Signature Page

Name	Meaning	Date & Time of Signature (DD/MM/YYYY hh:mm:ss UTC)
COLE Mark	Writing	21/10/2019 11:33:43
MARCIANO Frederic	Proofreading	24/10/2019 08:36:40
WILLS Caroline	Approval	31/10/2019 20:02:25

Table of Contents

1. PURPOSE AND OBJECTIVES

The purpose of this procedure is to define the mandatory process for Incident Management by all Sanofi ITS teams.

2. SCOPE

This Incident Management procedure applies to the entire global Sanofi ITS organization, Sanofi employees outside of ITS that support ITS Service Management processes, and to external service providers who support Sanofi ITS – including all Application Maintenance & Support (AMS), Infrastructure Maintenance & Support (IMS), and Service Desk vendors.

3. DEFINITIONS AND ACRONYMS

Please refer to the Sanofi ITS Glossary for the definition of ITS Service Management terms.

3.1 DEFINITIONS

Incident: An Incident is defined as an unplanned interruption or a reduction in the quality of an IT service, or a failure of a configuration item (CI) that has not yet impacted an IT service

ITS Solution: The key, customer-relevant technology that is used to deliver one or more business services or outcomes

Key-User: An end-user of ITS services with special training on a particular service that may assist or augment ITS staff in support of the service

Known Error: A Known Error is a problem that has a documented root cause and a Workaround. A Known Error might have a permanent solution, or it may stay open forever. A Known Error can be closed when a permanent solution has been found and implemented, through a change if necessary

Outage: The complete unavailability of an ITS Service Offering to the entire or significant portion of the user community

Problem: Unknown cause of one or more Incidents

Service Offering: A service variant that represents a meaningful difference in service level commitment, application, support structure, application instance, subscription, etc.

Service Level Agreement: Within an Incident, SLA is the target time for the Incident resolution

Workaround: A Workaround is a temporary way of overcoming the difficulties of an Incident. A Workaround is valid until a permanent solution is implemented

Validated Critical Incident: This flag is checked when both the Sanofi Control Tower and the Incident Manager agree that an Incident has been properly prioritized as a “P1-Critical”

3.2 ACRONYMS

AMS: Application Maintenance & Support

CI: Configuration Item

GxP: Regulations such as Good Clinical Practice (GCP), Good Laboratory Practice (GLP), Good Manufacturing Practice (GMP) and Good Distribution Practice (GDP), as well as any other regulations applicable to Sanofi

IMS: Infrastructure Maintenance & Support

ITS: Information Technology & Solutions

ITSM: Information Technology Service Management

KE: Known Event

KPI: Key Performance Indicator

OLA: Operational Level Agreement

PRB: Problem record within the ITSM Solution

RCA: Root Cause Analysis

RFC: Request for Change

SLA: Service Level Agreement

SLM: Service Level Management

SME: Subject Matter Expert

VIP: Very Important Person

4. REFERENCES

Global Standard Operating Procedure *ITS: Asset Management* (GDSOP-014177)

Global Standard Operating Procedure *ITS: Change Management* (GDSOP-014174)

Global Standard Operating Procedure *ITS: Configuration Management* (GDSOP-014175)

Global Work Instruction *Incident Management Priority Setting* (GDWIN-000028)

Global Work Instruction *Incident Manager* (GDWIN-000027)

Global Standard Operating Procedure *ITS: Knowledge Management* (GDSOP-014173)

Global Standard Operating Procedure *ITS: Problem Management* (GDSOP-014180)

Global Standard Operating Procedure *ITS: Quality Risk Management* (GDSOP-014163)

Global Operational Standard *ITS: Service Management* (GDOPS-014349)

Global Standard Operating Procedure *ITS: Service Level Management* (GDSOP-014166)

Global Supporting Document *ITS: Service Level and Operational Level Key Performance Indicators* (GDSD-014450)

5. PROCEDURE

5.1 PRINCIPLES AND BASIC CONCEPTS

5.1.1 Incident Resolution Time Frame

Incident resolution timeframe targets are specified in the Service Level Management procedure and configured within the Sanofi ITS Standard ITSM Tool. Within the Incident record, the overall SLA for the application or platform is defined, as well as the remaining time available for the currently assigned group.

