servicenow®

# Process Guide

# Incident Management

Version: 1.2
CALGARY Release

# Table of Contents

# List of Figures

# 1 Introduction

The concepts described in this guide align with ITIL 2011 and may reference capabilities that are dependent upon other ServiceNow applications. These references are noted by *blue italicized font.*

## 1.1 Overview

A process is defined as a set of linked activities that transform specified inputs into specified outputs, aimed at accomplishing an agreed-upon objective in a measurable manner. The incident management process definition laid out in this document further breaks down these activities into actions and the role(s) responsible for their execution.

This document also describes how ServiceNow supports the incident management process with its abilities to record, categorize, prioritize, assign to appropriate groups, escalate, and manage incidents through to resolution and reporting.

## 1.2 Process Description

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. Incidents can include failures or degradation of services reported by users, technical staff, third-party suppliers and partners, or automatically from monitoring tools.

Incident management is responsible for managing the lifecycle of all incidents.

## 1.3 Process Goal

The primary goal of the incident management process is to restore normal service operation as quickly as possible and minimize the adverse impact of incidents on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. *Normal service operation* is defined here as an operational state where services and CIs are performing within agreed service and operational levels.

## 1.4 Process Objectives

The objectives of the incident management process are to:

- Ensure that standard methods and procedures are used for efficient and prompt incident response, analysis, documentation, ongoing management, and reporting.
- Increase visibility and communication of incidents to business and support staff.
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur.
- Align incident management activities and priorities with those of the business.
- Maintain user satisfaction with the quality of IT services.

## 1.5 Relationship with Other Processes

| Process | Relation Description | Input | Output |
|---|---|---|---|
| Configuration Management | The configuration management system underpins all incident management activities. It not only hosts the incident and other service management records, but contains details of the infrastructure vital to efficient call handling. | X | |
| | When CI records are identified as inaccurate, incident records are created and assigned to configuration management for correction. | | X |
| Problem Management | • Problems can be initiated from an incident when determining the root cause of the incident needs further investigation.<br>• Incident information is proactively analyzed to detect trends in service behavior that may be indicative of an underlying problem. | | X |
| | • Information about known errors and their workarounds is used to diagnose and resolve recurring incidents faster. | X | |
| Change Management | • A request for change (RFC) can be submitted in order to implement a workaround or a resolution. | | X |
| | • Can detect and resolve incidents that arise from changes.<br>• Change management is responsible for keeping the Service Desk informed of all scheduled changes. | X | |
| Service Level Management (SLM) | • Defines measurable responses to service disruptions.<br>• Provides historical data that enables SLM to review service level agreements (SLAs) objectively and regularly.<br>• Assists SLM in defining where services are at their weakest so that SLM can define actions as part of the service improvement plan (SIP). | | X |
| | SLM defines the acceptable levels of service within which incident management works, including:<br>• Incident response times<br>• Impact definitions<br>• Target fix times<br>• Service definitions<br>• Rules for requesting services | X | |

## 1.6 Principles and Basic Concepts

### Policies

Incident management policies are required to guide all staff in the behaviors needed to make incident management effective.  Policy statements will be very dependent on the culture of the organization, but typically address the following:

- Use of a single management system for all incidents.
- Incident management should be aligned with overall service levels and objectives.
- Hierarchical escalation for appropriate IT management notification.
- Routine audits of incident records to ensure correct incident categorization and documentation.

### Timescales

Timescales must be agreed for all incident-handling stages (these will differ depending upon the incident's priority level), based on the overall incident response and resolution targets within SLAs. See Defining a SLA in the ServiceNow Wiki for a description of how to use the ServiceNow SLA plugin to establish incident activity targets.

### Incident Models

Many incidents are not new; they involve dealing with something that has happened before and may well happen again. An incident model is a way of predefining the steps that should be taken to handle a particular type of incident in an agreed manner. See Creating an Incident Template in the ServiceNow Wiki for a description using the incident template feature of ServiceNow to support this concept.

### Major Incident

A separate procedure, with shorter timescales and greater urgency, must be used for *major incidents*. A definition of what constitutes a major incident must be agreed and mapped onto the overall incident prioritization scheme so that they can be dealt with through this separate procedure.

**NOTE:** An incident always remains an incident. It may grow in impact or priority to become a major incident, but an incident never *becomes* a problem.

### Incident States

Incidents should be 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 what the next step in the process might be. The typical uses of the base system state values are:

- **New:** default value upon record creation.
- **Active:** work is in progress.

- **Awaiting User Info:** pauses the incident SLA timer.
- ***Awaiting Problem:*** pauses the incident SLA timer when a workaround does not exist and a related problem is created to immediately pursue a workaround or permanent solution. The incident can be automatically closed when the problem is resolved.
- **Resolved:** the incident has been resolved but not yet confirmed with the customer or user.
- **Closed:** customer or user satisfaction has been confirmed; the record can no longer be updated.

# 2 Process Roles

Each role is assigned to perform specific tasks within the process. Within the 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, though typically not at the same time. Depending on the structure and maturity of a process, all roles described may not exist in every organization.

The following describes the typical roles defined for incident management.

| Role | Description |
|---|---|
| Process Owner | A senior manager with the ability and authority to ensure the process is rolled out and used by the entire IT organization.<br>**Responsible for:**<br>• Defining the overall mission of the process.<br>• Establishing and communicating the process mission, goals, and objectives to all stakeholders.<br>• Resolving any cross-functional (departmental) issues.<br>• Ensuring consistent execution of the process across the organization.<br>• Reporting on the effectiveness of the process to senior management.<br>• Initiating any process improvement initiatives. |
| Incident Manager | **Responsible for:**<br>• Managing the day-to-day activities of the process.<br>• Driving the efficiency and effectiveness of the incident management process.<br>• Gathering and reporting on process metrics.<br>• Managing major incidents.<br>• Developing and maintaining the process procedures. |

| Role | Description |
|---|---|
| Agent (1st level) | **Responsible for:**<br>• Recording, ownership, monitoring, tracking, and communication about incidents.<br>• Investigating and diagnosing incidents.<br>• Providing resolutions and workarounds from standard operating procedures and existing known errors.<br>• Escalating incidents to incident support.<br>• Closing of incidents. |
| Incident Support (2nd level) | **Responsible for:**<br>• Investigating and diagnosing incidents escalated from the Service Desk.<br>• Developing workarounds.<br>• Resolving and recovery of assigned incidents.<br>• Creating incidents after detecting a service failure or quality degradation or a situation that may result in one. |
| Service Desk Manager | **Responsible for:**<br>• Managing resources assigned to the Service Desk.<br>• Managing Service Desk activities.<br>• Monitoring and reporting on Service Desk performance.<br>• Taking overall responsibility for incident and service request handling by the Service Desk.<br>• Making improvements to the Service Desk. |
| Caller | **Responsible for:**<br>• Bringing incidents to the attention of the Service Desk.<br>• Participating in the implementation of a solution or workaround and verifying correct operation once implemented, as needed. |

