	All staff involved in Incident Management shall perform Incident Management tasks per formalized processes and procedures.
	1.4	Where relevant, processes and procedures shall comply with WWT Guidelines.
	1.5	This process shall be used in conjunction with and not supersede statutory obligations.
	1.6	All staff involved in Incident Management shall record and manage incident records within a single centralized support tool.
	1.7	Incidents shall be classified using a standardized set of criteria.
	1.8	Incident records shall be verified on an ongoing basis to ensure performance in formalized processes and procedures.
	1.9	Problems shall be tracked separately from incidents.
<b>2.0 Engagement</b>	2.1	The Command Center Service Desk (Service Desk) is the main point of contact for the ownership, monitoring, tracking, and communication of all incident records in scope 24X7.
	2.2	Staff shall refer users wanting to report an incident to the Service Desk or Client Portal.
	2.3	Every incident record shall have a responsible party.
	2.4	The team shall have the authority to assign incident records to the appropriate support teams. The incident manager or Team Manager shall have the authority to escalate any assignment non-responsiveness to senior management.
	2.5	MS shall commit appropriate resources to conduct activities as required by Incident Management.
	2.6	Resources assigned to incidents shall update their tickets regularly to keep all stakeholders informed. They shall provide detailed troubleshooting steps that led to incident resolution.
<b>3.0 Communication</b>	3.1	The Service Desk shall be the main point of contact or channel of communication for all incidents.
	3.2	The Service Desk shall provide the status of incidents to customers.
	3.3	The Service Desk shall follow through promptly for requests for status updates.

Category	#	Statements
	3.4	All staff involved in Incident Management shall have access to relevant information such as known errors, problem resolutions, changes, and the configuration management database.
<b>4.0 Escalation</b>	4.1	Incidents shall be escalated according to specified criteria, as identified in supporting procedures.
<b>5.0 Critical Incidents</b>	5.1	MIIs shall be classified and managed following documented procedures.
<b>6.0 Record Status</b>	6.1	<p>The following are valid motives to place an incident into a “Pending” status. Reasons outside those listed shall not be allowed:</p> <ul style="list-style-type: none"> <li>• Waiting for customer/user approval or additional info</li> <li>• Waiting for an associated Scheduled Event</li> <li>• Waiting for additional information from a third-party</li> <li>• Waiting for the associated problem</li> </ul>
	6.2	Only incidents in the pending state may have Service level target calculations paused.
	6.3	The Incident Assignee must update open records regularly following documented procedures and the agreed timescale. Updates must contain meaningful information regarding the progress and status of the request.
<b>7.0 Closure</b>	7.1	<p>Only the following roles shall have the authority to close records:</p> <ul style="list-style-type: none"> <li>• Service Desk</li> <li>• Incident Process Manager</li> <li>• Affected customer/user</li> </ul>

## 5 Roles and Responsibilities

Many roles assist the MS team in managing incidents optimally. Below is the complete list of those roles and their responsibilities.

Role	Responsibility
Incident Management Process Owner	<ul style="list-style-type: none"> <li>• Accountable for managing the process and ensuring all users perform the tasks as per the outlined procedures.</li> <li>• Promotes awareness of Incident Management within MS</li> <li>• Responsible for Incident Management continuous improvement reviews and decision making on improvement suggestions.</li> <li>• Collaborates with other process owners to ensure integration with related processes.</li> </ul>

	<ul style="list-style-type: none"> <li>• Works with the organization concerning the strategy for capacity and capability, as related to Incident Management.</li> </ul>
Incident Management Process Manager	<ul style="list-style-type: none"> <li>• Plans and manages the support for Incident Management tools and processes.</li> <li>• Develops and maintains the Incident Management process and procedures.</li> <li>• Coordinates with other process managers to ensure integration with related processes.</li> <li>• Acts as liaison with stakeholders to resolve incidents and incident-related information.</li> <li>• Liaises with resolution groups to ensure swift resolution of incidents and Requests within Service Level Agreement (SLA) targets.</li> <li>• Authorizes the inclusion of knowledge information into the Knowledge Base (KB) in consultation with the problem Process Manager</li> <li>• Formally closes incident records</li> <li>• Produces management information</li> <li>• Documents all follow-up activities relating to Critical incident reviews</li> </ul>
Tier 1 – Service Desk	<ul style="list-style-type: none"> <li>• Provide first-line support for incidents when they occur using the Incident Management process.</li> <li>• Provide ownership, monitoring, tracking, and communication of incidents.</li> <li>• Record incidents.</li> <li>• Routing incidents to support specialist groups when needed</li> <li>• Analyze for correct prioritization, classification, and providing initial support.</li> <li>• First-call resolution of incidents not assigned to support specialist groups</li> <li>• Monitor the status and progress towards resolution of assigned incidents.</li> <li>• Keeps customers and other teams informed about incident progress.</li> <li>• Escalate incidents as necessary per established escalation policies.</li> <li>• Command Center Service Desk will perform customer-related direct communications.</li> <li>• Will Provide warm transfer if transferred or escalated to another support group.</li> </ul>
Tier 2 – Network Operation Center (NOC)	<p>This team consists of staff with mid-level technical skills. They do the following:</p>

	<ul style="list-style-type: none"> <li>• Handles many of the slightly complex 'day-to-day' incidents, needing support higher than Tier 1 services.</li> <li>• Will provide warm transfer if transferred or escalated to another support group.</li> </ul>
Tier 3 – Manager Services Engineering	<p>This team consists of high-level engineers. They typically:</p> <ul style="list-style-type: none"> <li>• Handles complex, deep-rooted incidents, problems, or new developments.</li> <li>• Initiate the Change Management process where necessary.</li> <li>• Open Change Requests (RFCs) and implement Changes.</li> </ul>
Tier 4 – Command Center – MS Support	<p>This team consists of highly specialized Solution Architects (SAs) and subject matter experts in a particular domain.</p> <ul style="list-style-type: none"> <li>• Handles complex, deep-rooted incidents.</li> <li>• Leads long-range planning and prevention of critical incidents.</li> <li>• Identifies of root cause and determines permanent fixes.</li> <li>• Provides subject matter expert level support on MIs.</li> <li>• Provides technical consulting services to the customer upon request./</li> <li>• Command Center will interface with 3rd party vendors as required.</li> </ul>
Third-Party Vendor	<ul style="list-style-type: none"> <li>• Highly specialized, deeply technical external suppliers who handle complex, deep-rooted incidents for their clients.</li> <li>• Will provide technical support on incidents escalated to them.</li> </ul>
Command Center Technical Operations Manager	<p>Escalation and Incident Process Manager, coordinates MIs, including communications and SA assignment, to critical Incidents.</p> <ul style="list-style-type: none"> <li>• Documents escalation troubleshooting activities in the escalated incident ticket.</li> <li>• Coordinates and assigns Engineering SA to Incident or MI.</li> <li>• Participates on MI Bridges.</li> <li>• Sends internal status communications to WWT leadership and stakeholders.</li> <li>• Communicates relevant business impact information during critical and high severity incidents.</li> </ul>
Client Relationship Manager/Champion	<p>Single point of contact between the customer and MS regarding incidents.</p> <ul style="list-style-type: none"> <li>• Consults with the Process Owner to review performance metrics.</li> <li>• Provides guidance and support to Process Manager and affected Business Owners.</li> <li>• Involvement generally limited to critical Incidents which affect large volumes of business customers.</li> </ul>



Business Owner	<p>The information owner is accountable for the productive use of the information system for the organization.</p> <ul style="list-style-type: none"> <li>• Provides input to assist in the improvement of the Incident Management process.</li> <li>• Provides business impact information to the Customer Relationship Manager (CRM).</li> <li>• Consulted on the escalation of critical Incidents.</li> </ul>
----------------	--

## 6 Incident Management Process

There are six Incident Management activities:

- Detection
- Registration
- Classification
- Diagnosis
- Resolution
- Closure

This section describes each management activity and how they work in WWT MS Operations.

### 6.1 Incident Detection or Identification

Incident identification or Incident detection is the initial activity in the Incident Management process. It is where an end-user, support team, or monitored system has identified a malfunction in the environment. The Service Desk agent performs the initial triage to confirm that the fault does refer to an incident.

### 6.2 Incident Registration

Incident Registration is the second activity in the process. Here, the Service Desk manually adds available data to the Incident record. The Service Desk agent also records the event details; who (total users impacted), what, when, and contact information. Alternatively, the event monitoring tool automatically registers the Incident, associates it with the affected Configuration Item (CI), and sends a notice to the technical stakeholders.