Details regarding Service Level Management process and the predefined time frames are captured in the following documents:

- *ITS: Service Level Management* (GDSOP-014166)
- *ITS: Service Level and Operational Level Key Performance Indicators* (GDSD-014450)

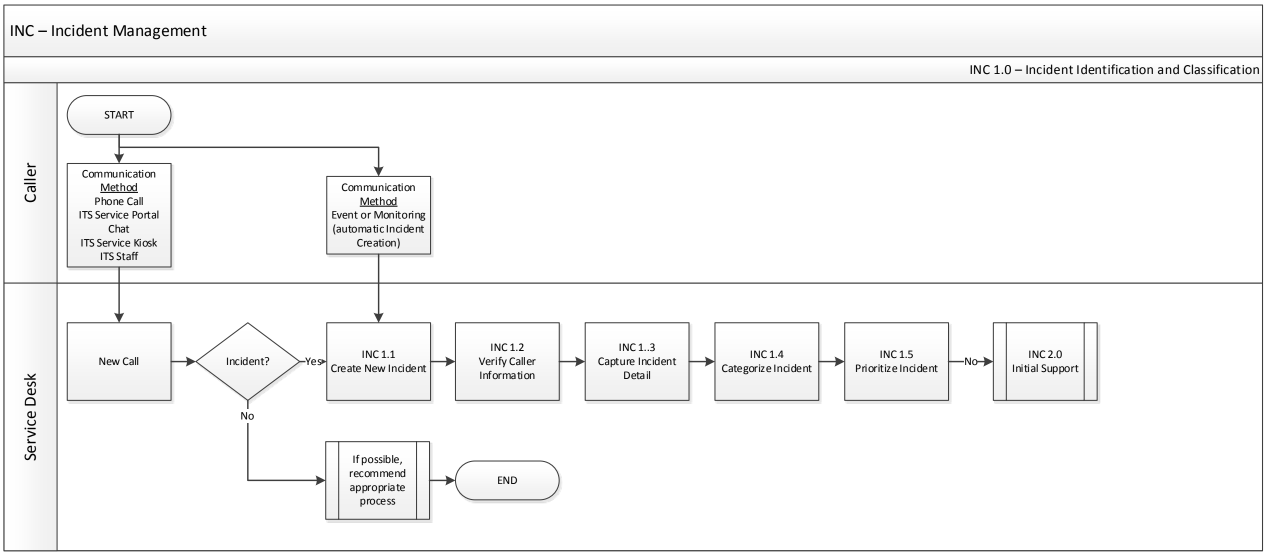
5.1.2 Incident States

Incidents are tracked throughout their lifecycle to support proper handling and reporting. The **State** of an Incident indicates where it is in relation to the lifecycle and helps determine the next step in the process. The Incident **State** values are:

- **New**: Newly created Incidents are initially set to this status. Typically, there is not yet an action taken on restoration of services
- **In Progress**: The Incident has been assigned to an assignment group. The interruption to services is under investigation and/or the services are in the process of being restored
- **Pending:** Before the Incident can be moved to the next State, there is some type of technical action / process to be performed or information is needed from the customer, a third party vendor or an internal Sanofi support team

  Pending Reasons may be awaiting Customer Feedback, Vendor, Awaiting Sanofi's Inputs or Technical Dependency. To understand how Service Level timeframes are impacted by Pending, refer to Global Supporting Document *ITS: Service Level and Operational Level Key Performance Indicators* (GDSD-014450)
- **Resolved**: The assignment group believes that services have been restored. All notes and transactions are added into the Incidents. Customer can accept the restoration or choose to re-open the Incident within a set number of days if the Incident is not resolved or recurs
- **Closed**: This is the final Incident state. The Incident cannot be modified further or re-opened

5.2 INC 1.0 INCIDENT IDENTIFICATION AND CLASSIFICATION


INC – Incident Management
INC 1.0 – Incident Identification and Classification
Caller
Service Desk
START
Communication Method
Phone Call
ITS Service Portal
Chat
ITS Service Kiosk
ITS Staff
Communication Method
Event or Monitoring (automatic Incident Creation)
New Call
Incident?
Yes
No
INC 1.1 Create New Incident
INC 1.2 Verify Caller Information
INC 1..3 Capture Incident Detail
INC 1.4 Categorize Incident
INC 1.5 Prioritize Incident
No
INC 2.0 Initial Support
If possible, recommend appropriate process
END

<u>INC 1.1</u> <u>Create New Incident</u>: The Service Desk determines if the Call is an Incident. If issue being reported is not an Incident, the Service Desk attempts to direct the Call to the appropriate Service Request or process. This applies to:

- Call records created via Customer Call / Chat or Self Service Entry
- ITS Staff creating Incidents directly
- Event Management and Monitoring tools automatically create the Incident and bypass the New Call step

From the time of Incident creation (from a Call), a Triage Timer will start. The Service Desk has an agreed amount of time to “triage” the Incident by filling in the required fields. The Triage Timer stops when the **Save** button is clicked. The purpose of the triage period is to quickly identify key attributes that determine the Priority and handling of the Incident. For details on the Triage Timer, please refer to Global Supporting Document *ITS: Service Level and Operational Level Key Performance Indicators* (GDSD-014450)

<u>INC 1.2</u> <u>Verify Caller Information</u>: The Service Desk looks up the user reporting the Incident (Caller) and ensures the contact information is correct by verifying:

- Name
- Contact Number
- Current Location
- Check for VIP status

The Service Desk updates any information as necessary on the Incident ticket only.

