EFFECTIVE DATE

(07-26-2023)

PURPOSE

(1) This transmits revised IRM 2.148.2, IT Support Services Management, Incident Management Process.

MATERIAL CHANGES

(1) Revised entire document with updated IT IRM policy and process templates incorporating required internal controls.

EFFECT ON OTHER DOCUMENTS

IRM 2.148.2 dated May 11, 2020 is superseded.

AUDIENCE

This process description is applicable to all organizations within the IRS requesting Information Technology (IT) support through the IT Service Desk, by anyone in the Internal Revenue Service Information Technology (IRS IT) following the IRM 2.148 who has the responsibility of providing service and support to Information Technology customers.

Kaschit Pandya
Acting, Chief Information Officer

2.148.2
Incident Management Process

Table of Contents

2.148.2.1
(07-26-2023)
Program Scope and Objectives

(1) Overview - IRM 2.148.2 describes the formal process for managing the Incident Management process.

(2) Purpose - This Internal Revenue Manual (IRM) describes the formal process for implementing the requirements of the Incident Management Process.

(3) Audience - The primary users of IRM 2.148.2 are all organizations within the IRS requesting IT support through the IT Service Desk.

(4) Policy Owner - The policy owner is the User and Network Services (UNS), Associate Chief Information Officer (ACIO), who is responsible for oversight of Incident Management.

(5) Program Owner - UNS is the program owner for Incident Management.

(6) Primary Stakeholders - The primary stakeholders are UNS, Enterprise Operations (EOps), Strategy & Planning (S&P), Application Development (AD), Cybersecurity, and Enterprise Services (ES).

(7) Program Goals - Successfully manage the lifecycle of an Incident and restore service as quickly as possible.

2.148.2.1.1
(07-26-2023)
Background

(1) This IRM describes what happens within the Incident Management Process and provides an operational definition of the major components. Incident Management is the process responsible for recording and tracking incidents throughout their lifecycle. The major phases within the Incident Management Process are defined further in this document and accompanied with a visual diagram in Figure 2.148.2-1. The Incident Management Process can only be tailored in extenuating circumstances with the prior approval of the Process Owner.

2.148.2.1.1.1
(07-26-2023)
Objectives and Goals

(1) This IRM describes a set of interrelated activities to achieve a given purpose and states the guidelines that all projects should follow regarding the Incident Management Process. The document also includes metrics, role definitions, and other process related attributes.

(2) Specific Process Goals:

- Incidents are properly logged and coded
- Incidents are properly routed
- Incident reassignments are properly documented
- Incident state is accurately reported
- Queue of unresolved incidents is visible and reported
- Incidents are properly prioritized and handled accordingly
- The Service Level Agreement (SLA) targets are met

2.148.2.1.2
(07-26-2023)
Authority

(1) All proposed changes to this document should be directed to the IRS IT UNS Customer Service Support (CSS) Director as owner of this process.

2.148.2.1.3
(07-26-2023)
Roles and Responsibilities

(1) Each role is assigned to perform specific tasks within the process. The responsibilities of a role are confined to the specific process. Within a specific process, there can be more than one individual associated with a specific role. Additionally, a single individual can assume more than one role within the process, although typically not at the same time. The following roles have been identified for this process:

Name	Description
Process Owner	Accountable for ensuring that a Process is Fit for Purpose. The Process Owner's responsibilities include sponsorship, Design, Change Management, the continual improvement of the process and its metrics, and performing the review of service (provided measuring customer satisfaction, field coding, accuracy of assignment groups, etc.).
Process Manager	Responsible for Operational management of a Process. The Process Manager's responsibilities include planning and coordination of all activities required to carrying out, monitoring and reporting on the Process, and managing review of service.
Incident Manager of Record	Executive, Director, Senior Manager or Branch Chief that is designated and trained to lead the activities of resolving an incident, updating an incident record, sending out periodic email updates to leadership and applicable personnel, and maintaining incident record quality.
First Level Support / IT Service Desk Specialist	Responsible for performing any procedures related to incidents, from recording to closure, using the approved instructions in the Incident Management Knowledge Base (KB). Reviews and monitors progress of incidents. Provides status updates to customers.
Second Level Support	Responsible for routine incidents, as well as providing a higher level of technical expertise for specific incidents when the incidents cannot be resolved by the First Level Support IT Service Desk Specialist.
Service Provider	Any organization that delivers a standard service or product to a Customer.

Name	Description
Service Operations Specialist	An IT specialist trained in Incident Management (IM) Escalation, skilled in evaluating IM outages for the purpose of coordinating and escalating P1 and P2 incidents for premium and non-premium production outages, when resolutions to these outages aren't achieved within the ITIL IM guidelines.
Total Contact Ownership	IT Service Desk Personnel that are assigned to the escalation gate with focus on oversight and monitoring of P1 and P2 incidents.
Customer	The Customer of an IT Service Provider is the person or group who defines and agrees on the Service Level targets.

2.148.2.1.4
(07-26-2023)
Program Management and Review

(1) Customer Satisfaction Surveys, Quality Reviews, IT Service Manager dashboards, and monthly metrics reviews measure the effectiveness of the Incident Management program.