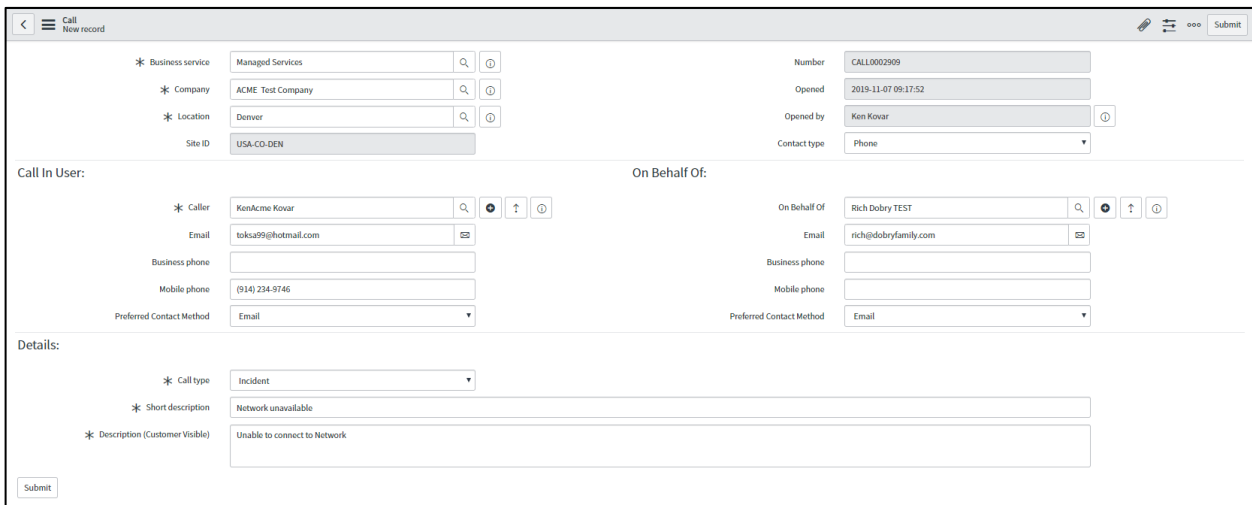
There are five different ways to initiate the incident record:

- Generated from a Call Record after the customer calls the Command Center Service Desk.
- Created from the Awaiting Triage Queue in ServiceNow after a customer sends an email to the Command Center Service Desk.
- Customer initiated via the Customer Service Portal.
- Event monitoring and registration via the WWT Event Management Tool.
  - **Note:** MS Operations covers the Event Management Process in a separate SOP.
- Manually creating an incident record via the ServiceNow interface.

## New Call Record

The Service Desk can register a new call from two sources:

- **Customer Phone Call:** When the Service Desk agent answers the help desk number, a new call record screen pops up. If the customer is a registered user, the “New Call” screen will prepopulate the Company, Location, Caller, and call type fields (see Figure 1). The SLA clock will start once the Agent completes capturing the customer’s issue details and converts the call to an Incident record.



The screenshot shows the 'New record' form for a call. It is divided into several sections:

- Business service:** Managed Services
- Company:** ACME Test Company
- Location:** Denver
- Site ID:** USA-CO-DEN
- Number:** CALL0002909
- Opened:** 2018-11-07 09:17:52
- Opened by:** Ken Kovar
- Contact type:** Phone

**Call In User:**

- Caller:** KenAcme Kovar (Email: toksa99@hotmail.com)
- Business phone:**
- Mobile phone:** (914) 234-9746
- Preferred Contact Method:** Email

**On Behalf Of:**

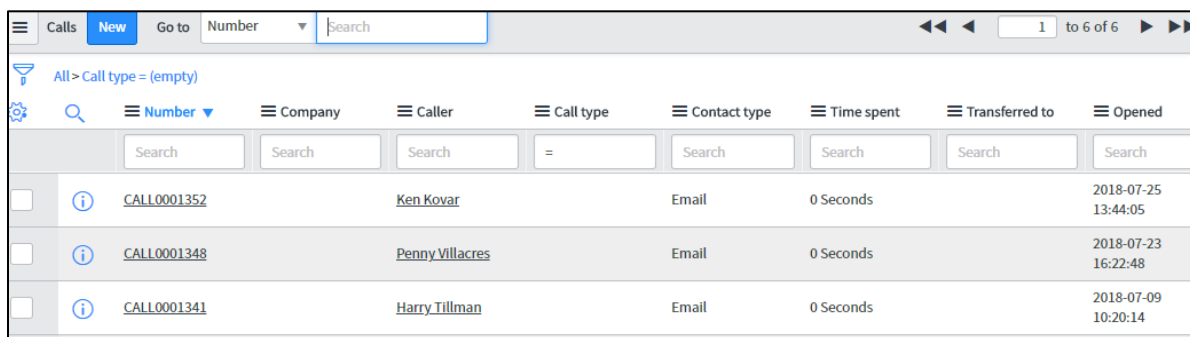
- On Behalf Of:** Rich Dobry TEST (Email: rich@dobryfamily.com)
- Business phone:**
- Mobile phone:**
- Preferred Contact Method:** Email

**Details:**

- Call type:** Incident
- Short description:** Network unavailable
- Description (Customer Visible):** Unable to connect to Network

**Figure 1: MS ServiceNow New Call Record**

- **Customer Email:** The customer sends an email to the Service Desk via the WWT MS Service Desk [wwt1se@service-now.com](mailto:wwt1se@service-now.com) email. The message posts a call record to the “Calls Awaiting Triage” queue in ServiceNow, which the Service Desk monitors regularly. Depending on if the customer is a registered user, a “New Call” may have the following fields prepopulated: Company, Location, Caller, and call type (see Figure 2).



The screenshot shows a list of calls in the 'Calls Awaiting Triage' queue. The table has the following columns: Number, Company, Caller, Call type, Contact type, Time spent, Transferred to, and Opened.

	Number	Company	Caller	Call type	Contact type	Time spent	Transferred to	Opened
	CALL0001352		Ken Kovar		Email	0 Seconds		2018-07-25 13:44:05
	CALL0001348		Penny Villacres		Email	0 Seconds		2018-07-23 16:22:48
	CALL0001341		Harry Tillman		Email	0 Seconds		2018-07-09 10:20:14

**Figure 2: MS ServiceNow Calls Awaiting Triage queue**

### Customer Service Portal Self Service

The Customer Service Portal is a portal framework that allows customers to use self service to “Report an Issue” (see Figure 3). The initial submission of the issue will generate an incident record (see Figure 4). The Service Desk agent will monitor the Incident Management queue for unassigned groups. Once the system creates an Incident record in ServiceNow, the Service Desk agent will start the Incident triage process.

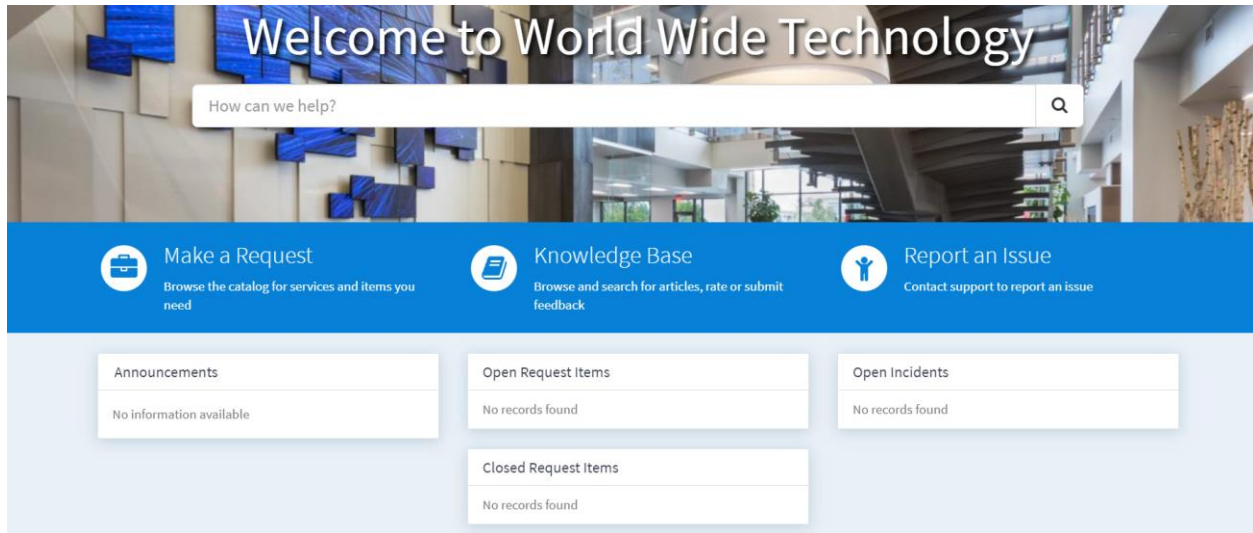
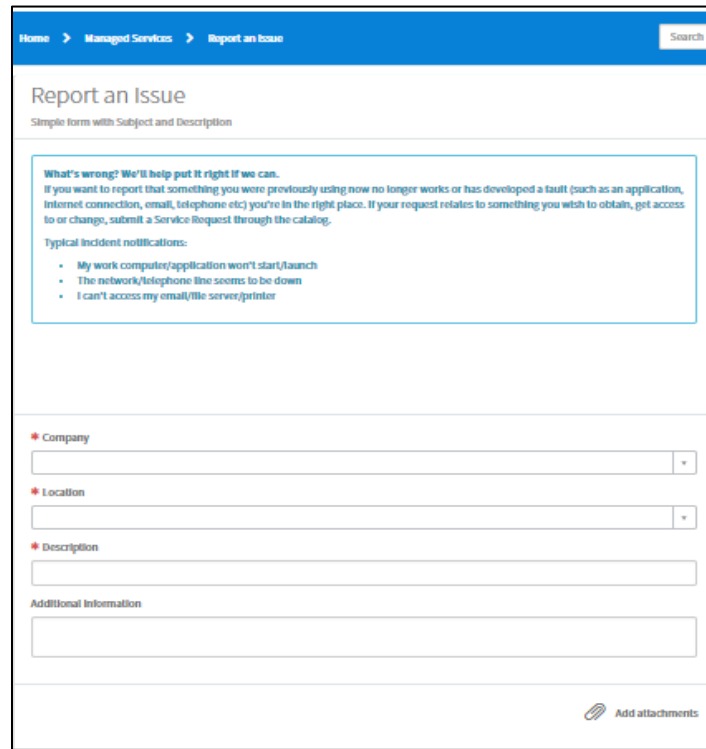


Figure 3: MS ServiceNow Customer Service Portal



Home > Managed Services > Report an Issue

Report an Issue

Simple form with Subject and Description

What's wrong? We'll help put it right if we can.  
If you want to report that something you were previously using now no longer works or has developed a fault (such as an application, Internet connection, email, telephone etc) you're in the right place. If your request relates to something you wish to obtain, get access to or change, submit a Service Request through the catalog.