INC 1.3 Capture Incident Detail:

- Select the **Contact type**
- Summarize the Incident *from the customer perspective* in the **Short Description** field
- Select the appropriate **Service Offering**
  - The **Service Level Commitmen**t field will populate automatically based on the **Service Offering** selected. The Service Desk should refer to this to ensure the correct Service Offering was selected
  - The **Impact** field will populate automatically based on the **Service Offering** selected. Only individuals with the role of Incident Manager can modify the Impact
- Select a specific **Configuration item**, if known
- In the **Notes** section, the Service Desk provides any additional comments from the customer that gives more detail to other Assignment Groups. Examples include:
  - What is the Caller trying to do?
  - What is happening, what are they seeing?
  - Are other users experiencing the same situation?
  - When did the Incident first occur?
  - If there an error message, add text or screen-print to the Incident record

If the Incident represents a reoccurrence of a previous Incident for the same Caller and the Service Desk cannot resolve it via Incident Management, the Service Desk flags the issue for Problem Management.

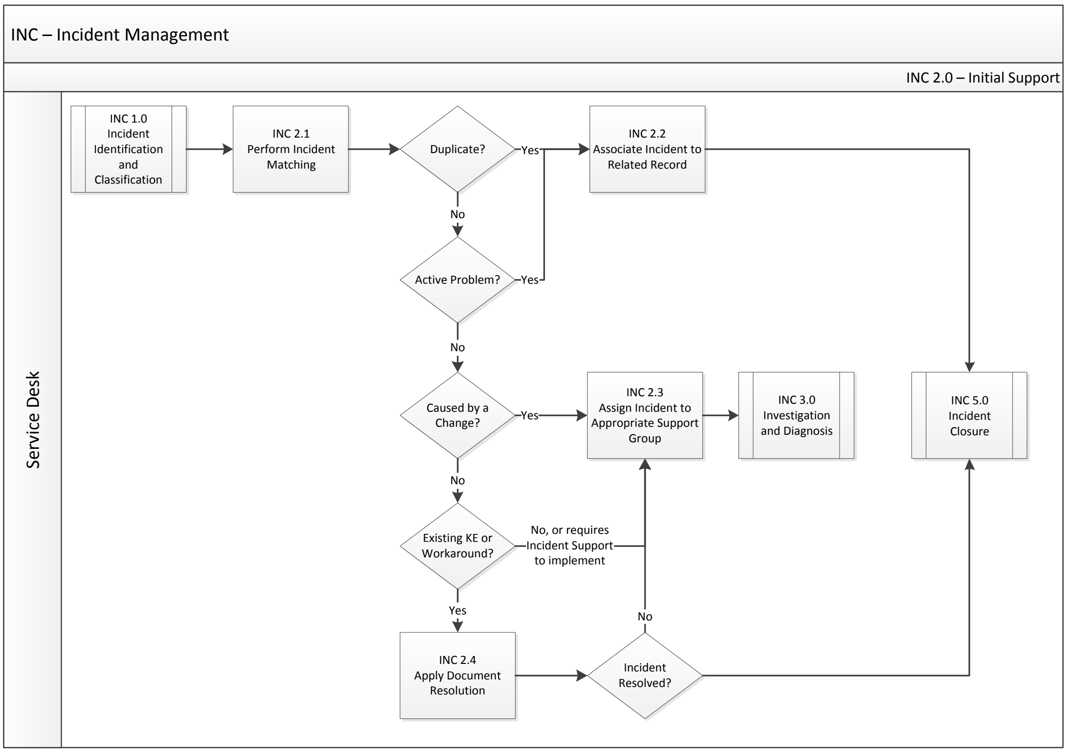
INC 1.4 Categorize Incident: Select the appropriate **Category** and **Symptom** as described by the Caller. The Category may be changed at resolution, if necessary.

INC 1.5 Prioritize Incident: To complete the prioritization of the Incident, the Service Desk selects the appropriate **Urgency**, based on information provided by the Caller. For detailed information on determining the **Urgency, Impact**, and **Priority** of an Incident, please refer Global Work Instruction *Incident Management Priority Setting* (GDWIN-000028)

Once the **Priority** is determined, the Incident Manager is responsible to apply the appropriate Incident Response Level. Please refer to Global Work Instruction *Incident Management Priority Setting* (GDWIN-000028).

For Event Management Incident Creation, Incidents identified through the use of Monitoring and Event Management tools are automatically created via electronic interface, or manually created by Vendor. When created automatically, the Event Management system provides categorization and initial assignment. This information must be confirmed by the assigned resource(s) during INC 3.1 Acknowledge Incident and adjusted as necessary.

