Master the incident management process

Restore services fast and minimize the impact of incidents

Introduction

This success guide is a detailed explanation of how you can use ServiceNow® Incident Management to maintain the best possible levels of service quality and availability—even when incidents occur. When an incident happens, following a solid incident management process will help you restore normal service operation as quickly as possible and minimize the adverse impact the incident could have on business operations.

Incident management process scope

Incident management includes:

- The identification and diagnosis of incidents through event management, technical identification, and the user reported
- Resolving all incidents as quickly as possible using:
    - Defined resolution processes
    - Known errors identified through problem management (workarounds)
    - New resolution activities identified through diagnosis
- Identifying incidents and groups of incidents that require further analysis in the problem management process to eliminate them or to reduce their resolution times

Incident management process objectives

Your incident management process should:

- Require that your team uses standard methods and procedures for efficient and prompt incident response, analysis, documentation, management, and reporting
- Increase your business and support staff's visibility and communication of incidents
- Enhance the business's perception of IT by using of a professional approach to quickly resolve and communicate incidents when they occur
- Align incident management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services

Regardless of your level of maturity with ServiceNow, follow this guide as closely as possible. At ServiceNow, we encourage using the same simple, lean ITSM processes that are reflected in our out-of-the-box designs.

In this guide, you'll find additional recommendations from ServiceNow Professional Services beyond the specific out-of-the-box (OOTB) functionality. You may add additional functionality to what's offered, but you should only do so in scenarios when you will achieve a required business outcome that can't be achieved using an OOTB method. When you follow this approach, your upgrade paths will be smoother, and you'll be better able to expand your use of the Now Platform®.

This success guide will help you develop and maintain an effective incident management process by:

- Explaining how to identify and diagnose incidents
- Explaining how to resolve incidents through resolution processes and known errors
- Defining when incidents require further investigation
- How to integrate other processes with incident management

BEFORE YOU START, YOU NEED:

- A process owner who is the authoritative voice for the organization and is able to make decisions
- A willingness to critically examine your current working practices

Terms and definitions

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, ensuring that the best possible levels of service quality and availability are maintained.

Normal service operation is defined as an operational state where services and configuration items (CIs) are performing within agreed service and operational levels. Incident management is responsible for managing the lifecycle of all incidents. A temporary workaround to restore service is all that is required in many cases to complete the process.

ServiceNow focuses on the use of automation and information to speed the path to resolution.

ServiceNow Incident Management – This process relies heavily on:

- The configuration management process for incident assignment and impact analysis
- The problem management process to investigate the root causes of incidents and provide workarounds and permanent resolutions
- The change management process to control the changes required to resolve incidents and minimize the incidents caused by the change

Roles and responsibilities

Caller

The caller is the person being impacted by degradation to a service or someone who has discovered an impact or potential impact to a service. A caller could be a member of an operational support team. Alternatively, if the issue has been discovered automatically through an event monitoring system, the caller may be captured against that system.

Responsibilities

- Bring incidents to the service desk's attention.
- Participate in the implementation of a solution or workaround.
- Confirm the team successfully resolved the incident.

ServiceNow role – No role is required, but the caller needs a login.

First line – The service desk agent

The service desk agent (SDA) is the front line or face of your technology organization. They're the people the rest of the organization interact with most commonly—typically when they're experiencing some sort of technology-related issue.

The SDA's goal is to deal with as many incidents as possible themselves at the time they receive the incident (called a first-call or initial-contact resolution). Ideally, they want to solve the caller's issue immediately without involving other support teams and without the caller having to contact them a second time.

Even if the SDA can't resolve the issue and others provide the solution, many organizations still keep the incident's ownership and communication with the SDA.

Since SDAs are expected to resolve incidents themselves, they need a very broad range of knowledge across all technical services and may be considered "jacks of all trades, masters of none." Given their possibly limited knowledge on each subject, they need access to information to help them diagnose issues. SDAs must, at least, try to determine a good line of investigation so they can pass the incident to the correct IT support team for further diagnosis.

Responsibilities

- Record, own, monitor, track, and communicate about incidents.
- Investigate and diagnose incidents.
- Provide resolutions and workarounds from standard operating procedures and existing known errors.
- Escalate incidents to IT support.
- Communicate with the caller.

The SDA engages in the process by setting the **Assignment Group** field to the **Service Desk group** and the **Assigned to** field to the individual SDA.

ServiceNow role – The **itil** role is required.

Second and third line – IT support teams

When the SDAs are unable to resolve incidents on their own, they must pass responsibility to someone else with more knowledge and experience. Organizations will differ in how they structure their support teams, but it's a common approach to have second-line support teams within the service desk reporting structure who specialize in particular services and are considered the subject matter experts (SMEs) for these services. Escalating to the second line of support still keeps the incident within the service desk.

The third line of support is typically the operational team responsible for the service. For example, it might be database support, network support, application development, etc. These are the teams with their main focus on delivering and maintaining that service.

Your organization may not have a fourth line of support (you may not need one). If you do, the service is could be supplied by an external vendor after all internal support teams have failed to resolve the issue.

Essentially, the higher the line of support is, the more knowledge and experience the support group is expected to have on the specific service in question. Keep in mind that the high-level support groups will also have less general knowledge across all services.

Responsibilities

- Investigate and diagnose incidents escalated from the service desk.
- Develop workarounds.
- Resolve and recover assigned incidents.
- Create incidents after detecting a service failure, quality degradation, or a situation that may result in one.