Typical incident notifications:

- My work computer/application won't start/launch
- The network/telephone line seems to be down
- I can't access my email/file server/printer

\* Company

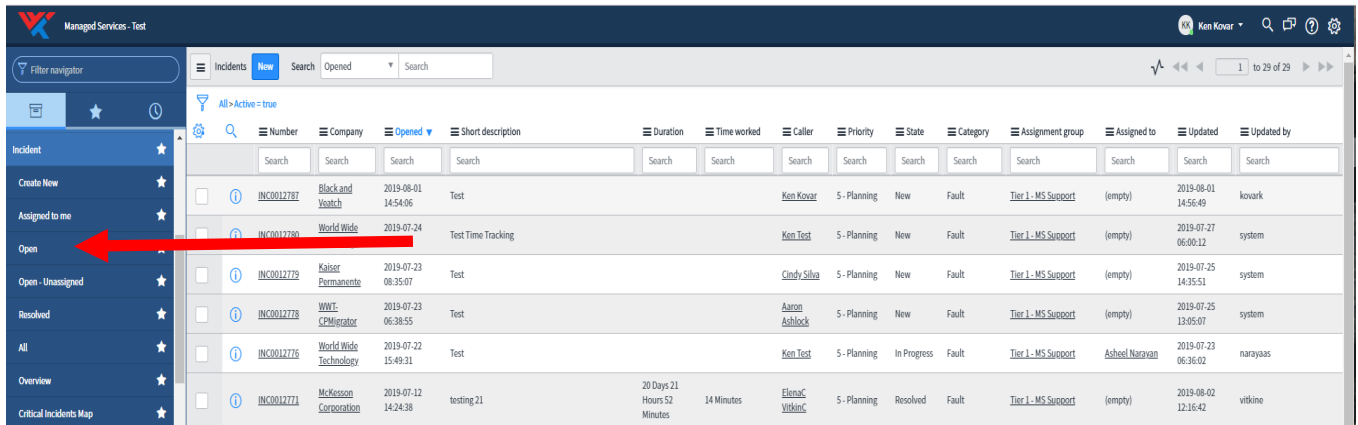
\* Location

\* Description

Additional Information

Add attachments

**Figure 4: MS ServiceNow Self Service Report an Issue Form**



Number	Company	Opened	Short description	Duration	Time worked	Caller	Priority	State	Category	Assignment group	Assigned to	Updated	Updated by
INC0012787	Black and Veatch	2019-08-01 14:54:06	Test			Ken Kovar	5-Planning	New	Fault	Tier 1 - MS Support	(empty)	2019-08-01 14:56:49	kovark
INC0012780	World Wide	2019-07-24	Test Time Tracking			Ken Test	5-Planning	New	Fault	Tier 1 - MS Support	(empty)	2019-07-27 06:00:12	system
INC0012779	Kaiser Permanente	2019-07-23 08:35:07	Test			Cindy Silva	5-Planning	New	Fault	Tier 1 - MS Support	(empty)	2019-07-25 14:35:51	system
INC0012778	WWT - CPM/escalator	2019-07-23 06:38:55	Test			Aaron Ashlock	5-Planning	New	Fault	Tier 1 - MS Support	(empty)	2019-07-25 13:05:07	system
INC0012775	World Wide Technology	2019-07-22 15:49:31	Test			Ken Test	5-Planning	In Progress	Fault	Tier 1 - MS Support	Ashled Narayan	2019-07-23 06:36:02	narayasa
INC0012771	McKesson Corporation	2019-07-12 14:24:38	testing 21	20 Days 21 Hours 52 Minutes	14 Minutes	ElenaC VitkinC	5-Planning	Resolved	Fault	Tier 1 - MS Support	(empty)	2019-08-02 12:16:42	vitkine

**Figure 4: MS ServiceNow Incident Queue**

### Manually Opening an Incident

Sometimes the Service Desk may need to open an incident record manually, for example, in situations where the event monitoring tool is not functioning correctly (see Figures 6 and 7).

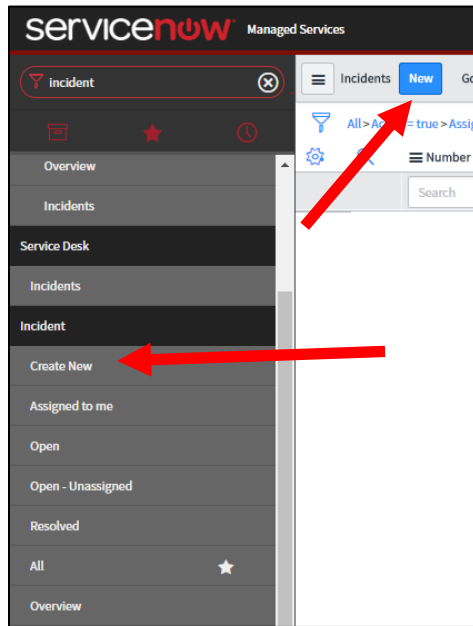


Figure 5: MS ServiceNow Create New Incident

Incident - INC0014500  
New record
📎 ⚙️ ∞

\* Business service

\* Company

\* Location

Site ID

Number

Opened

Opened by

Contact type

Priority:

Priority  State

Impact

Urgency

Call In User:

\* Caller

On Behalf Of:

On Behalf Of

What & Why:

Configuration item

Assignment:

Assignment group

Figure 6: ServiceNow New Incident Form

### 6.3 Incident Classification and Categorization

The classification and categorization activity involves setting a priority on the Incident based on the Impact and Urgency. It also involves setting the category and subcategory based on the nature of the failure reported.

#### Incident Classification

After Incident Registration, the incident record state is “New.” The Service Desk agent will start the incident classification process and capture the initial data required in the incident record. The SLA timer starts once the Agent creates the Incident record. Should the Agent create the Incident record through a new Call record, the SLA timer will begin before the incident creation.

The Service Desk agent will gather all the pertinent details of the impacted sites, systems, and devices from the user reporting the Incident. Then, the Agent will assess the priority code based on the Impact and Urgency Table (see Tables 2 and 3). The Impact and Urgency set the priority, and the latter setting determines the Response and Resolution SLAs (see Table 4) settings. These settings drive the speed at which Tiers 1 – 4 engineers should react (See Table 5). Once all the required fields are populated, the Service Desk agent must assign the ticket to themselves then save the record. Setting the Incident ticket owner changes the Incident state from “New” to “In Progress” (see Figure 8).

**Note:** The SLA timer for response will stop once the Incident changes to “in Progress” or any other state other than “New.”

**Table 2: ServiceNow Impact Classifications**

Impact	Definition
<b>1 – Major</b>	<ul style="list-style-type: none"> <li>Service down affecting the entire organization, department, or line of business.</li> <li>50% outage impacting 50% or more of devices or end-users on covered equipment.</li> </ul>
<b>2 – Moderate</b>	<ul style="list-style-type: none"> <li>Service down for single user or;</li> <li>Service degraded for a group of users or;</li> <li>10% or more of total end-users on covered equipment at a site.</li> </ul>
<b>3 – Minor</b>	<ul style="list-style-type: none"> <li>Non-outage or service impairment issue affecting &lt; 10% of users at a site or;</li> <li>The Incident is for a single user.</li> </ul>

**Table 3: ServiceNow Urgency Classifications**

Urgency	Definition
<b>1 – High</b>	<ul style="list-style-type: none"> <li>Core (critical) Business Service as identified by Business Impact Analysis (BIA) or;</li> <li>Critical peak business period (e.g., Month-end, Start of Day) or;</li> <li>Business process stopped; users cannot work and;</li> <li>No workaround available.</li> </ul>

<b>2 – Medium</b>	<ul style="list-style-type: none"> <li>Support Service that directly supports the execution of a core business service (e.g., Medium BIA rating) or;</li> <li>Business Processes affected; key functionality unavailable and;</li> <li>No workaround available.</li> </ul>
<b>3 – Low</b>	<ul style="list-style-type: none"> <li>Non-urgent service that is not time-sensitive (e.g., Low BIA rating) or;</li> <li>Process degraded or;</li> <li>Workaround available.</li> </ul>

**Table 4: Priority Level Classification Matrix**

		Urgency		
		High	Medium	Low
Impact	Major	1	2	3
	Moderate	2	3	4
	Minor	3	4	4

**Table 5: Priority Level Response and Target Resolutions**

Priority Classification	Priority	Response SLA Time	Resolution SLA Time	Availability
1	Critical	15 minutes	4 Hours	24x7
2	High	2 Hours	24 Hours	24x7
3	Medium	4 Hours	48 Hours	24x7
4	Low	8 Hours	96 Hours	24x7

### Incident Categorization

Part of the Incident’s initial logging will be to select the correct incident category and subcategory coding to record the exact type of Incident. This coding is critical for establishing trends for use in problem management and other service management activities. The following categories and subcategories further support incident types to give more specific data regarding incidents managed by the process (see Table 6).