5.3 INC 2.0 INITIAL SUPPORT


INC – Incident Management
INC 2.0 – Initial Support
Service Desk
INC 1.0 Incident Identification and Classification
INC 2.1 Perform Incident Matching
Duplicate?
Yes
No
INC 2.2 Associate Incident to Related Record
Active Problem?
Yes
No
Caused by a Change?
Yes
No
INC 2.3 Assign Incident to Appropriate Support Group
INC 3.0 Investigation and Diagnosis
INC 5.0 Incident Closure
Existing KE or Workaround?
No, or requires Incident Support to implement
Yes
INC 2.4 Apply Document Resolution
No
Incident Resolved?

<u>INC 2.1</u> <u>Perform Incident Matching</u>: The Service Desk searches open Incidents with same Caller, Service Offering, Configuration Item and/or Categorization to determine if a duplicate Incident exists.

- If duplicates are found, proceed to INC 2.2
- If no duplicates are found, proceed to INC 2.3

<u>INC 2.2</u> <u>Associate Incident to Related Record</u>: When related records exist, the Service Desk matches the Incident against other related events: Incidents, Problems, Known Errors or Changes that are open or have been recently closed.

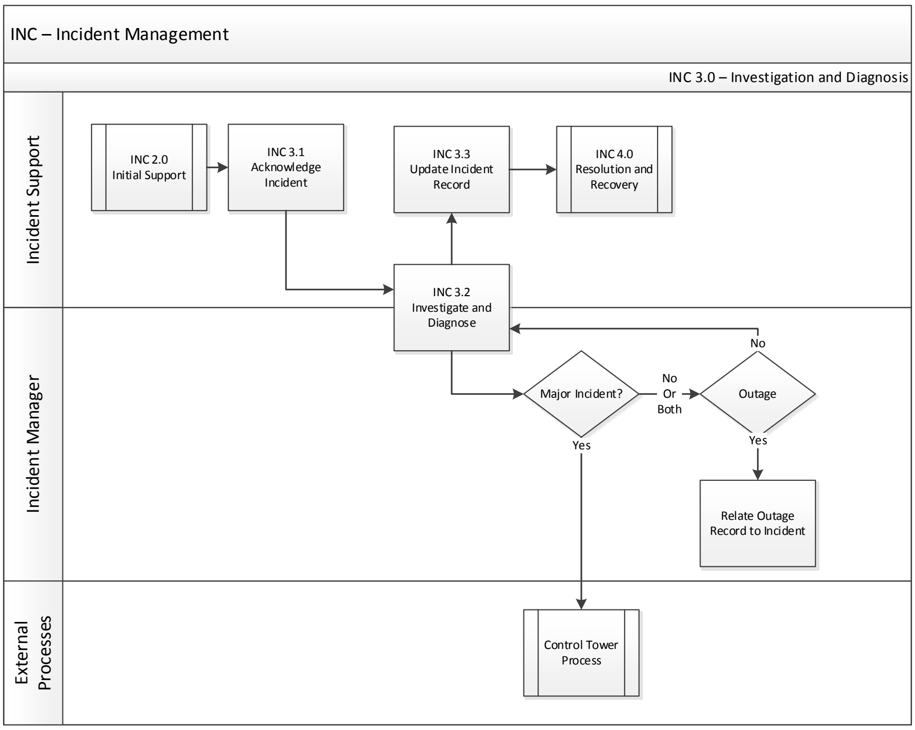
- If the record is a duplicate active Incident of the same customer, cancel the newly created Incident
- If the Incident appears to be related to the same cause as a previous Incident (Parent), log the Parent ID in the **Related Records** section, Parent Incident field
- If the Incident appears to have been caused by a Change, log the Change # in the in the **Caused by Change** field
- If the Incident will be resolved by a Change, log the Change # in the **Change Request** field
- If the Incident appears to be related to an existing Problem, log the Problem # in the **Problem** field

INC 2.3 Assign Incident to Appropriate Assignment Group: The Service Desk assigns the Incident to the most appropriate Assignment Group based on the Service Offering, Categorization, and any applicable Knowledge article. If the Incident was clearly caused by a recent Change, it may be assigned to the Change Assignment Group. In order to ensure defined SLAs are met for Incident Resolution, if the currently assigned Service Desk Agent cannot resolve the issue quickly, he/she must re-assign the Incident

INC 2.4 Apply Documented Resolution: If a Known Error or Knowledge article is available to provide Resolution, and it can be implemented by the Service Desk, the solution is applied. If the Known Error or Knowledge article requires escalation for implementation, refer to INC 2.3 Assign Incident to Appropriate Assignment Group.

If the Incident is resolved, proceed to INC 5.0 Incident Closure.