The IT support team engages in the process by changing the **Assignment Group** field to the appropriate support group and the **Assigned to** field to the individual support staff.

ServiceNow role – The **itil** role is required.

Major incident manager

The incident management process doesn't include a review process, like the change management process, which requires process managers to review each ticket in some manner. The major incident manager is concerned entirely with major incidents and is the coordinator for resolving a major incident as soon as possible and ensuring that it does not reoccur.

Responsibilities

- Coordinate the investigation and resolution of major incidents assigned to you.
- Assign tasks to other teams to investigate and resolve the major incident.
- Manage the communications during the major incident to both business and IT stakeholders.
- Conduct a review of the major incident once it's resolved.

The major incident manager engages in the process by changing the **Assignment group** field to the responsible major incident management group and the **Assigned to** field to the correct agent within the assigned group.

ServiceNow role – The **major_incident_manager** role is required.

Incident admin

The incident admin is the person assigned the **incident_manager** role within ServiceNow and is able to configure certain elements of the incident process that do not require assistance from the system admin.

Responsibilities

- Configure incident properties.
- Configure major incident trigger rules.

ServiceNow role – The **incident_manager** role is required for incident administration. This role will gain additional capabilities in future releases.

Incident management process owner

The incident management process owner's primary objective is to own and maintain the incident management process. The process owner role is usually filled by a senior manager with the ability and authority to ensure all stakeholders roll out and use the process.

Responsibilities

- Define the overall mission of the process.
- Establish and communicate the process's mission, goals, and objectives to all stakeholders.
- Document and maintain the process and procedures.
- Resolve any cross-functional (departmental) issues.
- Ensure proper staffing and training for execution.
- Direct the incident management roles.
- Ensure consistent execution of the process across the organization.
- Monitor, measure, and report on the effectiveness of the process to senior management.
- Continually improve the process.

How incidents are initiated

Directly in ServiceNow – The SDA can create an incident directly as a result of a phone call or email from a user. A member of IT support can raise an incident when they discover evidence of one.

Self-service – End users can make use the Self-Service Portal to create a ticket. The Self-Service Portal uses a record producer to generate an incident record rather than exposing the full incident form to users who wouldn't understand most of it.

Automatically via integrations – Incidents can be automatically generated via external systems such as event monitoring.

Support chat – A service agent can generate incidents from chat conversations with a user. The chat log is included in the **Incident Activity Log** and a link to the incident is sent to the user.

Inbound email – Inbound emails can generate incident records. ServiceNow does not recommend this method since it cannot reliably collect enough information from the email in order to create an incident that a team can work on.

Walk-Up Experience – By visiting an onsite IT support location, users can create an incident using the Walk-Up interface.

Incident management lifecycle

The states in every ServiceNow application serve a specific purpose. They're designed to make it clear where a particular record currently resides in a process and to display progress. States should represent a unique phase in a process where a specific set of related activities are grouped together and designed to achieve a particular outcome so you can move to the next phase of the process.

For example, in the incident management process, the **Resolved** state should contain all activities required to understand what was done to resolve the incident. OOTB ServiceNow Incident Management has the following state model:

- **New**
- **In Progress**
- **On Hold**
- **Resolved**
- **Closed**
- **Canceled**

Process overview

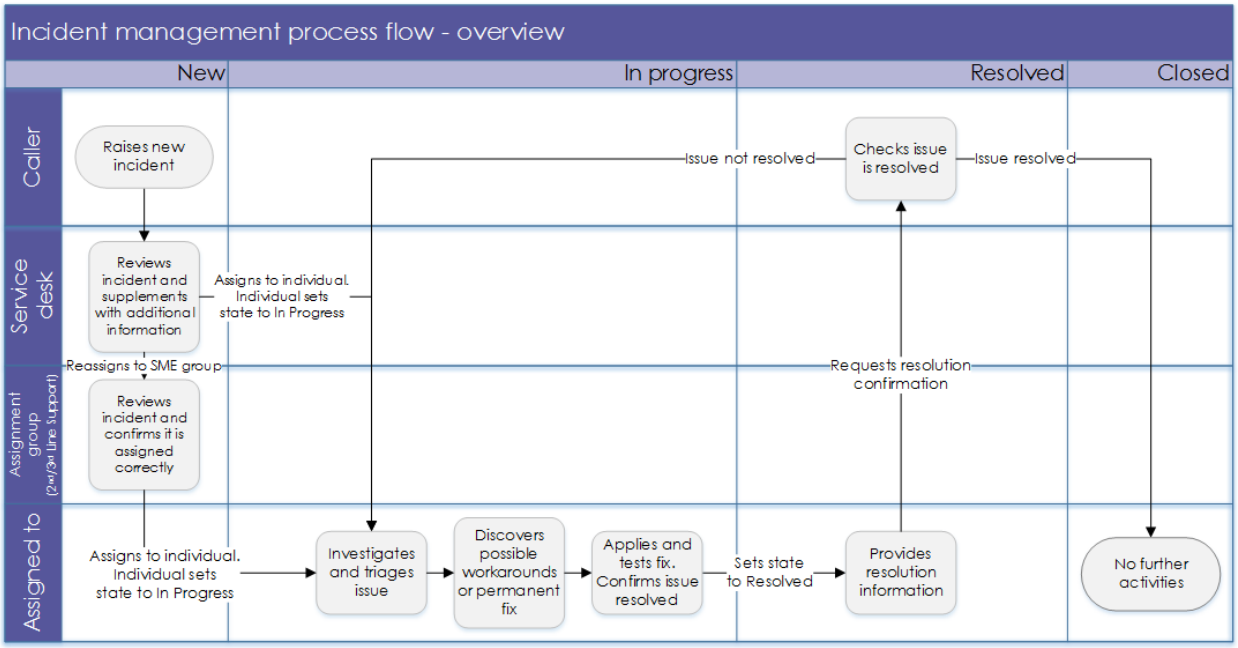
Incident management process flow - overview
New
In progress
Resolved
Closed
Caller
Service desk
Assignment group (2nd/3rd line Support)
Assigned to
Raises new incident
Reviews incident and supplements with additional information
Assigns to individual. Individual sets state to In Progress
Reassigns to SME group
Reviews incident and confirms it is assigned correctly
Assigns to individual. Individual sets state to In Progress
Investigates and triages issue
Discovers possible workarounds or permanent fix
Applies and tests fix. Confirms issue resolved
Sets state to Resolved
Provides resolution information
Requests resolution confirmation
Checks issue is resolved
Issue not resolved
Issue resolved
No further activities