## 2.1 RACI Matrix

Roles and responsibilities are assigned to specific process activities.

| ID | Activities | Caller | Service Desk Agent | Incident Support | ServiceNow |
|---|---|---|---|---|---|
| **INC 1.0** | **Incident Identification and Classification** | | | | |
| INC 1.1 | Create new incident | C | R/A | R | |
| INC 1.2 | Verify Caller information | C | R/A | | |
| INC 1.3 | Capture incident details | C | R/A | I | |
| INC 1.4 | Categorize incident | C | R/A | | |
| INC 1.5 | Prioritize incident | C | R/A | | |
| **INC 2.0** | **Initial Support** | | | | |
| INC 2.1 | Perform incident matching | | R/A | | |
| INC 2.2 | Apply documented resolution | I/C | R/A | | |
| INC 2.3 | Associate incident to related record | | R/A | | |
| INC 2.4 | Assign incident to appropriate support group | | R/A | I | |
| **INC 3.0** | **Investigation and Diagnosis** | | | | |
| INC 3.1 | Acknowledge incident assignment | | | R/A | |
| INC 3.2 | Investigate and diagnose | C | C | R/A | |
| INC 3.3 | Update incident record | | | R/A | |
| **INC 4.0** | **Resolution and Recovery** | | | | |
| INC 4.1 | Document and submit RFC | | | R/A | |
| INC 4.2 | Implement resolution or workaround | I/C | | R/A | |
| INC 4.3 | Validate initial categorization | C | | R/A | |
| INC 4.4 | Ensure incident is fully documented | | R/A | R | |
| INC 4.5 | Initiate Problem record | | I | R/A | |
| **INC 5.0** | **Incident Closure** | | | | |
| INC 5.1 | Send Incident resolution confirmation email | I | | | R/A |
| INC 5.2 | Confirm Incident resolution | C/R | R/A | | |
| INC 5.3 | Close Incident | I | R/A | | R |
| | **R**: Responsible, **A**: Accountable **C**: Consulted, **I**: Informed | | | | |

# 3 Incident Management Activity Description

## 3.1 Process Overview Diagram

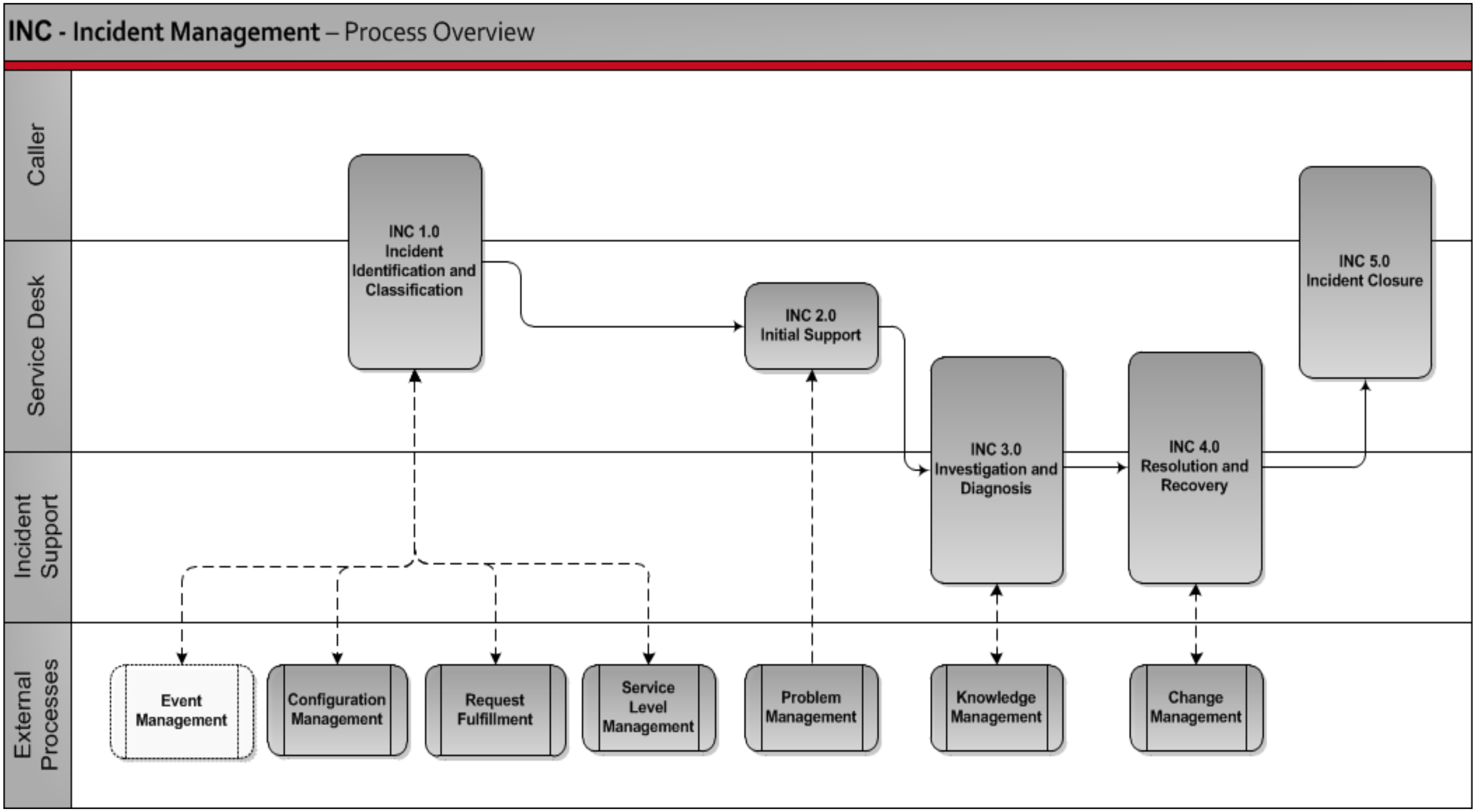


**Figure 1. Process Overview**

## Process Activity Overview Description

| ID | Tasks | Description |
|---|---|---|
| INC 1.0 | **Incident Identification and Classification** | • Gathering information needed to facilitate service disruption analysis and assignment.<br>• Redirecting improperly routed service requests to the request fulfillment process.<br>• Associating the incident with a relevant SLA.<br>• Determining the incident priority.<br>• Invoking the major incident procedure where applicable. |
| INC 2.0 | **Initial Support** | • Matching the incident against other related calls, events, incidents, known errors, or changes that are open or have been recently closed.<br>• Escalation to 2nd-level support, if necessary.<br>In many cases, corresponding workarounds, known errors, or quick fixes documented in the knowledge base allow incidents to be resolved at 1st-level support without recourse to further resources. |
| INC 3.0 | **Investigation and Diagnosis** | • Performing full investigation and diagnosis of the assigned incident.<br>• Providing advice on possible workarounds or temporary fixes.<br>• Using standard operational procedures and work instructions to ensure that service can be restored as quickly as possible. |
| INC 4.0 | **Resolution and Recovery** | • Repairing or replacing the faulty CI(s).<br>• Restoring the service so that it is available for use.<br>• Submitting a RFC when a change is necessary to achieve incident resolution.<br>• Informing the customers and users that the service is restored.<br>• Verifying with the customer or callers that service restoration is satisfactory. |
| INC 5.0 | **Incident Closure** | As far as practicable, confirmation that the service is truly restored should be obtained from the affected caller(s) before the incident is closed. |