5.4 INC 3.0 INVESTIGATION AND DIAGNOSIS


INC – Incident Management
INC 3.0 – Investigation and Diagnosis
Incident Support
Incident Manager
External Processes
INC 2.0 Initial Support
INC 3.1 Acknowledge Incident
INC 3.3 Update Incident Record
INC 4.0 Resolution and Recovery
INC 3.2 Investigate and Diagnose
Major Incident?
No Or Both
Outage
No
Yes
Yes
Relate Outage Record to Incident
Control Tower Process

INC 3.1 Acknowledge Incident: Each Incident Assignment Group is responsible for monitoring their respective queues for assigned Incidents.

- If correctly assigned, delegate Incident to a specific Support Team Member; **Or**
- If incorrectly assigned, reassign to another Assignment Group

INC 3.2 Investigate and Diagnose: Each Assignment Group involved with handling the Incident performs full a investigation and diagnosis of the assigned Incident in order to determine what has gone wrong. Key activities include investigating related records:

- Configuration items
- Changes

- Problems and Known Errors
- Knowledge Articles

Once the investigation is complete, the Assignment Groups attempt to diagnose the root cause. If a diagnosis is not determined:

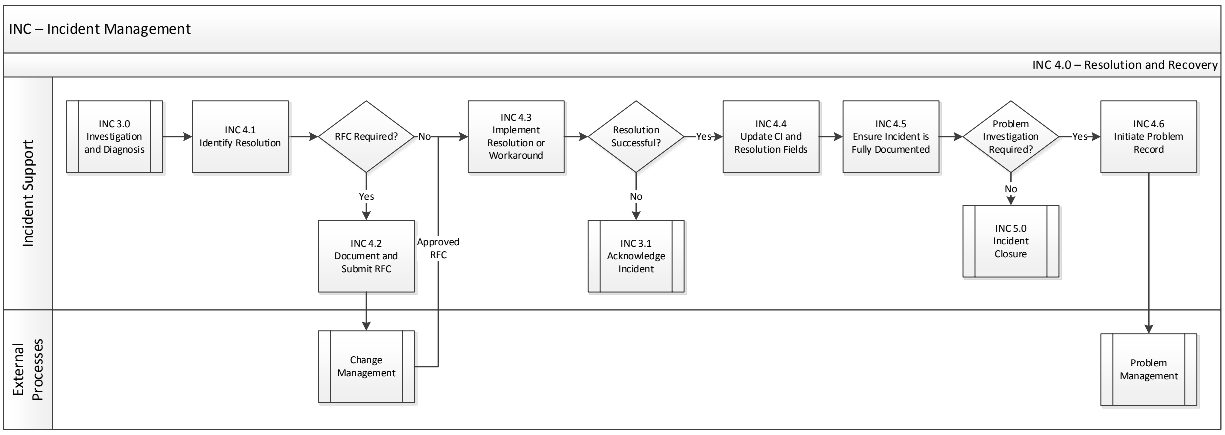
- If it is suspected or determined that the root cause lies in a technical area supported by different Operational Support Team, such as Infrastructure or On-Site Support, the Incident is re-assigned to the appropriate Assignment Group for Resolution
- If the sending team requires the Incident be returned to their Assignment Group prior to Resolution, it must be documented in the Work Notes
- If the diagnosis is not completed within expected SLA or OLA time, the Incident assignee will inform the Incident Manager to request additional resources and manage communications
- If there is no resource assigned or Work Notes updated within time period defined by Service Level process, the Incident Manger must ensure the Incident is progressing towards restoration
- The Incident Manager must assess if the Incident needs to be re-prioritized, using guidance in the Global Work Instruction Incident Management Priority Setting (GDWIN-000028) and Global Work Instruction Incident Manager (GDWIN-000027)

INC 3.3 Update Incident Record: In the Notes section, the sending team will:

- Update the Work Notes field with details of all activities performed to this point and why the Incident is being re-assigned to the new Assignment Group
- Update the Additional Comments field with Customer visible details on the current status

If a diagnosis was determined, proceed to INC 4.0.

5.5 INC 4.0 RESOLUTION AND RECOVERY


INC – Incident Management
INC 4.0 – Resolution and Recovery
Incident Support
External Processes
INC 3.0 Investigation and Diagnosis
INC 4.1 Identify Resolution
RFC Required?
No
Yes
INC 4.2 Document and Submit RFC
Approved RFC
INC 4.3 Implement Resolution or Workaround
Resolution Successful?
Yes
No
INC 3.1 Acknowledge Incident
INC 4.4 Update CI and Resolution Fields
INC 4.5 Ensure Incident is Fully Documented
Problem Investigation Required?
Yes
No
INC 5.0 Incident Closure
INC 4.6 Initiate Problem Record
Change Management
Problem Management

INC 4.1 Identity Resolution: Once the diagnosis is determined, the Incident Assignment Group identifies the resolution to restore service.