Figure 1: The incident management process flow

State – New

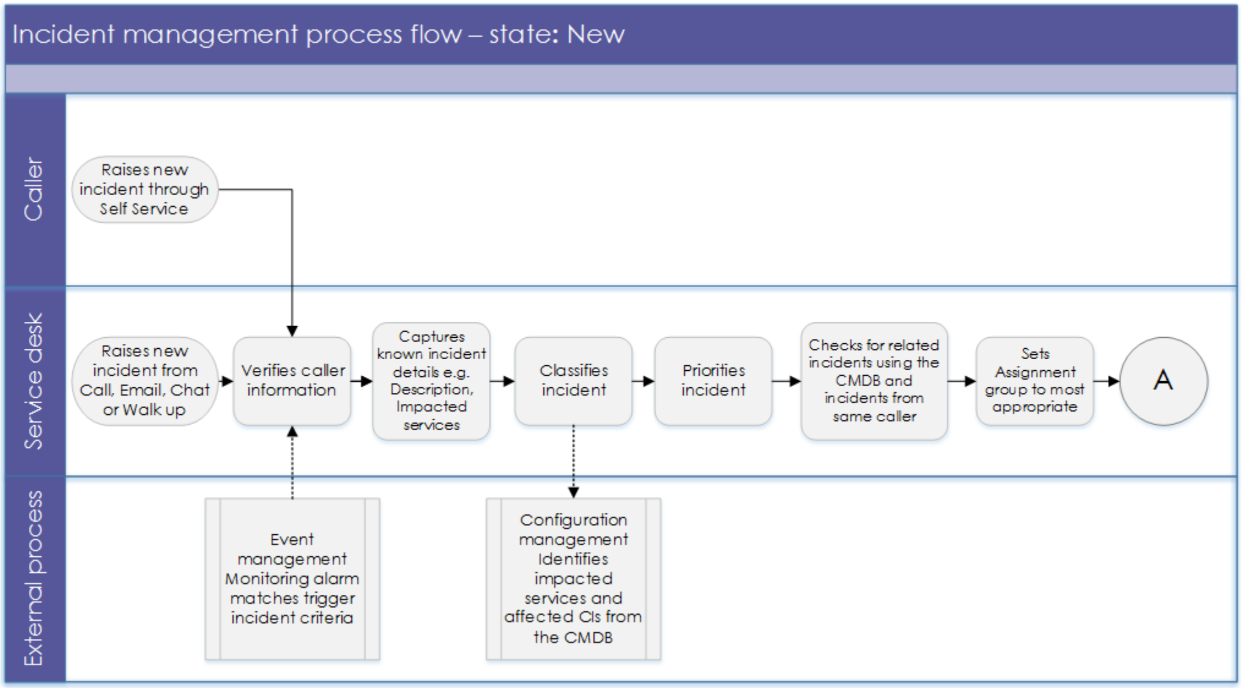
Incident management process flow – state: New
Caller
Service desk
External process
Raises new incident through Self Service
Raises new incident from Call, Email, Chat or Walk up
Verifies caller information
Captures known incident details e.g. Description, Impacted services
Classifies incident
Priorities incident
Checks for related incidents using the CMDB and incidents from same caller
Sets Assignment group to most appropriate
A
Event management Monitoring alarm matches trigger incident criteria
Configuration management Identifies impacted services and affected CIs from the CMDB

*Figure 2: The incident management process flow for the **New** state*

When an incident is first created, it is in the **New** state. The incident is automatically assigned to the service desk as the front line to review anything coming into the IT department for action.

In this state, the SDA opens the incident ticket and captures all known information about the symptoms the caller experienced. Capturing sufficient and relevant detail at this stage is very important—it helps with diagnosis if the incident requires escalation. The SDA should record the description of the incident in the caller's own words so they can use those terms again as they work with the caller.

The SDA must complete these mandatory fields:

- **Caller**
- **Business service**
- **Configuration item**
- **Contact type**
- **Impact**
- **Urgency**
- **Priority –** This is automatically populated from the **Impact** and **Urgency** fields.
- **Assignment group**
- **Short description**
- **Description**

If the incident is raised through self-service or email, the end user only needs to provide these details since they aren't likely to know or understand most of the remaining fields in the incident form:

- Caller
- Urgency
- Short description
- Description

The SDA then reviews the information provided and supplements it with further details.