## 3.2 Incident Identification and Classification

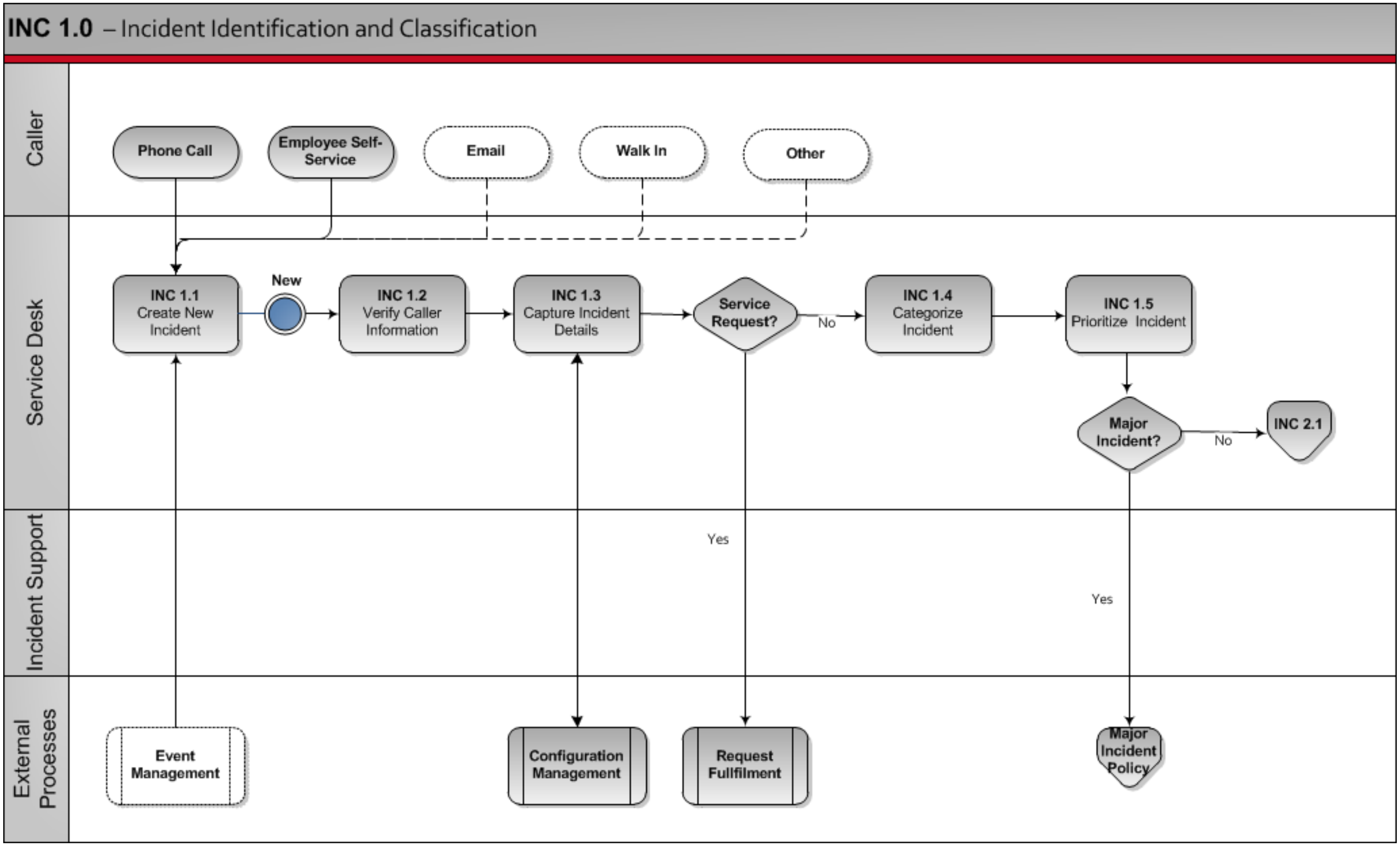


**Figure 2. Identification and Classification**

## Incident Identification and Classification Procedure

Capturing sufficient and relevant detail at this stage is very important; it will aid in diagnosis if the incident requires escalation. A description of the incident in the caller's own words should be recorded so that future contact with the caller can be made in their terms.

**NOTE:** These steps are taken when the caller contacts the service desk. They are not valid when the incident is reported through an employee self-service mechanism.

| ID | Tasks | Procedure | Primary Role | Input | Output |
|---|---|---|---|---|---|
| INC 1.1 | **Create New Incident** | From the Incident application, create a new incident record.<br>See Inbound Email Actions for a description of how to allow callers to log an incident via email.<br>The ServiceNow New Call Wizard feature can be used to capture call information before making a decision about whether the call is an incident or service request. | Service Desk | Email from caller<br>Call<br>Walk-in | New incident record |
| INC 1.2 | **Verify Caller Information** | Use the lookup list to identify the person reporting the incident.<br>Ensure that the caller's contact information is accurate by verifying:<br>• Phone number<br>• Email address<br>• Department<br>• Location<br>• *Associated CIs*<br>Update information when necessary. | Service Desk | New incident record | Incident record with identified source and accurate caller information |
| INC 1.3 | **Capture Incident Details** | Summarize the incident symptoms in the **Short Description** field.<br>In the **Notes** and **Additional comments** sections, describe the symptoms of the incident:<br>• What the caller is trying to do | Service Desk | Incident record with identified source and accurate caller information | Incident with detailed symptom information |

| ID | Tasks | Procedure | Primary Role | Input | Output |
|---|---|---|---|---|---|
| | | • What is happening<br>• What actions were taken by the caller<br>• When the incident occurred | | | |
| INC 1.4 | **Categorize Incident** | See **Appendix C** for categorization techniques. | Service Desk | Incident with detailed symptom information | Categorized incident |
| INC 1.5 | **Prioritize Incident** | See **Appendix D** for prioritization techniques. | Service Desk | Categorized incident | Prioritized incident |