- If the Resolution requires a Change, proceed to INC 4.2. If not, proceed to INC 4.3.

INC 4.2 Document and Submit RFC: The Incident Assignment Group follows the Change Management process to document the required activities. Refer to *ITS: Change Management* (GDSOP-014174) for more detail.

- Once the Change request is approved, continue with the implementation of Resolution.

INC 4.3 Implement Resolution or Workaround:

- Follow documented procedures to implement the Resolution or Workaround
- If Resolution or Workaround did not restore services, return to INC 3.2.

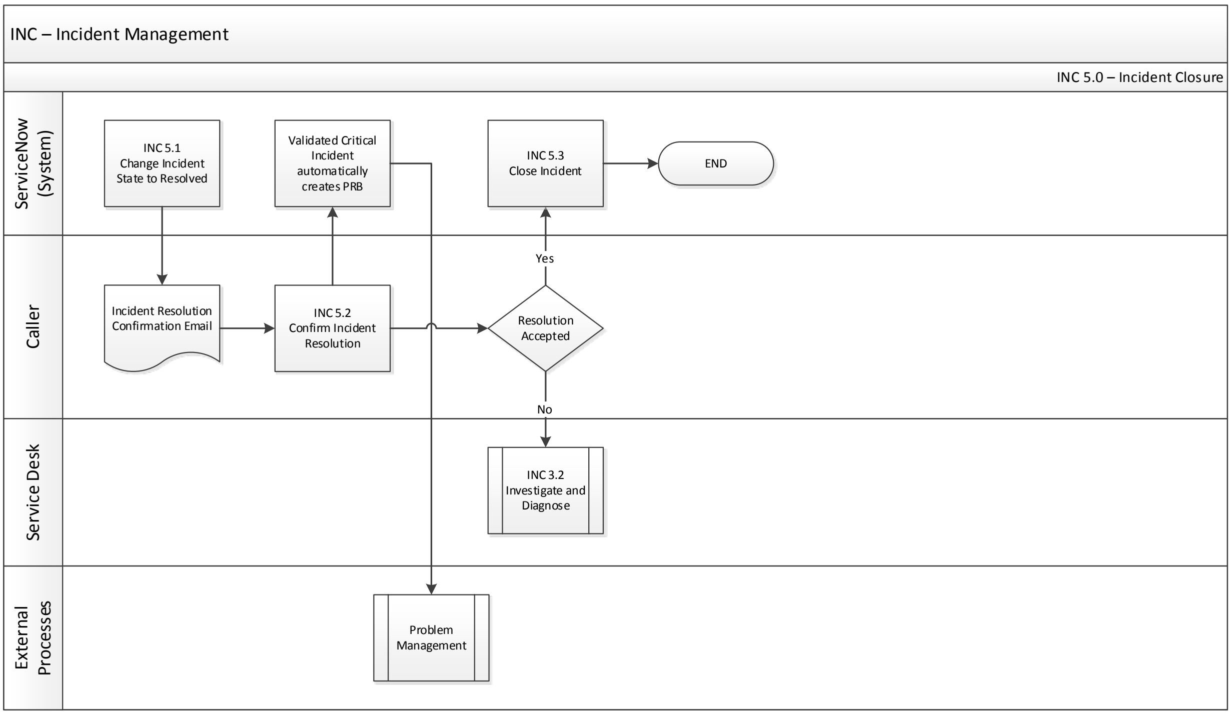
INC 4.4 Update CI and Resolution Fields:

- On the Incident form applet, ensure the correct **Configuration Item** (CI) is selected
- On the Resolution tab, update the following fields: **Resolution Category**, **Resolution Symptom**, and **Resolution**

INC 4.5 Ensure Incident is Fully Documented:

- In the **Resolution Notes**, the Incident Assignment Group must provide details on what steps were completed to restore services. This will be shared via an e-mail notification to the Caller when the Incident State is set to **Resolved**
- If the Resolution can be used to create or enhance the Knowledgebase, select the **Knowledge checkbox**. Updates to Knowledgebase are handled via the Knowledge Management process as documented in the Global Standard Operating Procedure *ITS: Knowledge Management* (GDSOP-014173)
- If the Incident caused a **Service Outage**, the Incident Manager is notified that Service is restored. Incident Manager must end the Service Outage.

5.6 INC 5.0 INCIDENT CLOSURE


INC – Incident Management
INC 5.0 – Incident Closure
ServiceNow (System)
Caller
Service Desk
External Processes
INC 5.1 Change Incident State to Resolved
Validated Critical Incident automatically creates PRB
INC 5.3 Close Incident
END
Incident Resolution Confirmation Email
INC 5.2 Confirm Incident Resolution
Yes
Resolution Accepted
No
INC 3.2 Investigate and Diagnose
Problem Management

INC 5.1 Change Incident State to Resolved: When an Incident is set to the **Resolved** state, an e-mail notification is automatically sent to the Caller.