There are four categories:

**Table 6: Incident Categories and Subcategories**

Categories	Description	Subcategories
Fault	Incidents from the users to restore services or components that are not functioning as designed or have malfunctioned.	<ul style="list-style-type: none"> <li>• Performance Issue</li> <li>• Power Issue</li> <li>• Connectivity Issue</li> <li>• Network Down</li> <li>• Management Tools</li> <li>• Other</li> </ul>
Monitoring	Incidents raised by automated monitoring systems.	<ul style="list-style-type: none"> <li>• Alert</li> <li>• Exception</li> <li>• Warning</li> <li>• Informational</li> </ul>
Technical	Malfunction identified by the WWT professional staff.	<ul style="list-style-type: none"> <li>• Hardware Issue</li> <li>• Environment/HVAC</li> <li>• Infrastructure/Layer 1</li> <li>• Resource availability</li> <li>• Device Configuration</li> <li>• Other</li> </ul>
Security	Issues related to vulnerabilities, intrusion detection, or malware.	<ul style="list-style-type: none"> <li>• Malware</li> <li>• Intrusion detection event</li> </ul>

Periodic reviews of incident tickets will produce updates to the categories and subcategories as the process managers identify ticket trends.

## 6.4 Incident Diagnosis

The Incident Diagnosis activity involves the technical teams investigating and trying to understand a solution to the issue, primarily when classification does not give insight to a solution. Diagnosis may include escalating the Incident between the teams and implementing collaborative troubleshooting techniques, such as swarming.

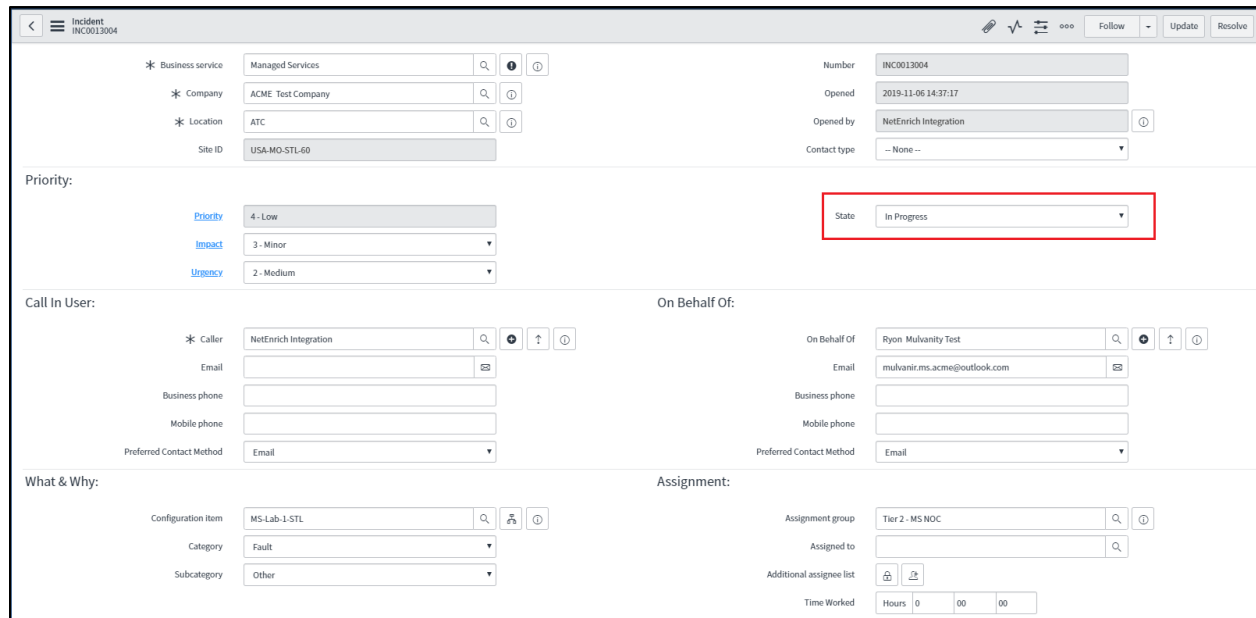
The agents will follow the desktop procedures and scripts to capture the correct details in the incident record. After gathering the initial data, the Service Desk agent will start the troubleshooting process and search for similar incident records from the past or Known Error Database. The Agent will evaluate the need to escalate to Tier 2. For P1 and P2 incidents, the Agent will assign the ticket to the Tier 2 support group within 15 to 20 minutes. For P3 through P4 incidents, the Agent will escalate the Incident to the Tier 2 support group in 1 hour.

### Configuration Items

A CI is any service component, infrastructure element, or other things that organizations manage to ensure the successful delivery of services. For example, network devices, server systems, UPS devices, and applications. The Service Desk agent must ensure that incidents have a CI associated with the ticket before transferring it to a support group. Associating a CI to the Incident is critical for analytics and



trending purposes. It relates to the root cause analysis process. The Agent will change the ticket state from “In Progress” to “Resolved” once the support team restores the CI to a steady-state.



The screenshot shows the ServiceNow incident form for incident INC0013004. The form is divided into several sections:

- Business service:** Managed Services
- Company:** ACME Test Company
- Location:** ATC
- Site ID:** USA-MO-STL-60
- Number:** INC0013004
- Opened:** 2019-11-06 14:37:17
- Opened by:** NetEnrich Integration
- Contact type:** -- None --
- Priority:** 4 - Low
- Impact:** 3 - Minor
- Urgency:** 2 - Medium
- State:** In Progress (highlighted with a red box)
- Call In User:** NetEnrich Integration
- On Behalf Of:** Ryon Mulvanity Test
- What & Why:** Configuration Item: MS-Lab-1-STL, Category: Fault, Subcategory: Other
- Assignment:** Assignment group: Tier 2 - MS NOC

**Figure 7: MS ServiceNow Incident in progress and field updates**

### Incident “Pending” State - SLA Pause Reasons

As the Managed Services Operations (MSO) team troubleshoots incidents, there may be times where an Agent or Engineer must use the “Pending” state, which stops the SLA clock. The Service Desk Manager or Technical Operations Manager (TOM) ensures that all support staff place tickets in a pending state for legitimate reasons. The conditions below are the only reasons to pause the SLA timer:

- **Customer (Awaiting User)** – If the support team is awaiting input from the customer or customer support team for any reason, then the Incident must be placed in a pending state. For example, considering the time required for a customer to fulfill a required dependency will contribute to a resolution.
- **Vendor (Awaiting 3<sup>rd</sup> Party)** – If the support team opens a case with the vendor and is waiting for feedback, the ticket assignee must place the Incident in a pending state. For example, when the OEM must ship resources or materials to resolve an issue.
- **Change Management (Awaiting Scheduled Event)** – If a resolution is awaiting a scheduled change, the ticket assignee must pause the SLA timer. Should the change be required to resolve a production environment issue, the Incident can be placed in pending and linked to the change record. Once the change implementor completes execution, the assignee must resume the SLA timer.
- **Waiting for Problem Resolution (Awaiting Problem)** – If the resolution is awaiting a problem record closure, the ticket assignee must pause the SLA timer. Once the problem resolver implements a solution on the problem record, the assignee must resume the SLA timer

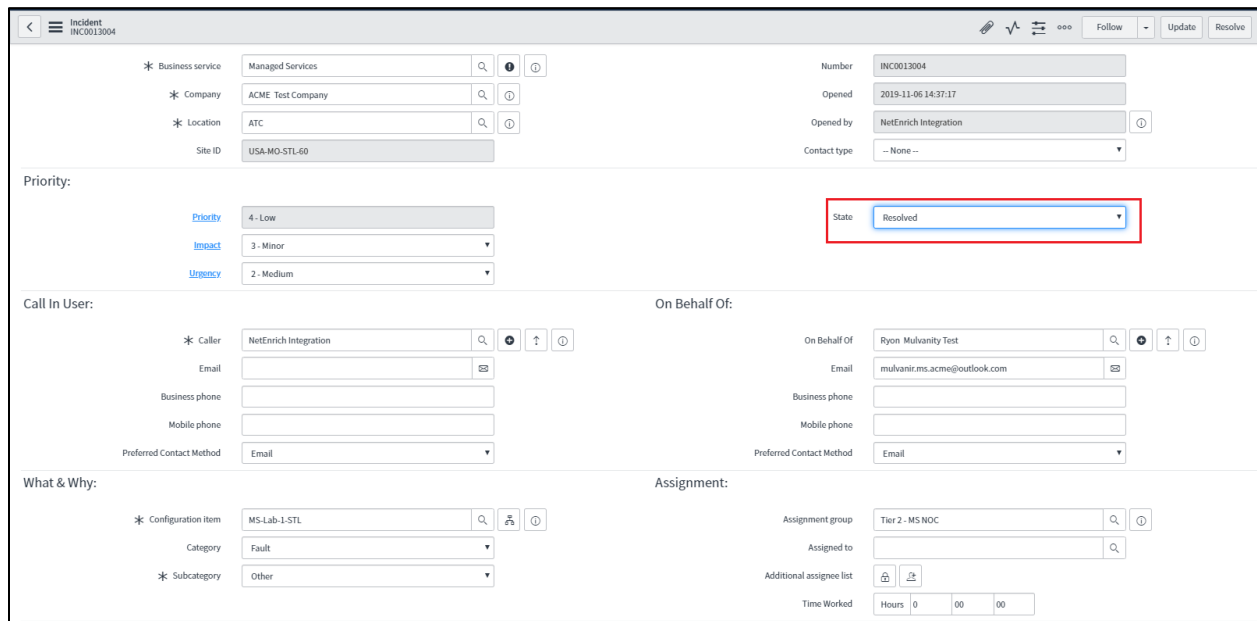
### Transferring Incidents to Other Teams

Before escalating a ticket or assigning it to another support group, the ticket assignee must update the Incident ticket with all troubleshooting steps taken and the results of those steps. The ticket assignee must initiate a warm transfer by speaking directly with the new assignee and talking through the troubleshooting steps.