Process-critical attributes

There are a number of particular attributes captured in an incident that drive aspects of the process.

Priority

Incident prioritization typically drives the schedule of the incident through its resolution. In particular, this will impact the service level agreements (SLAs) associated with the incident. Priority is calculated based on the incident's impact and urgency.

Be sure your customers are clear on how to define the different levels of impact, urgency, and response and restoration time frames associated with the priorities. This information is useful when you define SLAs—and it ensures consistency across the process.

- **Impact –** The effect that an incident has on business

  - For example, if the incident only impacts a single employee, its impact is low compared to 500,000 paying customers with social media accounts.

- **Urgency –** The extent to which the incident's resolution can bear delay.

Priority is generated from urgency and impact according to this table.

		Urgency		
		1 – High	2 – Medium	3 – Low
Impact	1 – High	Priority 1 – Critical	Priority 2 – High	Priority 3 – Medium
	2 – Medium	Priority 2 – High	Priority 3 – Medium	Priority 4 – Low
	3 – Low	Priority 3 – Medium	Priority 4 – Low	Priority 4 – Low

Table 1: How an incident's priority is determined by its impact and urgency

It's possible to automatically establish the priority of the incident based on the CI that's identified in the incident record. With this technique, the business criticality value of the CI is used to determine the priority of the incident. For example, an online banking service is considered critical to a financial organization. If the CI is related to the incident, the priority can automatically set to **Critical** as a result. Using this technique, you can more accurately and consistently prioritize incidents, since determining their impact and urgency can be subjective.

Categories, business services, and CIs

You can use the **Category** field to identify what the incident is impacting, but only if your organization isn't using a CMDB yet or if your CMDB is extremely immature.

If your CMDB is mature, its CI fields will identify what the incident is impacting with more significantly enhanced data that you can identify in the **Category** field. In this case, replace the **Category** field with the **Business service** and **Configuration item** fields and related lists to allow better interaction across the various ITSM processes. The business service CI is available across all ITSM processes, so it must be related to an incident to provide true insight into the service's performance and health. When you use categories, the data is limited to the incident management process only and doesn't provide value beyond that.

Incident assignment

Here's the incident assignment process:

1. The SDA may already be aware of the correct group to assign the incident to—if so, they reassign it to that group when it's in this state. If you're using automated assignment, that also happens in this state, usually once the SDA populates the business service or CI.

   - If the SDA needs to investigate and perform triage on the incident, that occurs during the **In Progress** state. At this point, they assign the incident to themselves using the **Assigned to** field and set the state field to **In Progress**.

2. The new assignment group reviews the incident that shows up in their work list and assigns it to one person.
3. The assigned person begins working on the incident and manually sets its state to **In Progress**. This stops the clock on any response SLAs that are running since changing the state to **In Progress** means someone is responding to the incident.

> **Heads up!**
>
> You *must* assign an individual to the incident in order for it to move to **In Progress**. This way, anyone who needs an update or who wants to discuss the issue will know who is responsible for it.

State – In Progress

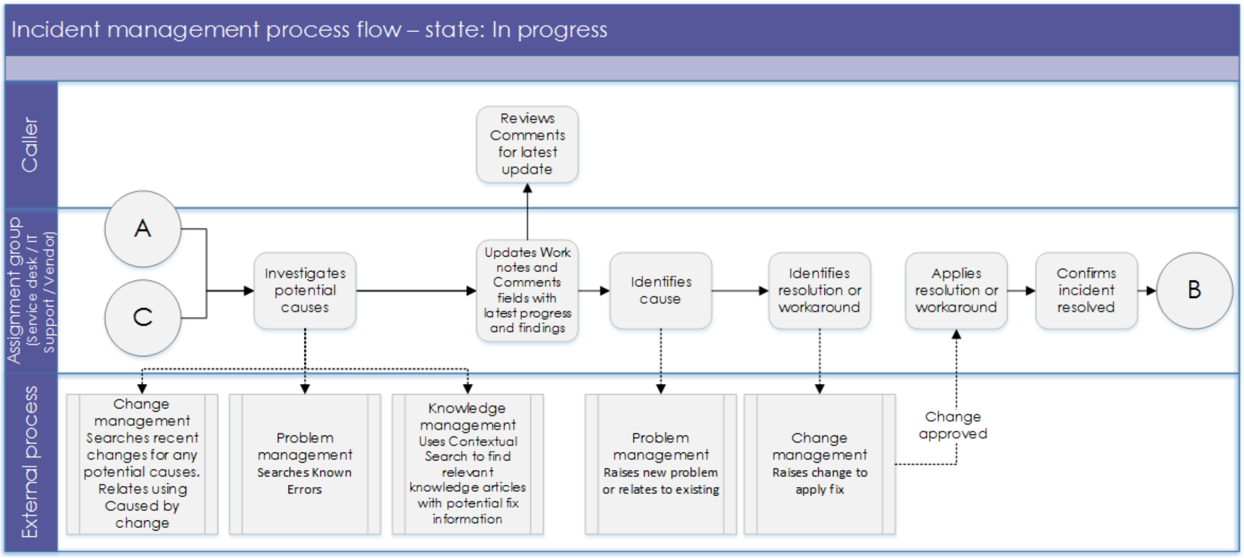
Incident management process flow – state: In progress
Caller
Assignment group (Service desk / IT Support / Vendor)
External process
Reviews Comments for latest update
A
C
Investigates potential causes
Updates Work notes and Comments fields with latest progress and findings
Identifies cause
Identifies resolution or workaround
Applies resolution or workaround
Confirms incident resolved
B
Change management Searches recent changes for any potential causes. Relates using Caused by change
Problem management Searches Known Errors
Knowledge management Uses Contextual Search to find relevant knowledge articles with potential fix information
Problem management Raises new problem or relates to existing
Change management Raises change to apply fix
Change approved