## 3.3 Initial Support

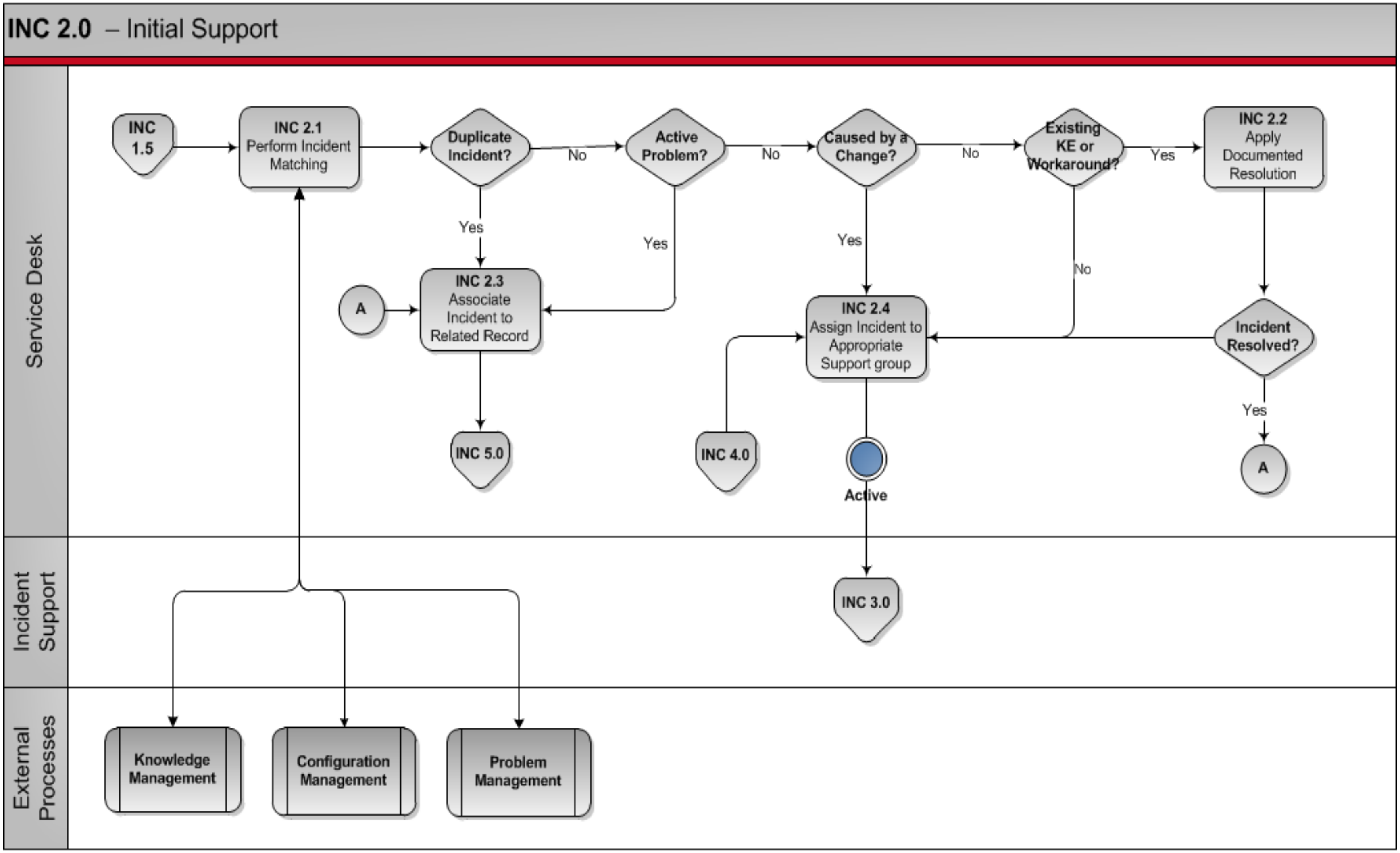


**Figure 3. Initial Support**

## Initial Support Procedure

Incident matching is performed in an attempt to identify duplicate incidents and locate a solution or workaround.

| ID | Tasks | Procedure | Primary Role | Input | Output |
|---|---|---|---|---|---|
| INC 2.1 | **Perform Incident Matching** | • Search opened incidents with the same categorization to determine if a duplicate incident exists.<br>• If the *affected CI has been identified*, see BSM Map for a description of how to use the ServiceNow business service management map feature to easily identify open incidents.<br>• Look for existing resolution action by *searching for existing problems and known errors* with corresponding category and symptoms. | Service Desk | Prioritized incident | Identified:<br>• Duplicate incident<br>• RFC as the cause of the incident<br>• Corresponding active problem<br>• Corresponding known error or workaround |
| INC 2.2 | **Apply Documented Resolution** | If a corresponding known error exists, apply the documented workaround or resolution as described. | Service Desk | Identified corresponding known error or workaround | Resolved or unresolved incident |
| INC 2.3 | **Associate Incident to Related Record** | Associate the related record to the incident if:<br>• An identical active incident (same error on the same CI) exists.<br>Or<br>• An active problem record related to the incident exists.<br>Or<br>• The applied workaround, known error, or resolution information resolved the incident.<br>Or<br>• The incident was caused by the implementation of a change. | Service Desk | • Duplicate incidents<br>• Corresponding active problem record<br>• Identified RFC as a cause of the incident<br>Or<br>• Resolution information from known error or workaround | Existing related records associated to incident |

| ID | Tasks | Procedure | Primary Role | Input | Output |
|---|---|---|---|---|---|
| | | | | applied successfully | |
| INC 2.4 | **Assign Incident to Appropriate Support Group** | If no documented known error or workaround exists, or if identified documented resolution did not resolve the incident, select the appropriate assignment group. | Service Desk | • Existing related records associated to incident<br>Or<br>• Unresolved incident | Incident escalated to Incident Support |