2.148.2.1.5
(07-26-2023)
Program Controls

(1) Controls are activities involved in ensuring a process is predictable, stable, and consistently operating at the target level of performance. They represent the policies and guiding principles on how the process will operate, and provide direction over the operation of processes and define constraints or boundaries the process must operate within.

2.148.2.1.5.1
(07-26-2023)
Metrics

(1) Metrics are used for the quantitative and periodic assessment of the Incident Management Process. They should be associated with targets that are set based on specific business objectives. Management will regularly review the metrics related to different aspects of the process to: make informed decisions; determine the success of the goals and objectives of the process; drive continual improvement of process effectiveness and efficiency; and take appropriate corrective action, if necessary.

(2) Examples of key measurements are:

- SLA breaches
- Average time to resolution
- Accuracy of incident coding and categorization
- Quality review - *KB00053008* **P1 and P2 Incident Quality Review**

2.148.2.1.6
(07-26-2023)
Terms/Definitions/Acronyms

(1) Definitions of Incident Management terms and acronyms.

2.148.2.1.6.1
(07-26-2023)
Defined Terms

(1) The definitions listed below are some commonly used terms and are provided as an aid to understanding Incident Management.

Terms	Definition
Configuration Item	A Configuration Item (CI) can be any piece of equipment or component that is tracked through a device record in Configuration Management.
Customer	The Customer of an IT Service Provider is the person or group who defines and agrees on the Service Level targets.
Escalation	An increase in the impact or urgency based on review of the severity.
Event	A change of state which has significance for the management of a CI or IT Service.
Impact	A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is used to assign Priority.
Incident	An unplanned interruption to an IT Service or a reduction in the quality of an IT Service.
Incident Record	A record containing the details of an Incident. Each incident record documents the lifecycle of a single Incident.
IT Service Management	The IT System that is used to record, classify, prioritize, document, provide supporting information, route, and track all events, incidents, problems, and requests within the IT environment.
Knowledge Article	An article providing written instructions or guidance on processes and procedures. Each article within the KB has an ID number and articles are often referred to by their Knowledge Base Article (KB#).
Knowledge Base	A published source of approved definitive workarounds and solutions for incidents and known errors, located within the Information Technology Service Management (ITSM) tool.
Known Error	A Problem that has a documented root cause and workaround that exists in the Knowledge Base.
Priority	Used to identify the relative importance of an incident, problem or change. Priority is based on Impact and Urgency and is used to identify required times for actions to be taken.

Terms	Definition
Problem	A cause of one or more incidents. The cause is not usually known at the time a Problem record is created and the PM Process is responsible for further investigation.
Problem Management	The Process responsible for managing the lifecycle of all problems. PM proactively prevents Incidents from happening and minimizes the impact of incidents that cannot be prevented.
Process Review	Review of incident to ensure that all internal processes were followed and documented to expedite problem resolution.
Resolution	Action taken to resolve an incident or problem, or to implement a workaround.
Role	A set of responsibilities, activities and authorities granted to a person or team. A Role is defined in a process. One person or team may have multiple Roles. For example, the Roles of Configuration Manager and Change Manager may be carried out by a single person.
Service Level Agreement	An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level targets, and specifies the responsibilities of the IT Service Provider and Customer. A single SLA may cover multiple IT Services or multiple Customers.
State	The name of a required field in many types of record. It shows the current stage in the lifecycle of the associated CI, incident, problem etc.
Urgency	A measure of how long it will be until an incident, problem or change has a significant Impact on the business. The lower the value number, the sooner it must be addressed. Urgency is used to assign Priority.
Workaround	Reducing or eliminating the Impact of an incident or problem for which a full resolution is not yet available.

2.148.2.1.6.2
(07-26-2023)
Acronyms

(1) The abbreviations and acronyms include an alphabetical listing of some commonly used terms in Incident Management.

Acronyms	Definition
ACIO	Associate Chief Information Officer
AD	Applications Development
CI	Configuration Item
CIO	Chief Information Officer
CSS	Customer Service Support
EOps	Enterprise Operations
IM	Incident Management
IMR	Incident Manager of Record
IRM	Internal Revenue Manual
IT	Information Technology
ITOCC	Information Technology Operations Command Center
ITSM	Information Technology Service Management
KB	Knowledge Base
PMR	Problem Manager of Record
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SOS	Service Operations Specialist
TCO	Total Contact Ownership
UNS	User and Network Services

2.148.2.1.7
(07-26-2023)
Related Resources

(1) Related Directives are:

- CIO, ACIO approved official Playbooks
- CIO, ACIO approved business rules
- CIO, ACIO approved measures

2.148.2.1.8
(07-26-2023)
Training

(1) Incident Manager of Record (IMR) Training

(2) Problem Manager of Record (PMR) Training

(3) Major Outage SOP Overview Training

(4) IMR Incident Management Tabletop Exercises

(5) Change Management Overview

(6) IMR Checklist, User Guide and Trifold (*ITOCC Central*)

2.148.2.2
(07-26-2023)
Process Workflow

(1) The IT Management Process Workflow consists of 6 phases, starting after an incident has been identified, and ending after incident closure. Below are the 6 phases and their descriptions:

Phase 1 - Incident Recording

- An incident has been identified and must be recorded in the ITSM tool.