## 6.5 Incident Resolution

Incident Resolution activity involves applying a solution to resolve the issue. This activity may require the initiation of a change. If the solution does not work, the support team will continue diagnosis activities. Otherwise, the assignee resolves the Incident.

Once an Incident is in the Resolved state, the Agent or Engineer completed the tasks required to restore service. The customer will receive an email informing them of service restoration and letting them know that they should validate recovery and approve or reject the resolution. Resolving the ticket stops the SLA Resolution timer. As a best practice, the Service Desk agent should gather customer approval as soon as possible, note the customer approval in the ticket, and move the Incident from “Resolved” to “Closed.” This practice will allow the incidents to close more efficiently with the customer agreement.



The screenshot shows the ServiceNow incident form for incident INC0013004. The form is divided into several sections:

- Business Service:** Managed Services
- Company:** ACME Test Company
- Location:** ATC
- Site ID:** USA-MO-STL-60
- Number:** INC0013004
- Opened:** 2019-11-06 14:37:17
- Opened by:** NetEnrich Integration
- Contact type:** -- None --
- Priority:**
  - Priority: 4 - Low
  - Impact: 3 - Minor
  - Urgency: 2 - Medium
- State:** Resolved (highlighted with a red box)
- Call In User:**
  - Caller: NetEnrich Integration
  - Email: [empty]
  - Business phone: [empty]
  - Mobile phone: [empty]
  - Preferred Contact Method: Email
- On Behalf Of:**
  - On Behalf Of: Ryon Mulvanity Test
  - Email: mulvanir.ms.acme@outlook.com
  - Business phone: [empty]
  - Mobile phone: [empty]
  - Preferred Contact Method: Email
- What & Why:**
  - Configuration Item: MS-Lab-1-STL
  - Category: Fault
  - Subcategory: Other
- Assignment:**
  - Assignment group: Tier 2 - MS NOC
  - Assigned to: [empty]
  - Additional assignee list: [empty]
  - Time Worked: Hours 0 00 00

**Figure 8: MS ServiceNow Incident Resolved**

## 6.6 Incident Closure

The end goal of Incident Management is closing an incident record as quickly and efficiently as possible. An incident in a “closed” state means the customer approved the service restoration. If the customer confirms the normal service operations on a call, the Agent must update the record to closed. Otherwise, the customer has twenty-four hours to approve or reject the resolved Incident. If the customer does not respond in 24 hours, ServiceNow will automatically close the ticket.

**Note:** The ticket owner will place records into the resolved state for closure by the Service Desk, or it will close after 24 hours of inaction from the customer.

### Incident Cancellation

There are times when the ticket assignee or Service Desk must cancel an Incident ticket. The list below gives reasons for the Service Desk agent or user to place an incident record in a “Canceled” state:

- Customer or vendor requests to cancel the reported Incident
- Opened incident record in error
- When testing incident records

## 7 Periodic Incident Review

This activity focuses on the continuous service improvement of the Incident Management process for MSO. Quarterly, the process managers and the process owner will review incident reports for improvement opportunities. They will institute some process and quality management controls to ensure the managed support team performs as expected and adheres to service level expectations per contract agreements.

**Table 7: Key Metrics - Process and Quality Management**

Critical Success Factor	Category	Key Performance Indicator	Metric
Quickly resolve incidents	Compliance	Number of Incidents	Number of incidents registered by the Command Center Service Desk and Tier 2 grouped into categories.
	Compliance	Mean Time to Restore (MTTR)	Average time to resolve incidents by type/category.
	Efficiency	Efficiency rate	The total volume of non-resolved/closed incidents.
	Efficiency	Mean Time to Notify (MTTN)	The average time expended between the alert generated time and the time that the Command Center Service Desk and Tier 2 responds to that Incident.
	Quality	First Time Resolution Rate	Percentage of incidents resolved by the Tier 2 grouped into categories.
Maintain IT Service Quality	Quality	Number of repeated incidents	Number of repeated incidents, with known resolution methods.
Improve productivity	Quality	Random Spot Checks	Number and percentage of incidents incorrectly categorized.
	Effective	Incomplete incident volume	Number of non-closed/resolved incidents by priority level and support group.
Maintain user satisfaction	Effective	Support team involvement	SLT breaches by the support group.
Continuous Improvement	Effective	Monthly Incident Reports	Total number of incidents, MTTN, MMTR.

## 8 Incident Record Management

This section describes Service Desk setup requirements for Incident record management.

- **The customer calls into the Command Center Service Desk** – The Command Center Service Desk agent will see a screen pop up to create a new call record. The requirement for the Agent is to follow the documented desk procedures to endure readiness.
  - The Agent must log into the Telephony Application. Logging in will enable the screen to pop up when the Agent is receiving a call. The Agent can then generate a new Call record.
- **The customer sends emails into the Command Center Service Desk** – Command Center Service Desk agent monitors the “Calls Awaiting Triage” queue for new call records.
  - The Agent must monitor the “Call Awaiting Triage” queue regularly and manage it. There are two ways to navigate to view the triage queues.
  - The Management Dashboard (Figure 10) shows zero tickets in the queue. If there is one or more, the Agent must check the Calls Awaiting Triage queue, process the call record, and perform the classification process.

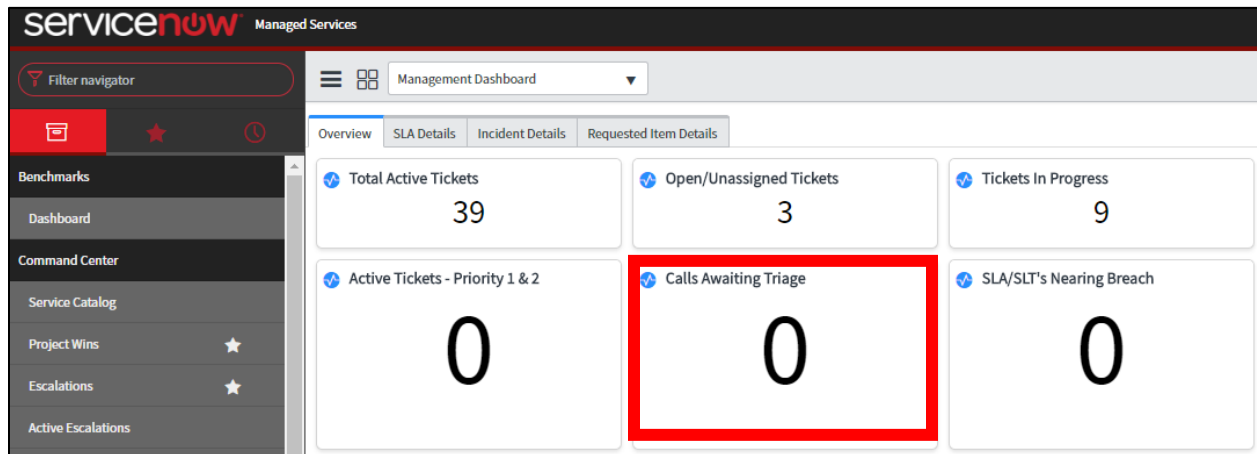
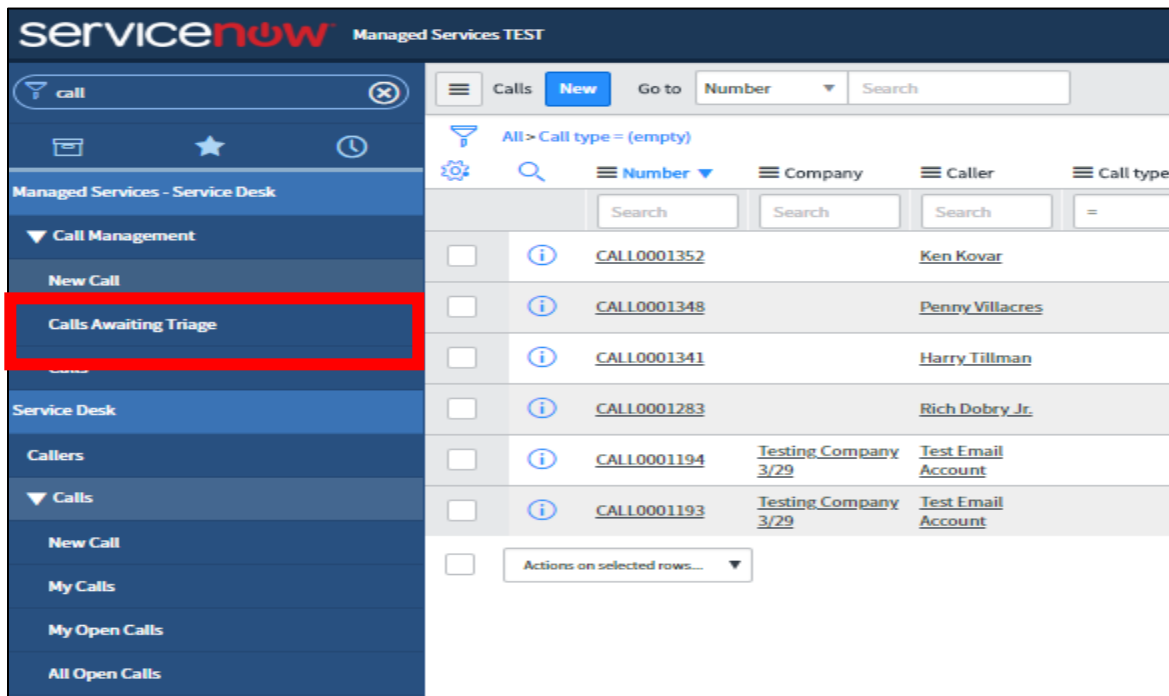


Figure 9: MS ServiceNow Management Dashboard – Overview – Calls Awaiting Triage

- Inside the square in Figure 11, the Agent can Navigate to the queue. If there is a record in the triage queue, then the Agent should process the call and perform the same process as above.