## 3.4 Investigation and Diagnosis

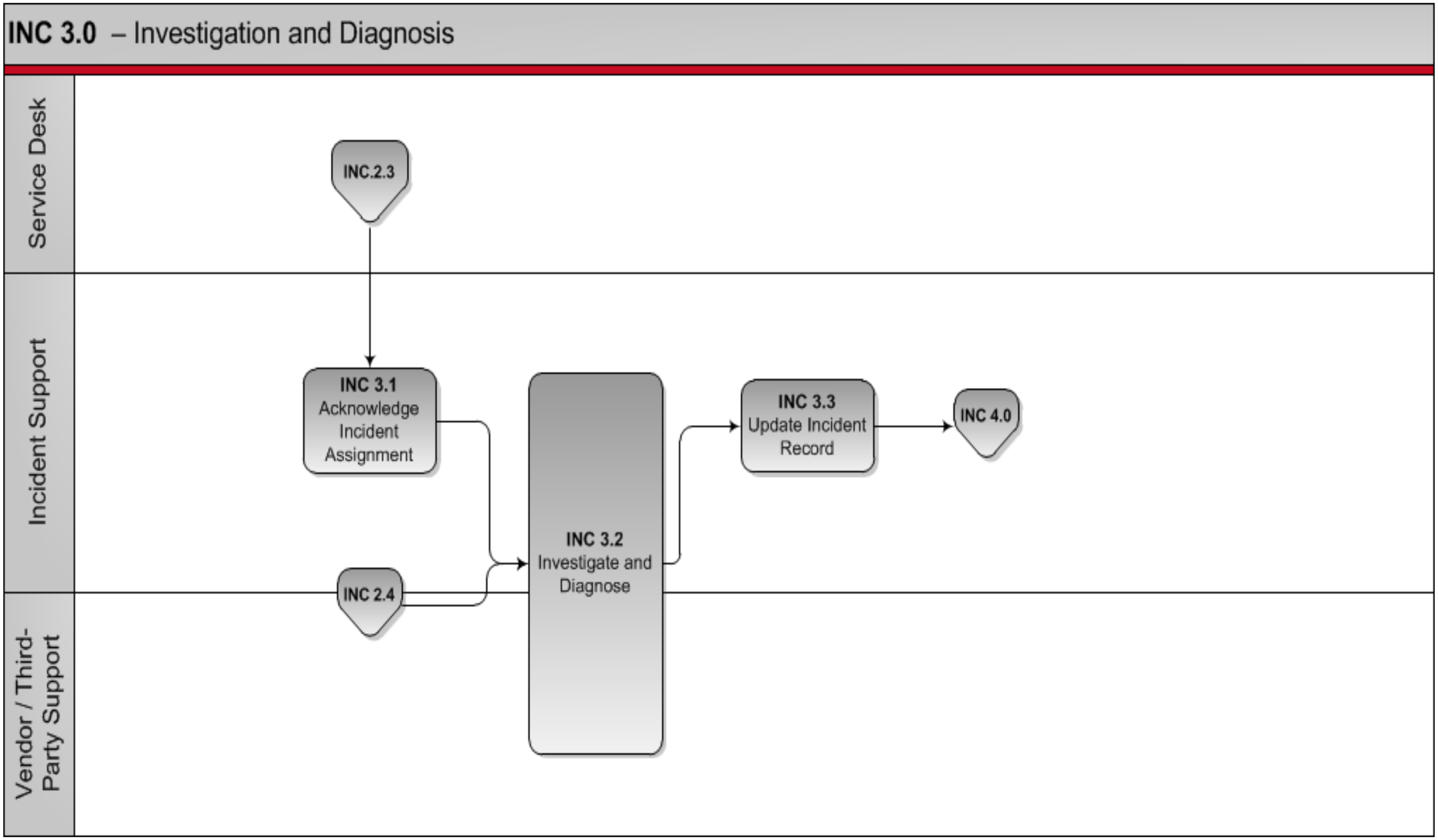

INC 3.0 – Investigation and Diagnosis
Service Desk
Incident Support
Vendor / Third-Party Support
INC.2.3
INC 3.1 Acknowledge Incident Assignment
INC 2.4
INC 3.2 Investigate and Diagnose
INC 3.3 Update Incident Record
INC 4.0

**Figure 4. Investigation and Diagnosis**

## Investigation and Diagnosis Procedure

| ID | Tasks | Procedure | Primary Role | Input | Output |
|---|---|---|---|---|---|
| INC 3.1 | **Acknowledge Incident Assignment** | Each 2nd-level support group is responsible for monitoring their respective queues for assigned incidents.<br>• Assign incident to specific support team member.<br>Or<br>• Reassign to another support group, if appropriate.<br>• Incident state is **Active** | Incident Support | Incident escalated to Incident Support | Active incident (under investigation) |
| INC 3.2 | **Investigate and Diagnose** | Each support group involved with handling the incident investigates and diagnoses what has gone wrong. | Incident Support | Active incident (under investigation) | Investigation and diagnosis findings |
| INC 3.3 | **Update Incident Record** | In the **Work notes** section, document all activities, including details of any actions taken to try to resolve or re-create the incident, so that a complete historical record of all activities is maintained at all times. | Incident Support | Investigation and diagnosis findings | • Identified solution or workaround<br>• Incident record documented with investigation and diagnosis findings |