Phase 2 - Triage

- A preliminary assessment of the incident must occur to determine if the incident can be resolved, or if it needs to be routed to a specialized service provider.
- When an incident is reassigned, a written justification should be documented along with a statement for actions needed.

Phase 3 - Severity Assessment

- The incident's priority is calculated using urgency and impact metrics. Refer to
KB00013646 **Business Rules for Prioritizing Incidents**.

Phase 4 - Troubleshooting and Remediation

- The incident follows protocol based off its determined priority, along with Knowledge Base (KB) research to determine a potential resolution.
- If an assessment call is needed/required for a P1/P2 Incident, it will occur in this Phase.

Phase 5 - Resolution

- The service is restored via workaround or permanent resolution.
- Knowledge should be created/updated if appropriate.
- If the Root Cause is not identified, consider the Problem Candidate Process. Refer to
KB00048127 **Identifying an Incident as a Problem Candidate**.

Phase 6 - Closure

- The record is closed after incident resolution is successful, and customer concurrence is obtained (if applicable).

2.148.2.2.1
(07-26-2023)
Main Process Diagram

(1) IT Incident Management Process Diagram

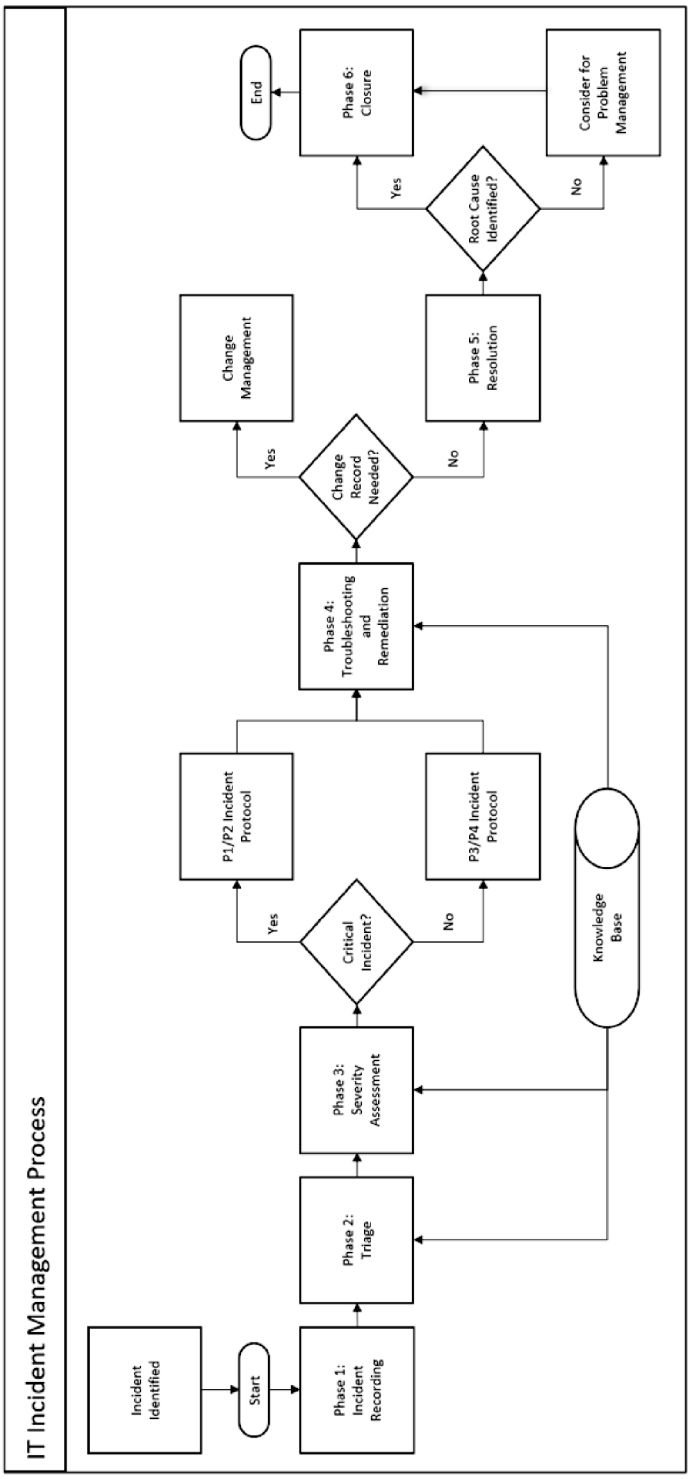

Figure 2.148.2-1

2.148.2.2.2
(07-26-2023)
Priorities

(1) Priority code values range 1 to 4. The Priority code is calculated by a formula that is based on the Impact and Urgency rating of the Incident. For more information on Priority, Impact, Urgency, and related SLA calculations, please reference
KB00013646 **Business Rules for Prioritizing Incidents**.