INC 5.2 Confirm Incident Resolution:

- If satisfied with the Resolution, the Caller may ignore the notification, as no additional action is required. The ITSM system will automatically close the Incident seven (7) calendar days after the notification has been sent
- If not satisfied with the Resolution, the Caller can re-open the Incident by following the instructions in the e-mail notification.
  - If the Incident is re-opened, it returns to the last assigned Assignment Group at INC 3.2 Investigate and Diagnose
- Service Desk can close an Incident, in advance of automatic closure, if they have verified with the Caller that the Incident is resolved. Details of the confirmation are captured on the Incident record, in the Resolution Notes field
- Validated Critical Incidents automatically create a Problem Record when the Incident State is "Resolved." Management of the Problem record follows the Problem Management process Global Standard Operating Procedure *ITS: Problem Management* (GDSOP-014180)

INC 5.3 Close Incident:

- The Service Desk can manually close an Incident record as stated in the detail for INC 5.2.

- Incidents move to the “Closed” State after seven (7) calendar days if the Caller has not disagreed with the resolution

5.7 ROLE OF THE SANOFI CONTROL TOWER

The Sanofi Control Tower has responsibility for the review and validation of all “P1-Critical” Incidents within their defined scope of responsibility. The Control Tower will contact the Incident Manager to confirm the Priority.

- This includes communication with the Incident Manager to confirm that an Incident has been properly prioritized as a “P1-Critial.” If there is agreement that the Incident is a “P1-Critical, the “Validated Critial Incident” checkbox will be ticked by the Control Tower
- When the Incident is flagged as a Validated Critical Incident, the system automatically creates a Problem Record upon Incident resolution
- If there is not agreement that the Incident is a “P1-Critical,” the Control Tower will mandate a downgrade. The Incident Manager will be responsible to downgrade the Incident to a Priority of “P2-High”

During the life of the Incident, the Sanofi Control Tower and Incident Manager may determine that the Incident is severe enough to constitute a “crisis” that should be communicated to ITS Leadership. The Control Tower will tick the Major Incident Communication checkbox to indicate this.

- The Control Tower has the sole accountability to communicate such crisis “P1-Critical” Incidents to the business and ITS Leadership

5.8 SERVICE OUTAGE PROCESS

An Outage is specific to the availability of a Service Offering. It is an additional indicator for an incident record to mark the start and stop time of service interruption. Within the Incident process the Outage term is used to record Unplanned Outages only.

Incident Managers must review their service operational procedures, if available, to determine what constitutes an outage for a specific Service Offering. The Incident Manager may then create an Outage Record to track the duration of the outage and to communicate to ITS staff.

5.9 INCIDENT AND PROBLEM MANAGEMENT

If the Validated Critical Incident flag is checked, a Problem record is automatically created upon Incident Resolution.

Ten (10) recurrences of an identical incident in a 30-day period may require a Problem record. It is the responsibility of the Incident Manager to determine and create a Problem record in this instance. At least on a weekly basis, the Incident Manager is responsible for monitoring dashboards for recurring identical Incidents.

5.10 QUALITY RISK MANAGEMENT AND INCIDENTS

Priority P1 Incidents with potential quality risks are escalated to the Problem Management Process.

6. RESPONSIBILITIES

6.1 PRIMARY OPERATIONAL ROLES

Caller or Requestor

- Requests support when necessary and provides the required information to help resolve the Incident
- Declares Incidents by contacting the Service Desk (or key user) via channels appropriate to the severity of the Incident
- Checks the provided Resolutions and accepts or rejects them
- May be an end-user or a key user

Control Tower

- Responsible to confirm “P1-Critical” Incidents within their scope
- Communicates “P1-Critical” Incidents to the Business, ITS, and the ITS Leadership Teams, as appropriate
- Establishes or participates on bridge calls with all responsible Operational Support Groups to manage “P1-Critical” Incident resolution

Incident Manager

- Oversees operational activities of the process
- End-to-end responsibility to manage the Incident
- Ensures all appropriate technical resources are engaged to work on the Incident
- Works with the resolver group managers to ensure proper resources are available to complete the resolution within service target
- Responsible to approve or reject modifications to the Impact of the Incident
- Acts as lead point of contact with the Control Tower for “P1-Critical” Incidents
- Follows the established Problem Management SOP to identify repetitive incidents for further analysis by the Problem Management process
- Oversees and escalates Incident SLAs
- Gathers and reports on process metrics
- Is responsible to monitor dashboards for recurring identical incidents on at least a weekly basis (for escalation to Problem Management process).