## 3.5 Resolution and Recovery

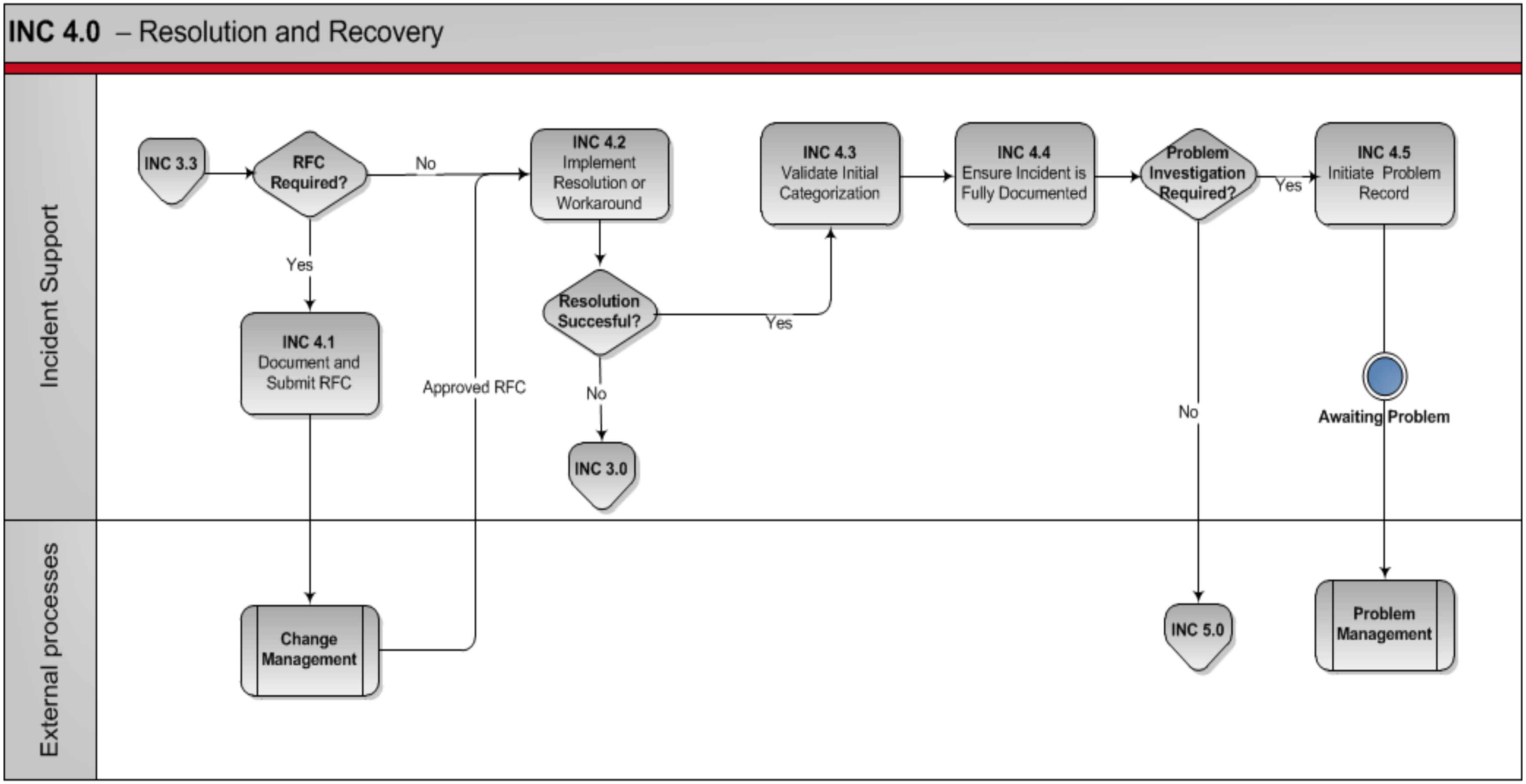

INC 4.0 – Resolution and Recovery
Incident Support
External processes
INC 3.3
RFC Required?
No
Yes
INC 4.1 Document and Submit RFC
Change Management
Approved RFC
INC 4.2 Implement Resolution or Workaround
Resolution Succesful?
Yes
No
INC 3.0
INC 4.3 Validate Initial Categorization
INC 4.4 Ensure Incident is Fully Documented
Problem Investigation Required?
Yes
No
INC 5.0
INC 4.5 Initiate Problem Record
Awaiting Problem
Problem Management

**Figure 5. Resolution and Recovery**

## Resolution and Recovery Procedure

| ID | Tasks | Procedure | Primary Role | Input | Output |
|---|---|---|---|---|---|
| INC 4.1 | ***Document and Submit RFC*** | If a change is needed, initiate a new RFC from the incident record. | Incident Support | Identified solution or workaround requesting an RFC | RFC submitted to Change Management |
| INC 4.2 | **Implement Resolution or Workaround** | Follow the documented procedure and implement the resolution or workaround.<br>• If the service is restored, change the incident state to **Resolved**.<br>• If the implemented resolution or workaround does not restore the service, return to **INC 3.2 – Investigate and Diagnose**. | Incident Support | Identified solution or workaround ready to be implemented | Resolution or workaround implemented successfully<br>Or<br>Additional investigation and diagnosis required |
| INC 4.3 | **Validate Initial Categorization** | Ensure the initial incident categorization still corresponds to the nature of the incident. Adjust if necessary. | Incident Support | Resolution or workaround implemented successfully | Active incident properly categorized |
| INC 4.4 | **Ensure Incident is Fully Documented** | • Ensure the incident contains full historic information at a sufficient level of detail.<br>• If the incident has previously been associated to a known error or problem, set the incident state to **Resolved**. | Incident Support | Active incident properly categorized | Fully documented incident set to the **Resolved** state<br>Or<br>Fully documented incident with no identified root cause |
| INC 4.5 | ***Initiate a Problem*** | If the incident was resolved with no root cause being identified, a problem record can be initiated to begin Root Cause investigation. | Incident Support | Fully documented incident with no identified root cause | New problem record related to the incident |

## 3.6 Incident Closure

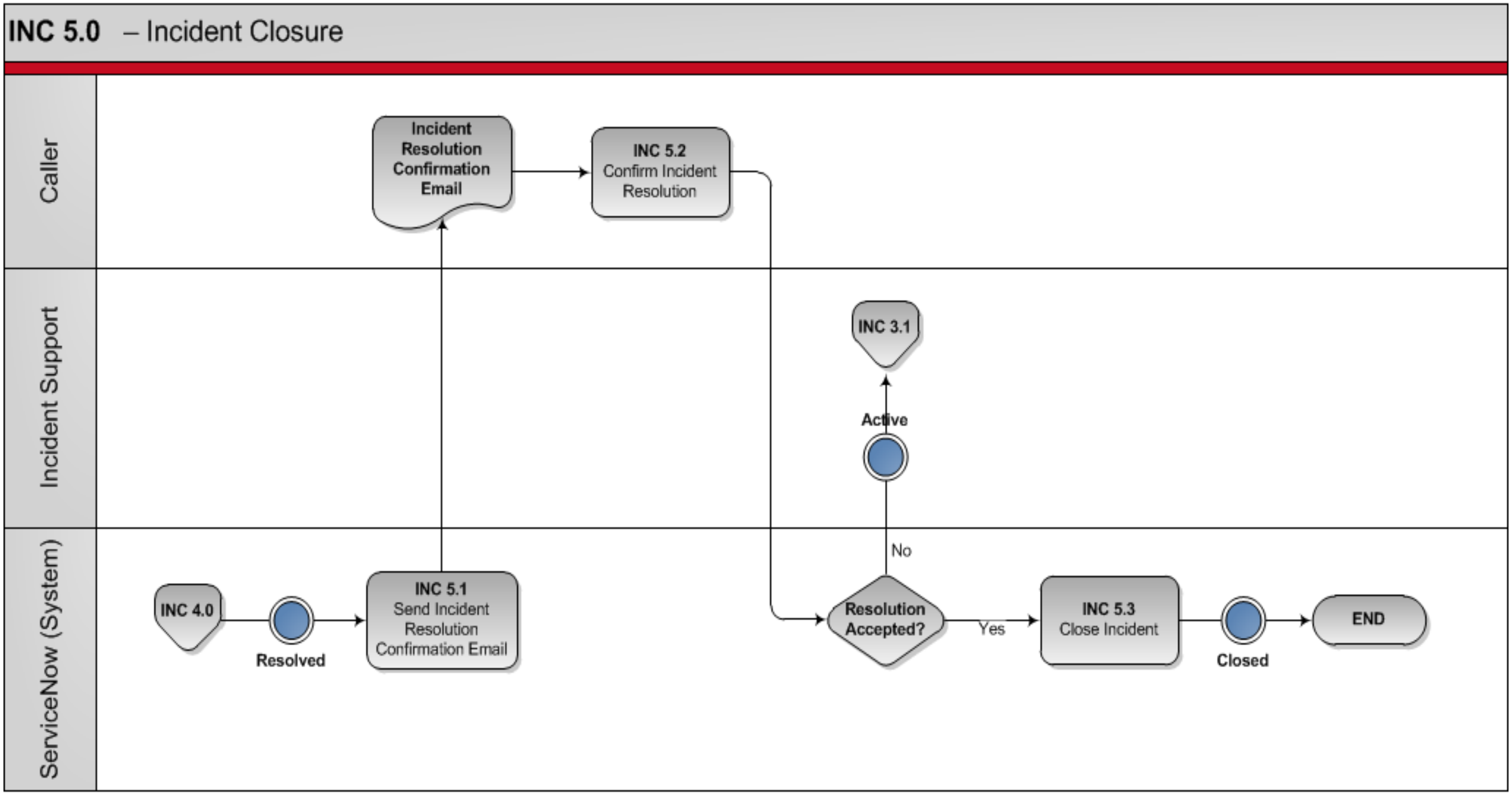

INC 5.0 – Incident Closure
Caller
Incident Support
ServiceNow (System)
Incident Resolution Confirmation Email
INC 5.2 Confirm Incident Resolution
INC 3.1
Active
No
INC 4.0
Resolved
INC 5.1 Send Incident Resolution Confirmation Email
Resolution Accepted?
Yes
INC 5.3 Close Incident
Closed
END