**Figure 10: MS ServiceNow Navigation Access – Calls Awaiting Triage**

- The idea is to keep this queue to zero. These requests are not supposed to be P1 or P2. However, these requests could be intricate in nature and may require engaging the Client Experience Champion. If the call is an incident, the SLA starts as soon as the Agent creates the call record. The urgency to classify the call quickly would be to determine which group should handle the Incident. Once the Agent transfers the ticket correctly, the Incident ticket can follow the expected service levels as appropriate. If the issue is a P1 or P2 incident, then the Agent must follow documented desk procedures.
- **Customer logs in to the Customer Service Portal and Reports an Issue** – Command Center Service Desk agent monitors the incident queue. After the customer submits an issue and generates the ticket, it will show up in the Unassigned Incidents in the Management Dashboard (see Figure 12). Figure 13 shows an alternate way to access the Unassigned Incidents queue. Navigate to the “Open – Unassigned” item on the ServiceNow left menu bar. The Agent must check this queue at regular intervals.

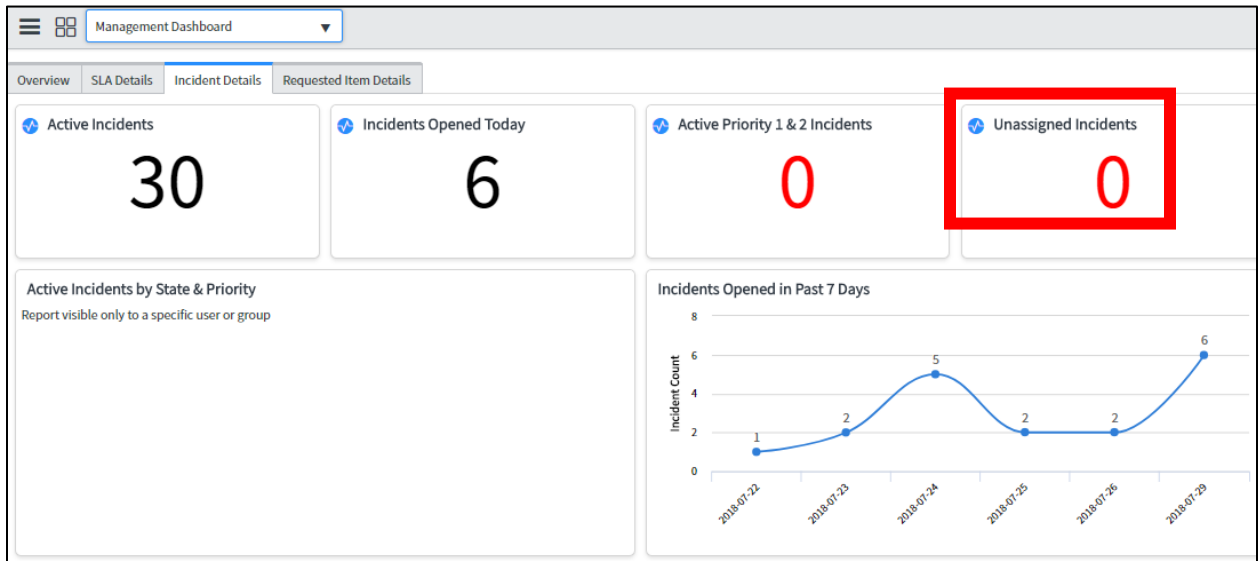


Figure 11: MS ServiceNow Management Dashboard – Incident Details – Unassigned Incidents

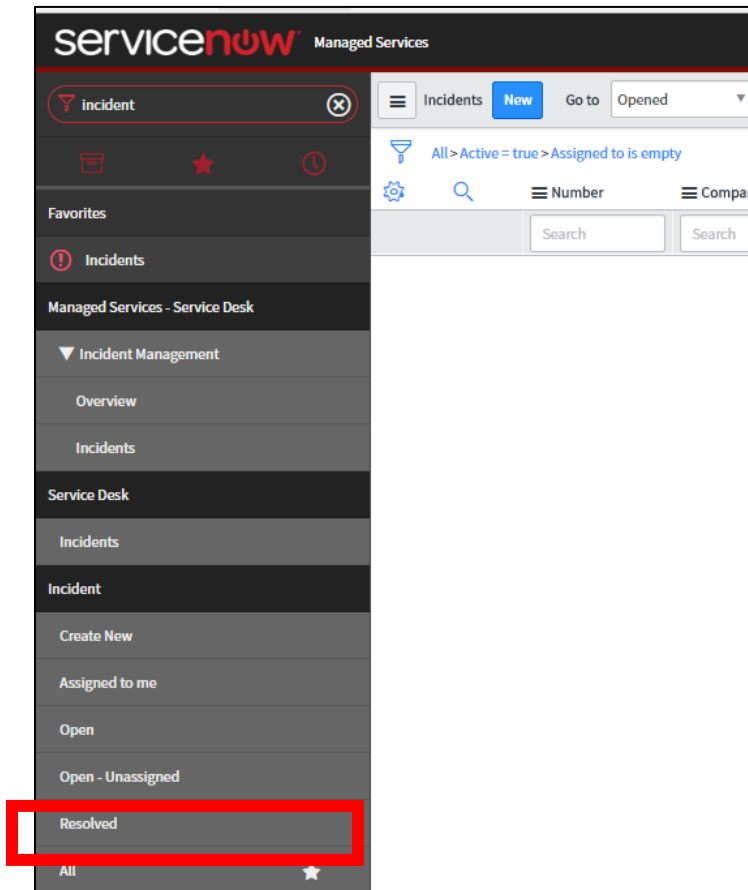


Figure 12: MS ServiceNow Navigation Access – Open – Unassigned

## 9 Incident Record Escalations

While troubleshooting a P2, P3, or P4 incident record, if the support engineer needs to escalate to the next support level, the ticket assignee will provide warm transfers. P1 incidents shall follow the MI Process.

### 9.1 Tier 2 Requires Command Center SA Tier 3 or 4 Support:

- Tier 2 will update the Incident with all troubleshooting steps taken.
- Tier 2 will call the Service Desk and provide the incident number.
- SD calls the on-call TOM.
- SD assigns Incident tickets to the on-call TOM.
- The TOM on-call contacts Tier 3 or Tier 4 to review the Incident.
- The TOM on-call will organize a conference with the client or Tier 2 if needed for troubleshooting.
- The TOM on-call manages ticket notes, ensures that Tier 3 or 4 updates the ticket with technical details.
- The TOM on-call manages the Incident communique.

### 9.2 The Command Center Requires Tier 2 or Tier 3:

- The TOM will contact the SD to notify Tier 2 that their assistance is needed.
- SD will contact Tier 2 and provide the incident number.
- SD will provide bridge details to Tier 2 to join incident troubleshooting if needed.
- SD will stay assigned as an additional assignee to track progress.

## 10 MI Management

### Objective:

A MI is a service interruption to critical business functions. Support teams must handle them with great urgency. The aim is the quick recovery of the service, and where necessary, using a workaround. If required, specialist support groups or third-party suppliers (Tier 3 and Tier 4) are involved. Once the team brings the environment to a steady-state using a workaround, the problem manager raises a problem ticket to investigate the root cause and design and implement a permanent solution.

### Key Steps include:

- Identifying an MI.
- MI - Key Characteristics.
- Handling of an MI.
- MI review.
- Notification of Service Failure and constant updates.

### 10.1 Identifying an MI

The customer impact is the most common criteria used to determine if a reported issue is an MI. Below are some of the examples.

- A corrupted critical business database.

- Company-wide MS Exchange/Email communication down.
- Inbound and outbound Network communication outage
- Company website down due to hefty traffic (for example to make purchases or book incidents or due to a cyber-attack) affecting business services and sales
- Virus cyber-attack on critical business servers
- Confidential information like personal details of a vast number of individuals disclosed on the Internet or hacked
- Most of the disaster that will need attention by the DR-BCP would constitute an MI; it may so happen that many incidents can lead to a single MI.

## 10.2 MI Key Characteristics

An MI is also likely to be categorized as a critical or high priority incident. Below are some of the main characteristics that constitute an MI.

- The cost to customers and is or will be substantial, both in terms of direct and indirect financial damages (including consequential loss).
- The ability of significant numbers of customers to use services or systems is or will be affected.
- The reputation of the customer or one of its customers is likely to be damaged.

***At times the amount of effort or time required to manage and resolve the Incident is likely to be significant, and the support team may breach agreed service levels (target resolution times).***

## 10.3 Handling a MI

The response to an MI is a shorter timeframe than that of a typical incident. It is critical to understand the SLA and SLT expectations per customer agreements.

**Note:** Tier 2 will warm contact our Tier 1 Service desk for any Critical incident generated by our monitoring tool. They will call (800-868-1525) and notify Tier 1 of an incoming P1 Critical incident.