Sevice Desk Agent

- Provides the interface to the service provider (ITS entity) for the end-users of its services

- When end-users or key-users are requesting support, obtains the necessary information and registers it efficiently, accurately, and completely in an Incident
- Ensures that registered Incidents are assigned efficiently and accurately to the most appropriate group for Resolution
- Within the limitations of access rights and time constraints, resolves as many registered Incidents as possible, without escalation

Operational Support Groups

- Diagnoses and resolves Incident declarations
- Updates Incident declarations with relevant information and status changes
- Develops Workarounds
- Creates Incidents after detecting a service failure, service degradation or a situation which may result in a failure or degradation
- Escalates technical issues to the Incident Manager as necessary to resolve Incidents within SLA targets
- Responsible for ensuring if GxP system is implicated, that Priority is adjusted

6.2 SUPPORTING AND ADDITIONAL PROCESS ROLES

Process Owner

- Involves all stakeholders and obtains resources to manage the process
- Ensures the definition and modeling of the process
- Coordinates process implementation within entities
- Ensures monitoring tools are in place to measure the performance of the process
- Ensures the continuous improvement of the process
- Ensures compliance with internal and external regulations
- Collaborates with other Process Owners to ensure consistency with related processes

Group Manager

- Manages Assignment Group membership
- Manages dispatch and ticket assignment

Service Owner

- Accountable for the overall performance of the service impacted by Incidents. No specific activities identified for Incident Management Process.

6.3 RESPONSIBILITY MATRIX

Roles are responsible for performing specific process activities. A RACI diagram (**R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed) visually indicates these responsibilities for Incident Management. Please see the following sections for RACI information:

ID	Activity	Caller	Incident Manager	Service Desk	Operational Support
INC 1.0	**Identification and Classification**				
New Call	Service Desk Interaction with Caller	C	A	R	--
INC 1.1	Create New Incident	C	A	R	R
INC 1.2	Verify Caller Information	C	A	R	--
INC 1.3	Capture Incident Detail	C	A	R	--
INC 1.4	Categorize Incident	C	A	R	--
INC 1.5	Prioritize Incident	C/I	A/I/R	R	--
INC 2.0	**Initial Support**				
INC 2.1	Perform Incident Matching	--	A	R	--
INC 2.2	Associate Incident to Related Record	--	A	R	--
INC 2.3	Assign Incident to Appropriate Assignment Group	--	A	R	--
INC 2.4	Apply Documented Resolution	--	A	R	--
INC 3.0	**Investigation and Diagnosis**				
INC 3.1	Acknowledge Incident	--	A	I	R
INC 3.2	Investigate and Diagnose	--	A/R	--	R
INC 3.3	Update Incident Record	I	A/R	I	R
INC 4.0	**Resolution and Recovery**				
INC 4.1	Identity Resolution	--	A	I	R
INC 4.2	Document and Submit RFC	--	A	I	R
INC 4.3	Implement Resolution or Workaround	--	A	I	R
INC 4.4	Update CI and Resolution Codes	I	A	I	R
INC 4.5	Ensure Incident is Fully Documented	--	A/C	I	R
INC 5.0	**Closure**				
INC 5.1	Send Incident Resolution Confirmation E-mail	I	A	R	--
INC 5.2	Confirm Incident Resolution	C/I	A	I/R	R
INC 5.3	Close Incident	--	A	I/R	--

7. SUPPORTING DOCUMENTS AND APPENDICES

7.1 SUPPORTING DOCUMENTS

N/A

7.2 APPENDICES

N/A

8. DOCUMENT HISTORY

Version Number	Previous Effective Date	Description of change
1.0	N/A	Creation of this document in geode+ - This document will replace GDSOP-014106 (once previous system is retired).
2.0	13 November 2017	Update of this document to : 1. Add references to GDWIN-000028 Incident Priority setting and GDWIN-000027 Incident Manager 2. Remove tables from section 5.2 as they are now in the GDWIN-000028 3. Remove sentence about Priority 2 incidents in section 5.10 4. Remove ITS Quality & Compliance responsibilities as they have no specific tasks in this SOP
3.0	01 October 2019	Update of this document based on new prioritization rules and establishment of Control Tower

End of Document

Specificities

Information Technology and Solutions		
E - Manage Information System	E.4 - Deliver, Service & Support	
DSS02 - Manage Service Requests and Incidents	No Subsystem	No Subsystem

Applicability

Entity / GBU	Sanofi Company		

Geography	Worldwide		

Applications Services	Information Technology and Solutions		

Supporting document

Reference	Title
GDWIN-000027	Incident Manager
GDWIN-000028	Incident Management: priority setting

Related documents

Reference	Title
GDSOP-014180	ITS: Problem Management