*Figure 3: The incident management process flow for the **In Progress** state*

During the **In Progress** state, someone is working on the incident. This state covers a large and varied number of activities that are required in order to resolve the issue.

The person assigned the incident begins by investigating and triaging to establish the incident's cause and how to fix it. To help them resolve the issue, they can:

- Use the contextual search feature to display knowledge articles that match the incident or are similar to its short description
- Refer to similar incidents and problem records

During this investigation and triage, they may discover that there is a better-suited group or individual to address the issue. If so, they'll reassign the incident. To do this, they'll update the **Assignment group** and **Assigned to** fields. This could involve passing the incident to second- or third-line SMEs. Next, the new assignees receive an email notification to make them aware they are now responsible for the incident.

An incident could be reassigned multiple times while it's in the **In Progress** state since multiple different teams may need to be involved. When reassigning an incident, the **Work note** field is mandatory because it explains why the incident is being assigned to the new group or individual and what is expected of them.

> **Heads up!**
>
> Reassigning an incident will not reset the SLAs attached to the incident unless the SLA is specifically tracking reassignment only. Given that, if an SLA only has one hour remaining before it breaches and is reassigned to a new team, that team still has only one hour.

While the incident is in the **In Progress** state, everyone assigned to it must use the **Work notes** field to update it and capture the actions they've taken and what they've learned.

When you need to provide an update to the original caller, use the **Comments** field. Updates to the **Comments** field can be automatically sent to the caller. This saves the help desk staff from having to update callers and the callers from having to chase down updates.

When a fix is identified by the investigation, the individual assigned to it will apply the fix to resolve the issue. The fix may be a permanent solution or a temporary workaround—either is acceptable if it solves the issue at that time.

The identified fix could be from:

- A knowledge article
- A known error
- Diagnostic steps undertaken by the individuals working on the incident
- An existing change to be implemented

The first three activities may result in needing to raise a change to resolve the incident. Whether to raise a change is often based on the service desk's operational model. For example, if there's an existing knowledge article associated with the incident that is an acceptable repeatable process, it would not require raising a change record, but a unique set of resolution steps would.

If the incident is purely waiting for the change to be implemented and no other activities are occurring, the **State** field can be changed to **On Hold** with an **On hold reason** of **Awaiting Change**.

Note: If, during investigation, someone discovers that a change was the cause of the incident, use the **Caused by Change** field to relate the change to the incident.

Once they've applied the fix or workaround, the person assigned the incident tests the fix to see if it resolves the issue. If they believe it does, they click the **Resolve** button to change its state to **Resolved**.

State – On Hold

Use the **On Hold** state to indicate when an incident isn't resolved yet and work on it is temporarily paused while the person assigned the incident waits for another group or person to take some action.

When you change the incident's state to **On Hold**, the **On hold reason** field becomes mandatory and provides these choices:

- **Awaiting Caller**
- **Awaiting Change**
- **Awaiting Problem**
- **Awaiting Vendor**

ServiceNow recommends removing **Awaiting Problem** from the choices. Resolving an incident should never be dependent on a problem.

The Service Level Management application makes heavy use of this state since putting something on hold (**Awaiting Caller**) typically acts as the pause condition for all SLAs.