**Figure 6. Incident Closure**

## Incident Closure Procedure

| ID | Tasks | Procedure | Primary Role | Input | Output |
|---|---|---|---|---|---|
| INC 5.1 | **Send Incident Resolution Confirmation Email** | When an incident is set to a **Resolved** incident state, an email notification is sent to the caller. | ServiceNow (System) | Fully documented incident set to the **Resolved** state | Incident resolution confirmation notification by email |
| INC 5.2 | **Confirm Incident Resolution** | • If satisfied with the resolution, may ignore the notification, as no additional action is required. ServiceNow automatically closes the incident X hours/days after the notification has been sent.<br>• If not satisfied with the resolution, reopen the incident by clicking on the link within the email notification. | Caller | Incident resolution confirmation notification by email | Incident reopened by caller<br>Or<br>Incident at the **Resolved** state for X hours/days |
| INC 5.3 | **Close Incident** | ServiceNow automatically closes the incident if the caller has not disagreed with the resolution after X hours/days. | ServiceNow (System) | Incident at the **Resolved** state for X hours/days | Closed incident record and closed incident email notification |

# 4 Process Control

## 4.1 KPIs

KPIs are best represented as trend lines and tracked over time. They provide information on the effectiveness of the process and the impact of continuous improvement efforts.

| KPI/Metric | Purpose |
|---|---|
| Percentage of incidents resolved within target time, by priority. | Measure of how well incident SLAs are achieved. |
| Number and percentage of incidents resolved, by priority. | Measure of the quality of IT services. |
| Number and percentage of incidents resolved, by support level. | Measure of the efficiency of the incident management process. |
| Average user/customer survey score. | Measure of customer satisfaction with IT services. |

## 4.2 Operational Data

Active incidents that require visibility, oversight and possible management intervention are best tracked on a dashboard or homepage that is monitored by the Incident Manager.

| Item | Purpose |
|---|---|
| Pie chart of active incidents, by priority. | Shows priority distribution of current workload with ability to drill into detail records. |
| List of active major incidents. | Provides high visibility to major incident events in progress. |
| List of active incidents that have breached an SLA. | Provides quick view of incidents that need immediate attention to prevent further degradation of resolution time. |
| List of incidents reactivated from caller feedback. | Provides quick view of incidents that need immediate attention to meet resolution target and customer satisfaction. |

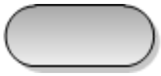
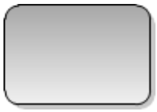
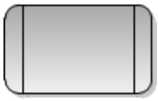
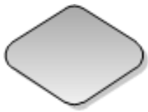
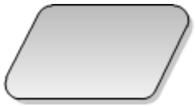
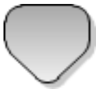
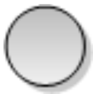
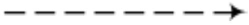
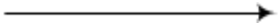
## 4.3 Reports and Homepages

There are numerous default reports available in ServiceNow that can be used to generate charts, can be published to a URL, or can be scheduled to be run and distributed at regular intervals. Users can also create custom reports. See Creating Reports in the ServiceNow Wiki for more detail on this capability.

In addition to reports, each user can create a personal homepage and add gauges containing up-to-the-minute information about the current status of records that exist in ServiceNow tables. See Customizing Homepages in the ServiceNow Wiki for details.

# *Appendices*

# Appendix A: Document Conventions

| Symbol | Description |
|---|---|
|  | **Process start or end point:** Represents the starting and ending point of the process. |
|  | **Process activity or task**: Presents an activity or task that needs to be accomplished to produce a specific outcome. |
|  | **Predefined external process or organization**: Indicates a contribution from an external process or organization. |
|  | **Decision:** Indicates that a question needs to be answered in order to identify the following activity or task in the process. The answers are indicated on the different connectors attached to the decision box. Every answer is linked to an associated activity or task. |
|  | **System Action or Function:**  Indicates that an action is being performed in the system as an output of the previous activity and an input to the next. |
|  | **Off-page reference**: Indicates a reference to another diagram within the same process. The number of the referenced diagram is indicated in the shape. |
|  | **On-page reference**: Indicates a link to another activity within the same diagram. |
|  | **Association:** Indicates an association or a relation between the connected, processes, tasks, or activities. May be represented by a dotted or dashed line. |
|  | **Sequence flow: S**hows the order in which the activities are performed. Represented by a solid line and arrowhead. |

# Appendix B: Glossary of Terms and Acronyms

| Term | Acronym | Definition |
|---|---|---|
| **Alert** | | A notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the event management process. |
| **Assessment** | | Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met. |
| **Attribute** | | A piece of information about a configuration item. Examples are name, location, version number, and cost. Attributes of CIs are recorded in the configuration management database (CMDB). |
| **Back-out** | | An activity that restores a service or other configuration item to a previous baseline. Back-out is used as a form of remediation when a change or release is not successful. |
| **Baseline** | | (ITIL *Continual Service Improvement)* (ITIL *Service Transition)* A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example:<br>▪ An ITSM baseline can be used as a starting point to measure the effect of a service improvement plan<br>▪ A performance baseline can be used to measure changes in performance over the lifetime of an IT service<br>▪ A configuration baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails. |
| **Category** | | A named group of things that have something in common. Categories are used to group similar things together. |
| **Change** | | The addition, modification, or removal of anything that could have an effect on IT services. |
| **Change Advisory Board** | CAB | A group of people who support the assessment, prioritization, authorization, and scheduling of changes. A change advisory board is usually made up of representatives from all areas within the IT service provider, the business, and third parties such as suppliers. |
| **Change Management** | CHG | The process responsible for controlling the life cycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services. |