Concerning MIs:

1. Caller contact SD (Email/Portal/Phone - preferred)
2. SD performs triage (registration, and initial investigation, starts bridge)
3. Start a bridge add Tom-on-call as alternate host, record bridge in INC
4. Assign ticket to Tier 2
5. Contact Tier 2 on-call
6. Contact TOM on-call and do warm hand-off
7. SD notifies MS Senior Leadership to determine communication plan
8. Diagnosis and Escalation
  - a. TOMs starts the clock and begins updating the ticket
    - i. Escalate to Tier 3 if not resolved in 60 minutes. Start contacting Tier 3 at 50th minute
    - ii. Escalate to Tier 4 if not resolved in 120 minutes start contacting Tier 4 at 110th minute



- iii. Give Tier 4 30 mins to get the history and ask if it is possible that we start an OEM ticket. Engineers should contact 3rd party supplier and invite them to the bridge
  - b. All troubleshoot until resolution
  - c. Complete and submit Root Cause Analysis (RCA)
9. Incident closure
  - a. TOM resolves Incident once RCA is attached.

### **MI Coordination**

An MI is an event with significant business impact and requiring an immediate coordinated effort. Due to the criticality of the circumstance, the on-call TOM manages and coordinates MI activities from inception to resolution. When the support team resolves the Incident, the TOM conducts a review of the Incident and coordinates all follow-up actions.

### **Confirming an MI Candidate**

End-users may consider a disruption as an MI. However, the user cannot instantly promote the issue to an MI. Users cannot do this because the MI process triggers several actions and activities in other teams of which said user is unaware. For this reason, during Incident Registration, the Service Desk initially proposes the disruption as a MI Candidate. The TOM can then confirm that MSO should execute the MI process. There are two possible ways to do this:

- Manually from an existing Incident.
- Manually where no Incident exists.

## **10.4 Root Cause Analysis**

The TOM on-call obtains the root cause and supporting information, completes the RCA form, and attaches it to the Incident record. After this, the TOM resolves the ticket, and the Incident ticket goes through normal closure activities.

## **10.5 MI Review**

Post MI resolution, the TOM conducts a Major Incident review session with WWT internal and external stakeholders to go over the event. The process involves reviewing the sequence of events as discovered during the diagnosis activities, communicating the root cause, contributing factors, resolution, corrective plans, and lessons learned. During the MI review session, the TOM on-call will place the Incident Pending state. After completing the review, the TOM will resolve the Incident, and the ticket will go through the standard closure process.

### **Closed-Loop Corrective Action**

The TOM on-call will perform a weekly review of MIs with the customer and technical teams. As part of the review, the engineering team will provide recommendations to stakeholders of appropriate problem remediation steps. The TOM will maintain records of corrective actions, advice, lessons learned, problem identification, RCA, and remediation steps in the ServiceNow KB.

## **11 References**

**Table 8: Table of References**

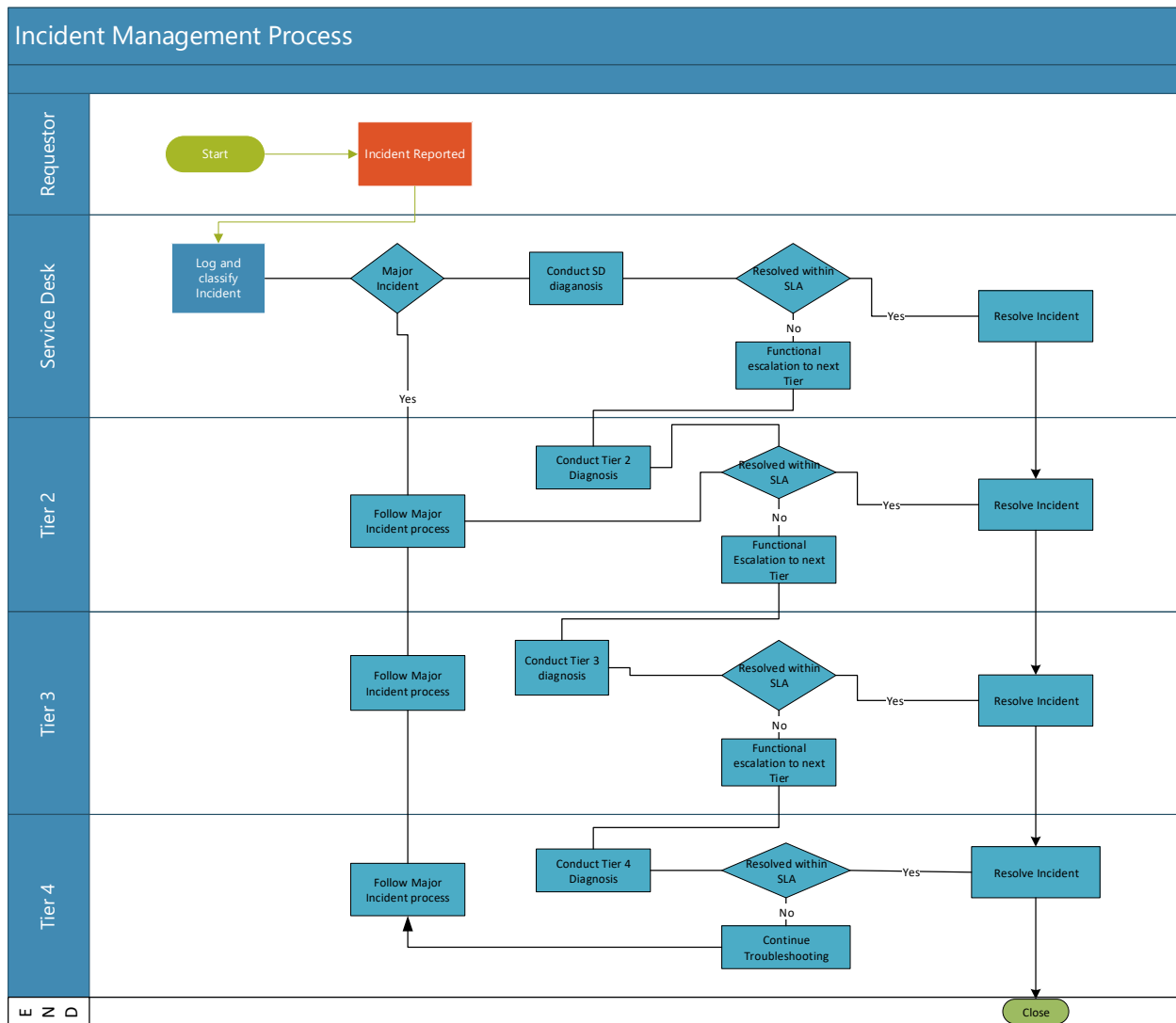
References	Relationship
Traceability	ISO 2000:2011, ISO 9001:2015, ITIL 4
Policy	Incident Management Policy
Tools	ServiceNow
Incident Management ITIL V4 Practice Guide	ITIL V4 Standards Guide and Best Practice