State – Resolved

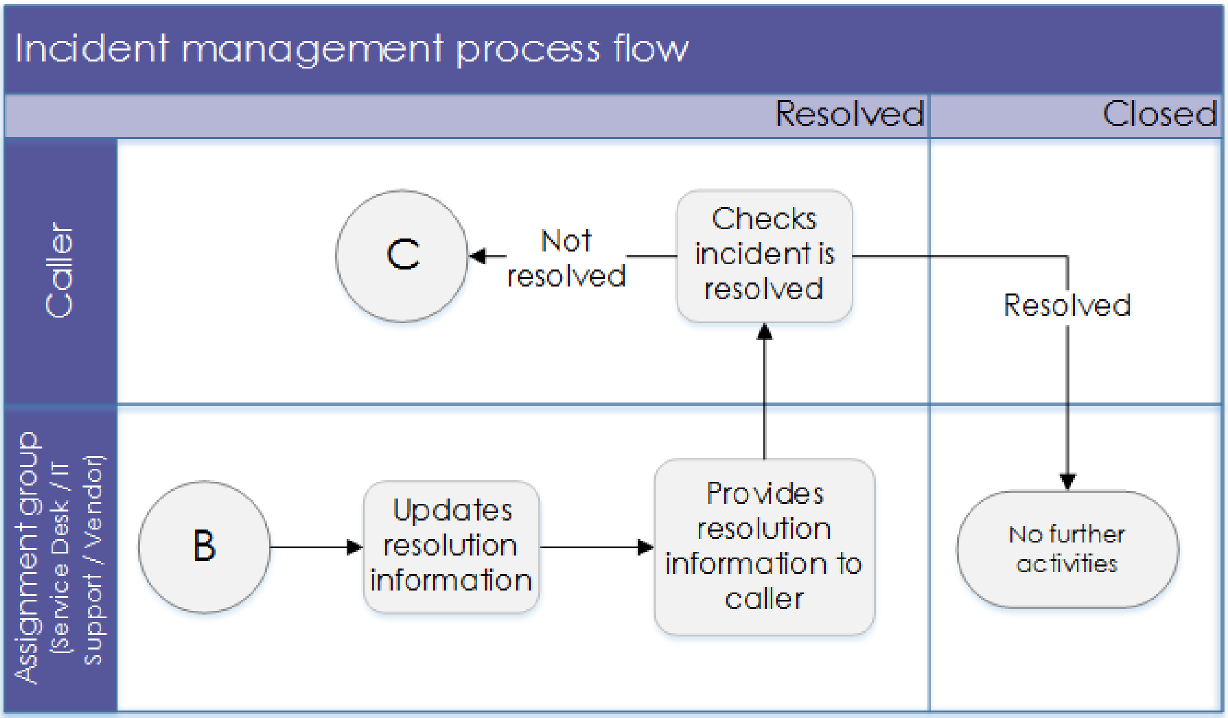
Incident management process flow
Resolved
Closed
Caller
Assignment group (Service Desk / IT Support / Vendor)
C
Not resolved
Checks incident is resolved
Resolved
B
Updates resolution information
Provides resolution information to caller
No further activities

Figure 4: Incident management process flow for the ***Resolved*** *state*

In order to move the state to **Resolved**, the person assigned to it needs to give some further details to explain what the problem was and how it was fixed. The mandatory fields are:

- **Resolution code –** This is a list of choices focused on the nature of the resolution provided, for example, whether it was a workaround or a permanent fix. These choices aren't intended to explain how the incident was resolved.
- **Resolution notes –** This is a free-text field where you can describe the issue and how it was resolved. This field was deliberately designed to be free text rather than a list of categories or other items to choose from.

Experience shows that there tend to be a large number of possible codes. These must be filtered based on the CI related to the incident. If the filter is not applied, the person resolving the incident has an overwhelming number of options, making the chance of selecting the correct data significantly reduced. If they select the wrong data, it won't offer value.

Expert tip

The effort involved in maintaining this level of related data is usually high, and the maintenance costs invariably outweigh the business benefits of being able to report on it. As such, if you require codes to track what the issue was and how it was fixed, you should only do it when you have a clear business benefit to achieve.

Once the resolution information is provided, the caller receives email notification that the incident is resolved and has seven days to disagree. If the caller believes the incident is *not* fixed:

1. The caller clicks the link to the incident in the email.
2. Once in the incident, the caller clicks the **Reopen Incident** button. They must complete the **Additional comment** field to explain why they believe the incident is not yet resolved.
3. The state for the incident returns to **In Progress** and clears the **Resolution code** and **Resolution notes** fields.
4. The person assigned the incident receives a notification containing the caller's additional comments.

If the caller agrees that the issue is resolved, no further action is required. The incident remains in the **Resolved** state for seven days, after which the **State** field automatically updates to **Closed**.

State – Closed

No activities take place in the **Closed** state. Should the incident reoccur, a new ticket must be raised. Once an incident is closed, it cannot be reopened. In addition, the associated SLAs typically stop in this state.

State – Canceled

There are very few scenarios when an incident is genuinely canceled. This only occurs when an incident was raised in error—usually prematurely, before realizing there is no real issue.