| Term | Acronym | Definition |
|---|---|---|
| | | |
| **Change Record** | | A record containing the details of a change. Each change record documents the life cycle of a single change. A change record is created for every request for change. |
| **Change Request** | | See Request for Change. |
| **Configuration Record** | CI Record | A record containing the details of a configuration item. Each configuration record documents the lifecycle of a single configuration item. Configuration records are stored in a configuration management database and maintained as part of a configuration management system. |
| **Configuration Type** | CI Type | A category that is used to classify configuration items. The CI type identifies the required attributes and relationships for a configuration record. Common CI types include hardware, document, and user. |
| **Classification** | | The act of assigning a category to something. Classification is used to ensure consistent management and reporting. CIs, incidents, problems, and changes are usually classified. |
| **Closed** | | The final status in the life cycle of an incident, problem, or change. When the status is closed, no further action is taken. |
| **Closure** | | The act of changing the status of an incident, problem, or change to closed. |
| **Configuration Item** | CI | Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its life cycle by service asset and configuration management. |
| **Configuration Management Database** | CMDB | A database used to store configuration records throughout their life cycle. The configuration management system maintains one or more CMDBs. Each CMDB stores attributes of CIs and relationships with other CIs. |
| **Configuration Management System** | CMS | A set of tools, data, and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management and includes tools for collecting, storing, managing, updating, analyzing, and presenting data about all configuration items and their relationships. The CMS also includes information about incidents, problems, known errors, changes, and releases. It may contain data about employees, suppliers, locations, business units, customers, and users. The CMS is maintained by service asset and configuration management and is used by all IT service management processes. |

| Term | Acronym | Definition |
|---|---|---|
| | | |
| **Configuration Record** | | A record containing the details of a configuration item. Each configuration record documents the life cycle of a single configuration item. |
| **Continual Service Improvement** | CSI | Ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. The performance of the IT service provider is continually measured and improvements are made to processes, IT services, and IT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness. |
| **Customer** | | Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees to the service level targets. The term is also sometimes used informally to mean user, for example, 'This is a customer-focused organization.' |
| **Diagnosis** | | A stage in the incident and problem life cycles. The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem. |
| **Effectiveness** | | A measure of whether the objectives of a process, service, or activity have been achieved. An effective process or activity is one that achieves its agreed objectives. *See also* Key Performance Indicator. |
| **Efficiency** | | A measure of whether the right amount of resource has been used to deliver a process, service, or activity. |
| **Emergency Change** | | A change that must be introduced as soon as possible, for example to resolve a major incident or implement a security patch. The change management process normally has a specific procedure for handling emergency changes. |
| **Employee Self Service** | ESS | A module in ServiceNow that allows users to make requests, view articles, log incidents, and search the knowledge base through a user-friendly website called the Employee Self-Service Portal (ESS Portal). |
| **Event** | | A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item, or monitoring tool. |
| **Impact** | | A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority. |
| **Incident** | | An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet |

| Term | Acronym | Definition |
|---|---|---|
| | | affected service is also an incident. |
| **Key Performance Indicator** | KPI | A metric that is used to help manage an IT service, process, plan, project, or other activity. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service, or activity. They should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed. |
| **Known Error** | KE | A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their life cycle by problem management. Development groups or suppliers may also identify known errors. |
| **Major Incident** | | The highest category of impact for an incident. A major incident results in significant disruption to the business. |
| **Metric** | | Something that is measured and reported to help manage a process, IT service, or activity. |
| **Policy** | | Formally documented management expectations and intentions. Policies are used to direct decisions and to ensure consistent development and implementation of processes, standards, roles, activities, IT infrastructure, and so on. |
| **Post-implementation Review** | PIR | A review that takes place after a change or a project has been implemented. It determines if the change or project was successful and identifies opportunities for improvement. |
| **Priority** | | A category 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. For example, the SLA may state that priority 2 incidents must be resolved within 12 hours. |
| **Problem** | | A cause of one or more incidents. The cause is not usually known at the time a problem record is created. The problem management process is responsible for further investigation. |
| **RACI** | RACI | A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted, and informed. |
| **Release** | | One or more changes to in IT service that are built, tested, and deployed together. A single release may include changes to hardware, software, documentation, process, and other components. |
| **Request for Change** | RFC | A formal detailed proposal for a change to be made. The term is often misused to mean change record or the change itself. |

| Term | Acronym | Definition |
|---|---|---|
| **Restore** | | Taking action to return an IT service to the users after repair and recovery from an incident. This is the primary objective of incident management. |
| **Risk** | | A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. |
| **Role** | | A set of responsibilities, activities, and authorities assigned to a person or team. A role is defined in a process or function. One person or team may have multiple roles. For example, a single person may carry out the role of configuration manager and change manager. |
| **Root Cause** | | The underlying or original cause of an incident or problem. |
| **Root Cause Analysis** | RCA | An activity that identifies the root cause of an incident or problem. Root cause analysis typically concentrates on IT infrastructure failures. |
| **Service** | | A means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks. |
| **Service Desk** | | The single point of contact between the service provider and the users. A typical service desk manages incidents and service requests, and also handles communication with the users. |
| **Service Level** | | Measured and reported achievement against one or more service level targets. |
| **Service Level Agreement** | SLA | An agreement between an IT service provider and a customer. A service level agreement describes the IT service; documents service level targets, and specifies the responsibilities of the IT service provider and the customer. |
| **Service Request** | | A formal request from a user for something to be provided, for example, a request for information or advice; to reset a password; or to install a workstation for a new user. |
| **Stakeholder** | | A person who has an interest in an organization, project, or IT service. Stakeholders may be interested in the activities, targets, resources, or deliverables. Stakeholders may include customers, partners, employees, shareholders, owners, or others. |
| **User** | | A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly. |

| Term | Acronym | Definition |
|---|---|---|
| **Workaround** | | Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available, for example, by restarting a failed configuration item. Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record. |

# Appendix C: Incident Categorization

Incident categorization is commonly used to drive assignment in the incident management process as well as establish trends (incident types/frequencies) for use in problem management, supplier management and other ITSM activities.

- See Categorizing Incidents in the ServiceNow Wiki for a list of the category and subcategory values available in the base system.
- See Assigning Incidents in the ServiceNow Wiki for a description of how to automate assignment based on categorization.

This method of categorization requires the creator of the incident to manually select the category and subcategory from predefined lists.

It is possible to *automatically categorize and assign the incident based on the CI* that is identified in the incident record. With this technique, the incident management process inherits the same categorization schema as CIs maintained through the configuration management process and the category of an incident is automatically determined once the affected CI is identified in the incident record. This technique ensures more accurate and consistent categorization of incidents and supports a CI-centric approach to IT service management.

# Appendix D: Incident Prioritization

Incident prioritization typically drives the timescales associated with the handling of the incident and the targeted time to resolution. There are a couple of methods that can be used to determine priority.

ITIL suggests that priority be made dependent on impact and urgency, where:

- **Impact** is the effect that an incident has on business.
- **Urgency** is the extent to which the incident's resolution can bear delay.

Priority is generated from urgency and impact according to the following table.

| | Urgency High | Urgency Medium | Urgency Low |
|---|---|---|---|
| Impact High | Priority 1 | Priority 2 | Priority 3 |
| Impact Medium | Priority 2 | Priority 3 | Priority 4 |
| Impact Low | Priority 3 | Priority 4 | Priority 5 |

It is possible to *automatically establish the priority of the incident based on the CI* that is identified in the incident record. With this technique, the business criticality value of the CI is used to determine the priority of the incident. This ensures a more accurate and consistent prioritization of incidents, as the determination of impact and urgency can be a subjective call.