## 12 Definitions

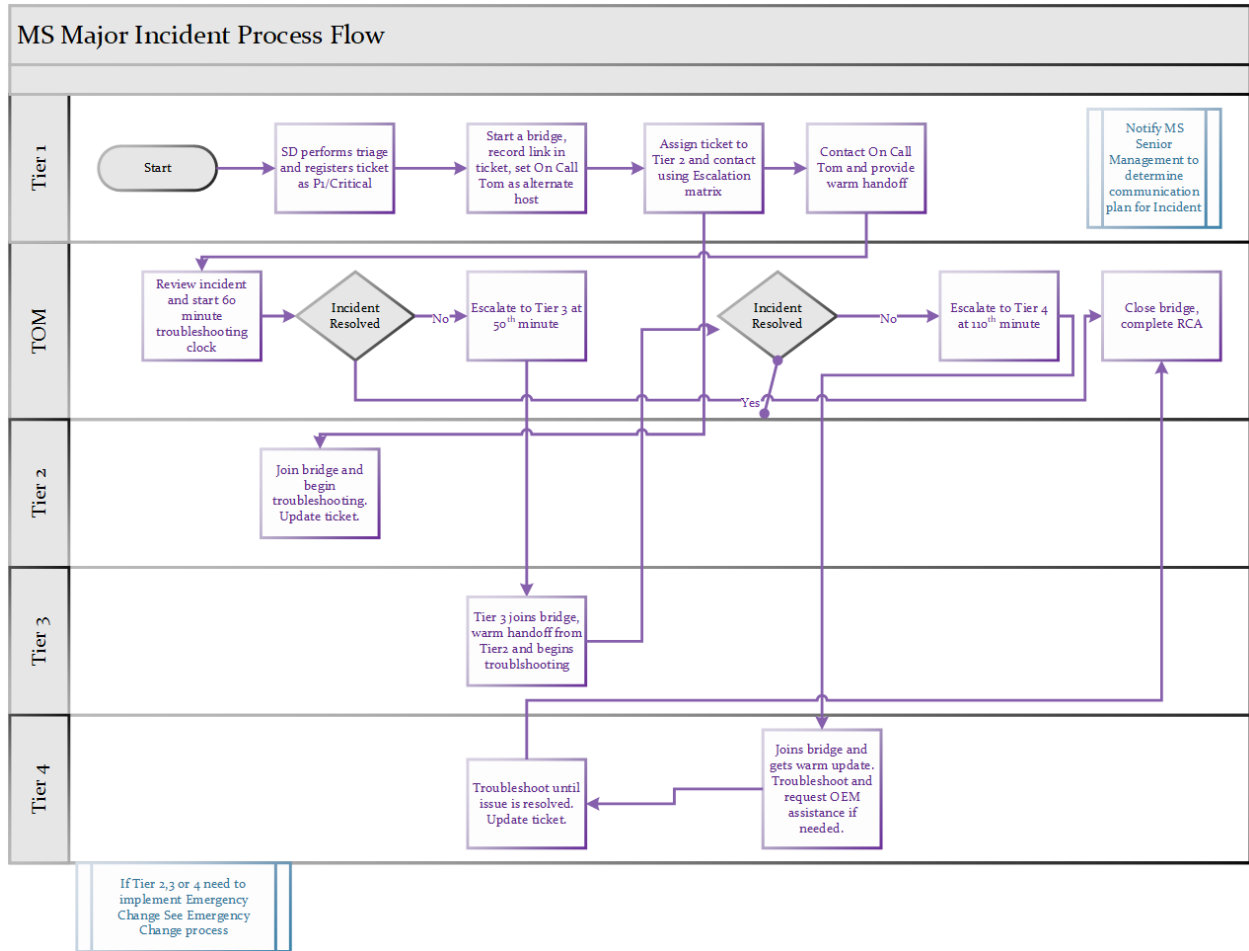
**Table 9: Table of Definitions**

Term	Meaning
Business Impact Assessment (BIA)	BIA is a business continuity management activity that identifies vital business functions and their dependencies and service recovery activities requirements. These requirements include recovery time objectives, recovery point objectives, and minimum service level targets for each service.
Customer	The entity paying for WWT the MS offering.
Incident	A request to resolve an unplanned interruption to, or a reduction in quality of service, system, or component. A malfunction with a business system or component that has not yet affected service is also considered an incident.
Incident Record	MS ServiceNow ticket to record and track reported incidents.
Response	The time duration to assign the ticket to a support team member.
Resolution	The time duration to solve the Incident through the application of a workaround or change.
Restoration	Return of regular service operation to the users after repair and recovery from an incident.
User	The individual who uses or consumes a WWT Managed Service offerings daily.
Workaround	The reduction or elimination of the impact of an incident for which a full resolution is not available. A temporary way of overcoming symptoms until the solution team defines and implements a justifiable permanent solution.
TOM	Technical Operations Manager (MI Manager).

## Appendix A: Incident Process Flow



## Appendix B: MI Process Flow



## Appendix C: ServiceNow Field Definitions for New Call and Incident

ServiceNow Fields	Field Definition
<b>New Call</b>	
<b>Number</b>	Each new call record will have a unique identifier on the upper left-hand side of the New call record. The naming configuration will start with "Call," proceeded by a number. EX. CALL001243.
<b>Opened</b>	Date and Time Opened.
<b>Company</b>	Customer/Client-Agent will select the appropriate account when opening a new call record.
<b>Opened By</b>	Agent or Customer (email requests).
<b>Location</b>	The Agent will enter the location of the Incident and CI impacted by the reported issue.
<b>Contact Type</b>	In the Contact Type Field, Agent will select the option that applies, such as email or phone. This field can be auto-populated, depending on how the Service Desk opens the record.
<b>Site ID</b>	Each account/client will have a unique identifier that will auto-populate when the location is selected.
<b>Call Type</b>	The Agent will select the appropriate call type concerning the new Call: <ul style="list-style-type: none"> <li>• Incident</li> <li>• Request</li> <li>• Status Call</li> <li>• Not Supported by WWT</li> <li>• Hang up/Wrong Number</li> <li>• Compliment</li> <li>• Complaint</li> </ul>
<b>Caller</b>	The Agent enters the account's authorized Caller, or a WWT resource can open the record on the customer's behalf.
<b>Business Service</b>	Service area affected: Managed Services = all services supported by the MS team. CPMigrator = All services maintained by CPMigrator team for PS; Non-MS clients.
<b>Business Phone</b>	Phone Contact.
<b>Mobile Phone</b>	Phone Contact.
<b>Short Description</b>	Should contain a short synopsis for the call, for example: <ul style="list-style-type: none"> <li>• Tech could not complete Step 3 for PC to PC migration.</li> <li>• Tech could not find Config File.</li> </ul>
<b>Description (Customer Visible)</b>	These are detailed notes. The Agent will describe the reported issue in detail, the impacted CIs, how many users are affected, and document the troubleshooting attempted to resolve.

ServiceNow Fields	Field Definition
<b>Incident Record</b>	
<b>Number</b>	Incident Number-When an incident is opened, it will create a unique identifier in the upper left-hand of the record. The ID will start with “INC,” proceeded by numbers. EX. INC0012153
<b>State</b>	Incident state Agent will select the appropriate drop-down item: <ul style="list-style-type: none"> <li>• New</li> <li>• In progress</li> <li>• Pending</li> <li>• Resolved</li> <li>• Canceled</li> </ul> Refer to Appendix A.
<b>Contact Type</b>	In the Contact Type Field, the Agent will select the option that applies: email or phone.
<b>Company</b>	Customer/Client-Agent will select the appropriate account when opening a new incident record.
<b>Location</b>	The Agent will enter the location of the Incident and CI impacted by the reported issue.
<b>Site ID</b>	Each account/client will have a unique identifier that will auto-populate when the location is selected.
<b>Caller</b>	Authorized client listed under the account or automated monitoring system generating the request.
<b>Assignment Group</b>	Workgroup resolving or assigned to resolve an incident, examples include: <ul style="list-style-type: none"> <li>• Tier 1-MS Support</li> <li>• Tier 2-MS Support</li> <li>• Tier 2-CPMigrator</li> <li>• Tier 3-MS Support</li> <li>• Tier 3-CPMigrator</li> <li>• ScienceLogic Admins</li> </ul>
<b>Assigned To</b>	Agent or Assigned Group member working the Incident to resolution.
<b>Time Worked</b>	Work duration on Incident.
<b>Impact</b>	The Agent will select the appropriate impact: <ul style="list-style-type: none"> <li>• 1-High</li> <li>• 2-Medium</li> <li>• 3-Low</li> </ul> Reference Table 4.

ServiceNow Fields	Field Definition
<b>Urgency</b>	The Agent will select appropriate urgency: <ul style="list-style-type: none"> <li>• 1-High</li> <li>• 2-Medium</li> <li>• 3-Low</li> </ul> Reference Table 4.
<b>Priority</b>	Calculated based on the Impact and Urgency. Please see the matrix in Table 4.
<b>Category</b>	See Table 6.
<b>Subcategory</b>	See Table 6.
<b>Business Service</b>	Service area affected; add the appropriate service to the ticket, <i>e.g.</i> , MS; CPMigrator Support.
<b>Configuration Item</b>	Application or system impacted.
<b>Notes →Customer Notes List</b>	This field contains a list of customer stakeholders, including the Caller, to receive a copy of customer notes added to the Incident. The Service Desk can add other customer contacts as needed for visibility.
<b>Notes →Internal Notes List</b>	This field holds a list of Internal stakeholders who have an interest in the progress of the ticket. The assignee can include additional agents or management for extra visibility.
<b>Notes →Internal Notes</b>	The Agent will log incident notes in real-time, capturing any troubleshooting and resolution details as the support Agent is working on the Incident
<b>Notes →Activities</b>	Running history of notes and incident updates, agents should be updating incidents in real-time capturing troubleshooting and resolution details.
<b>Related Records →Problem</b>	Relate incidents to a problem record, if there is a parent-child relationship to other reported incidents.
<b>Related Records →Change Request</b>	Relate incidents to a scheduled change.
<b>Related Records →Caused by Change</b>	Relate incidents to implemented changes via this field.
<b>Resolution and Recovery →Resolution Code</b>	Select the appropriate resolution from the drop-down menu: <ul style="list-style-type: none"> <li>• (From) KB</li> <li>• Solved (Undocumented Solution)</li> <li>• Solved (Work Around)</li> </ul>
<b>Resolution and Recovery →Closed By</b>	Agent or group closing record.
<b>Resolution and Recovery →Closed</b>	Date and time the record is closed.
<b>Resolution and Recovery →Resolution Notes</b>	Notes documenting resolution include actions and steps used to resolve the Incident.

---

ServiceNow Fields	Field Definition
<b>Affected CI's</b> →	Application or Systems Impacted by the threshold breach.
<b>Affected Time Worked</b>	Work Duration of Incident, the time it took to resolve the Incident.
<b>Affected Task SLA's (1)</b> →	SLA response time.



## 13 Version Control

Version	Date	Author/Contributor	Summary of Changes
V1.0 Draft	06.30.20	Julie Somerville, Leslie Okere	Updating Template SOP to MS Incident Management SOP.
V1.0 Draft	07.29.20	Bizzy Gonacha, Kay Bryant	Technical edit
V1.0 Draft	08.01.20	Julie Somerville, Leslie Okere	Additional edits
V1.0 Published	08.21.20	Bizzy Gonacha, Kay Bryant	Technical edit and publishing
V1.1	03.22.21	Leslie Okere, Julie Somerville	Added BR for updating tickets, removed phone number for on-call TOM. Replaced MIM flow diagram.
V1.1 Published	04.16.21	Bizzy Gonacha, Kay Bryant	Technical edit and publish.
V1.2	07.08.21	Leslie Okere, Julie Somerville	Update SD email. Updated MIM process steps.
V1.2	07.15.21	Bizzy Gonacha, Kay Bryant	Technical edit and publish.