Major incident management

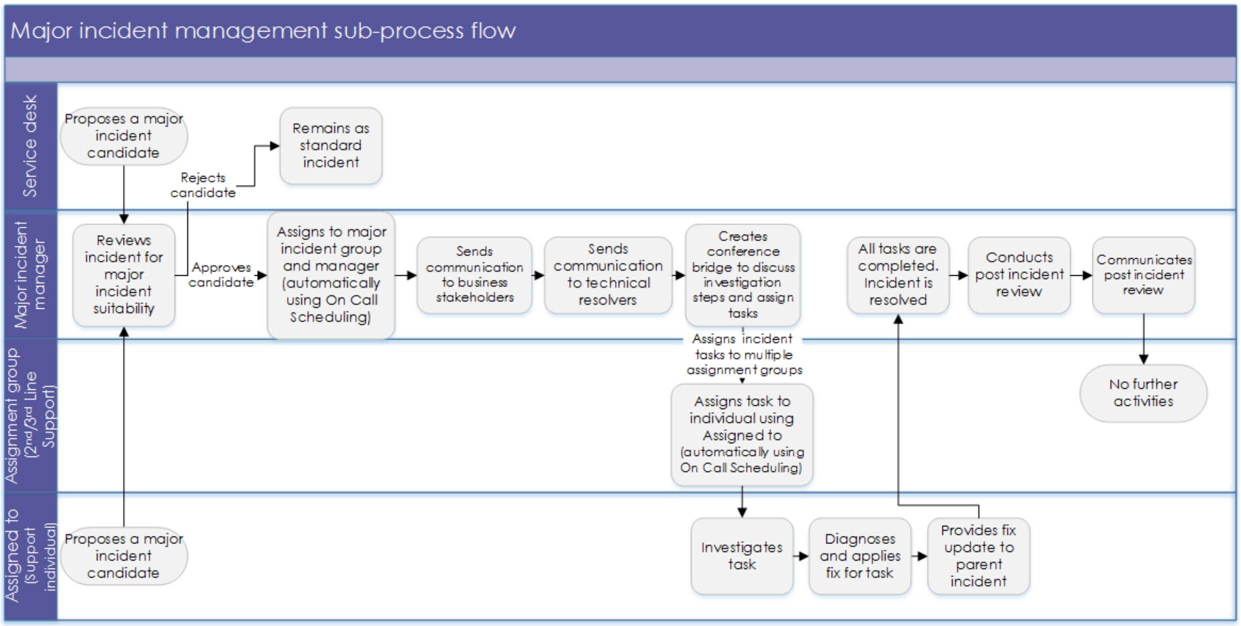
Major incident management sub-process flow
Service desk
Major incident manager
Assignment group (2nd/3rd Line Support)
Assigned to (support individual)
Proposes a major incident candidate
Remains as standard incident
Rejects candidate
Reviews incident for major incident suitability
Approves candidate
Assigns to major incident group and manager (automatically using On Call Scheduling)
Sends communication to business stakeholders
Sends communication to technical resolvers
Creates conference bridge to discuss investigation steps and assign tasks
Assigns incident tasks to multiple assignment groups
All tasks are completed. Incident is resolved
Conducts post incident review
Communicates post incident review
No further activities
Assigns task to individual using Assigned to (automatically using On Call Scheduling)
Proposes a major incident candidate
Investigates task
Diagnoses and applies fix for task
Provides fix update to parent incident

Figure 5: Incident management process flow for major incidents

When an incident's impact on the business is considered critical, it's considered a major incident. You'll manage these using an incident management subprocess that involves additional activities intended to reduce or remove the impact as quickly as possible.

The incident manager coordinates the major incident's activities through its lifecycle until it's resolved and:

- Uses incident tasks when multiple support groups and users need to work on the resolution concurrently
- Uses the major incident workbench to communicate updates on the progress of the incident as they become available
- When the incident is resolved, conducts a review of the incident and performs any necessary follow-up activities

Incident candidates

Users of the incident process may consider a particular incident to require major incident management, but they cannot automatically promote an incident into this process since it will trigger a number of actions and activities for other teams that they may not be aware of. Incidents are initially proposed as a **Major Incident Candidate** so incident managers can confirm whether it is truly a major incident. There are three possible ways to do this:

- **Automatically via predefined trigger criteria –** When these criteria are met, the incident is immediately proposed as a candidate.
- **Manually from an existing incident –** Users can manually propose a candidate from an existing incident by selecting **Propose Major Incident** from the drop-down menu.

- **Manually where no incident currently exists –** If an incident does not already exist, major incident managers can select the **Create Major Incident Candidate** option directly from the left navigation menu.

Once the candidate is proposed:

1. A new form section called **Major Incident** displays on the incident record. This section includes additional fields specific to major incidents. If you have relevant information for them, populate the **Business impact** and **Probable cause** fields.
2. The incident manager reviews all proposed candidates and either accepts or rejects them.
3. When a candidate is promoted to a major incident, the **Major incident state** field automatically updates to **Accepted** and the **Assignment group** field updates to the **Major Incident Management group** if it was previously empty.

   Note: The major incident manager reviewing the candidate should manually reassign it to the correct incident management group if it was previously assigned.

During the course of the major incident, the major incident manager can log the specific actions taken in the main incident record in the **Actions taken** field. This keeps these particular notes separate from any general notes that were added to the major incident.

Incident tasks

The incident remains assigned to the major incident management group for the remainder of the lifecycle. As part of the incident's investigation and resolution process, the major incident manager designates actions and activities to other groups and individuals by creating individual incident tasks from the **Incident Tasks** related list that's only available for major incidents.

Major incident workbench

The major incident manager can use the workbench to see much of the information associated with the major incident, but it's primarily used to coordinate communication activities.

Incident alerts

The **Communication** tab within the workbench includes a set of predefined communication tasks to complete. These tasks use the incident alert feature and are created when you initiate the task from the workbench. The major incident manager populates the content of the task and assigns it to the relevant individual for action.

When the tasks are closed, this is reflected in the workbench.

Conference calls

The **Conference** tab is only displayed if you've purchased and enabled the Notify plugin. You can initiate conference calls directly from this tab.

Major incident reviews

Once the major incident is in the **Resolved** state, the major incident manager reviews what happened. This usually involves understanding the root cause and concluding whether any steps can be taken to avoid the situation reoccurring. The manager captures any lessons learned during this review as well. If the review is comprehensive, the manager can create and assign incident tasks. Once the review is complete, the incident can be closed.

Managing all major incidents

Major incident managers can keep track of all major incidents using the Major Incident Overview module's dashboard.

Parent and child incidents

When an incident is causing a widespread impact, you'll see this from the number of incident records raised by different callers for the same issue. Although these incidents report the same thing and might be considered duplicates of each other, capture each instance so the impact's size can be more easily determined.

The downside of having many incidents logged with the same issue is that they'll all need to be updated as the incident is diagnosed and resolved. You can avoid this by designating one incident as the parent and relating all other incidents to it using the **Child Incidents** related list. When **Work notes** or **Additional comments** are added to the parent, they automatically copy to all related child incidents. In addition, when the parent is resolved, the child incidents are also resolved and the closure information is copied over. Incidents are related in this manner using the **Parent incident** field or **Child Incidents** related list.

Handling ad hoc questions and help

When a caller has an ad hoc question or request for help that does not involve an issue, you can capture it using the Service Desk Call feature. This allows you to handle the question without having to log an incident or create a service request.

Expert tip

Don't create a catalog item in your Service Catalog when callers have these types of questions—the request, requested item, and catalog task structure is too complex for this need. If the customer doesn't want to use the Service Desk Call feature, capture this interaction with an incident record. When using the category field, set the field to **Inquiry/Help** to distinguish it from a true incident.

Other processes

Change management

For many incidents, the solution will require work on a service, hardware, or software. Conducting this work requires raising a change record. To do this, select the **Create Normal Change** or **Create Emergency Change** option from the drop-down menu.

Emergency changes typically require a related incident record to prove that they're urgent enough to bypass the full process and lead times. You can also do this from the change record using the **Incidents Fixed by Change** related list.

In some cases, a change was implemented that resulted in an incident. An incident record can be created from the originating change record to show the cause and to link the chain of events together. To do this, use the **Incidents Caused by Change** related list.

Problem management

Problem management is the subsequent process for incidents that require further investigation to find the root cause. You can generate problem records directly from the incident record, which will copy over key data. To do this, select **Create Problem** from the drop-down menu.

There could be many incidents associated with a single problem—the more incidents you have, the clearer the scale of impact becomes. It may be that when the problem was first encountered, the number of associated incidents was low, so the team decided not to pursue a permanent fix. But as the number increases and the impact widens, you may review that decision. You can add multiple incidents to the problem using the **Incidents** related list.

If a workaround exists for the problem, log it in in the **Workaround** field of the problem record and click **Communicate Workaround**. This automatically pushes the workaround into all associated incident records.

Once the problem is fixed, all associated incidents can be automatically closed.

Configuration management

The configuration management system underpins all incident management activities. It not only hosts the incident and other service management records, it contains details of the infrastructure vital to efficient call handling.

The CMDB is used in the incident management process by relating CIs, including business services, to the incident. This allows you to use Dependency Views to display the relationship between the selected CI and other CIs related up and downstream.

Knowledge management

Knowledge is a vital part of the incident process. It's available using the contextual search feature embedded in the incident record and record producers to display relevant knowledge articles as the incident is being created. Contextual search uses the text entered into the **Short description** field or other text fields to find close matches in the knowledge base, then displays them.

Service level management

Service level management (SLM) defines measurable responses to service disruptions. Incident management provides historical data that lets users review SLAs objectively and regularly. SLM defines the acceptable levels of service that incident management works within, including:

- Incident response times
- Impact definitions
- Target fix times
- Service definitions

- Rules for requesting services

Process governance

Measurement

Key performance indicators (KPIs) evaluate the success of a particular activity toward meeting its critical success factors. You can successfully manage KPIs either by repeatedly meeting an objective (maintaining the KPI) or by making progress toward an objective (increasing or decreasing the KPI).

The Benchmarks feature in ServiceNow gives you instant visibility into your KPIs and trends, as well as comparative insight relative to your peers' industry averages. You can contrast the performance of your organization with recognized industry standards, and view a side-by-side comparison of your performance with global benchmarks. Benchmarks offers the following ITSM KPIs:

- % of high-priority incidents resolved
- Average time to resolve high-priority incident
- Average time to resolve an incident
- % of incidents resolved on first assignment
- Number of incidents created per user

Dashboards and reporting

Process KPIs

Process KPIs provide information on the effectiveness of the process and the impact of continuous improvement efforts, and they are:

- Best represented as trend lines and tracked over time
- Monitored by the process owner

Item	**Purpose**
Reassignment count	This metric shows the total number of times the **Assignment Group** field is changed and shows you how quick/easy it is for the incident to get to the right group for resolution.
Resolved on first assignment	This metric shows the percentage of incidents resolved by the first line or first person to be assigned to the ticket. This helps you understand how well the service desk is able to handle incidents without reassigning them to a costlier resource.
Resolved within SLA/OLA	Seeing the percentage of incidents resolved within an SLA/OLA helps you understand whether the SLAs/OLAs are unachievable and need a review or whether there is an issue with operational practices.

Table 2: Some process KPIs and their purpose

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 service desk and incident management team.

Item	Purpose
Pie chart of active incidents, by priority	This data shows the priority distribution of the current workload and allows you to drill down into detailed records.
List of active major incidents	This data gives you high visibility into the major incident events in progress.
List of active incidents that have breached an SLA	See a quick view of the incidents that need immediate attention to prevent further degradation of resolution time.
List of incidents reactivated from caller feedback	See a quick view of the incidents that need immediate attention to meet their resolution target (and provide customer satisfaction).

Table 3: Some operational KPIs and their purpose

Reports and homepages

There are numerous default reports available in ServiceNow that you can use to generate charts, publish to a URL, or schedule to run and distribute at regular intervals. You can also create custom reports.

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 the records that exist in the ServiceNow tables.

The takeaway

As you move forward with the incident management process, keep these things in mind:

- Provide training tailored to user's roles.
- Build champions to help you coach and mentor.
- Have measurement and reporting available from the start to measure process performance.