servicenow

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

ITSM Incident Management

Process Guide

San Diego Release

Last Updated: 2/28/2022

Ref: 0001016

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table of Contents

Introduction 4
Principles and Basic Concepts 4
Process Scope 5
Process Objectives 5
Roles and Responsibilities 5
  Caller 5
Support Center Agent (1st Line) 6
IT Support Teams (2nd / 3rd Line) 6
Major Incident Manager 7
Incident Admin 7
Incident Management Process Owner 8
How incidents are initiated 9
Incident Management Lifecycle 10
  Process Overview 10
  State: New 11
  Impact Ratings: 12
  Urgency Ratings: 12
  Target Response and Resolution Times 13
  State: In Progress 15
  State: On Hold 17
  State: Resolved 18
  State: Closed 19
  State: Canceled 19
Major Incident Management 20
  Incident Candidates 20
  Incident Tasks 21
  Major Incident Workbench 21
  On-Call Scheduling 22
  Major Incident Reviews 22
  Managing all Major Incidents 22
Parent and Child Incidents 23
Handling Ad Hoc Questions/Help 23
Other Processes 24
  Change Management 24

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Problem Management 24
Configuration Management 24
Knowledge Management 24
Service Level Management 25
User Experience 25
Process Governance 26
Measurement 26
Dashboards and Reporting 26
Appendix A: RACI Matrix 28
Appendix B: Roles and Responsibilities 31

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Introduction

This process guide will provide a detailed explanation of how the incident management process is enabled within the ServiceNow platform. It is intended that this process be followed as closely as possible. ServiceNow encourages simple, lean ITSM processes and that is reflected in the out-of-the-box design. Additional functionality can be incorporated into what is offered; however, this should only be in scenarios where there is a required business outcome gained that could not be achieved using an out-of-the-box method. Following this approach should also ease upgrade paths and the ability to expand the use of the platform.

Principles and Basic Concepts

An incident is defined as an unplanned interruption or a reduction in the quality of a technical service or a failure of a configuration item (CI) that has not yet impacted a technical service. Incidents can include failures or degradation of services reported by users, technical staff, third-party suppliers and partners, or automatically from monitoring tools.

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 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.

Incident Management relies heavily on:

- The Configuration Management process for incident assignment and impact analysis.
- The Problem Management process for investigating root causes of incidents and providing workarounds and permanent resolutions.
- The Change Management process for controlling changes needed to resolve incidents and minimizing incidents caused by change.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Process Scope

The scope of Incident Management includes:

- The identification and diagnosis of incidents through Event Management, Technical identification, and user reported
- Communication about incident status to customers
- The resolution of all incidents as quickly as possible using:
  - Defined resolution processes
  - Problem Management identified Known Errors (workarounds)
  - Identifying new resolution activities through diagnosis.
- Identifying incidents and groups of incidents that require further analysis in the Problem Management process for elimination or reduction in resolution time

Process Objectives

The objectives of Incident Management are to:

- Ensure standard methods and procedures are used for efficient and prompt incident response, analysis, documentation, 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 service

Roles and Responsibilities

Caller

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

Responsible for:

- Bringing incidents to the attention of the Support Center
- Participating in the implementation of a solution or workaround
- Confirming successful resolution

ServiceNow Role Required:

No role is required in ServiceNow for this; however, a login will be needed.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Support Center Agent (1st Line)

The Support Center Agent (SCA) is the front line or face of the Technology organization. They will be the people the rest of the organization interacts with most commonly and this will typically be when users are experiencing some sort of technology related issue. The goal of the SCA is to deal with as many incidents as possible themselves at the point of receiving the incident. This is first call or initial contact resolution. Ideally, they want to solve the Callers issue immediately without having to involve other support teams and without the Caller having to contact them a second time.

Even if the issue cannot be dealt with by the SCA, many organizations will keep ownership and communication of the incident with the SCA even though others may be providing the actual resolution.

Since the SCA is expected to resolve incidents themselves, they need a very broad range of knowledge across all technical services, they may be considered a 'jack of all trades, master of none.' This means they need access to information to help with their diagnosis, as they are likely to have limited knowledge on each subject. They must at least try to determine a good line of investigation so that they can pass the incident to the correct IT Support team for further diagnosis.

Responsible for:

- Recording, ownership, monitoring, tracking, and communication about incidents
- Investigating and diagnosing incidents
- Providing resolutions and workarounds from standard operating procedures and existing known errors
- Escalating incidents to IT support
- Communicating with the caller

The Support Center Agent is engaged in the process by setting the Assignment Group field to the Support Center group and the Assigned to field to the individual SCA.

ServiceNow Role Required:

Support Center Agents will require the **itil** role, or **sn_incident_read** and **sn_incident_write roles** introduced with Incident Management (com.snc.itsm.roles.incident_management) plugin.

IT Support Teams (2nd / 3rd Line)

If a Support Center Agent is unable to resolve an incident on their own, they must pass responsibility to someone else who will have more knowledge and experience.

2nd line support is typically the operational team responsible for the service. For example, Database Support, Network Support, Application Development etc. These are the teams whose main focus is the delivery and maintenance of that service.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3rd line support may not need to exist in many organizations, but this could be where the service is supplied by an external vendor and all internal support teams have failed to resolve the issue. The incident now needs to be escalated outside of the organization.

Essentially the higher the line of support the more knowledge and experience they should have on the specific service in question, the less general knowledge they will have across all services.

Responsible for:

- Investigating and diagnosing incidents escalated from the Support Center
- Developing workarounds
- Resolving and recovery of assigned incidents
- Creating incidents after detecting a service failure or quality degradation or a situation that may result in one
- Communicate status with customer

The IT Support Team is engaged in the process by changing the Assignment Group field to the support group in question and the Assigned to field to the individual support staff.

ServiceNow Role Required:

SMEs will require the **itil** role, or **sn_incident_read** and **sn_incident_write roles** introduced with Incident Management (com.snc.itsm.roles.incident_management) plugin.

Major Incident Manager

Unlike the change management process where each ticket needs to be reviewed in some manner by the process managers, incident management does not require this step. The Incident Manager is concerned entirely with major incidents. They are the coordinator responsible for getting a major incident resolved as soon as possible and ensuring that it does not reoccur.

Responsible for:

- Assigned to a major incident to co-ordinate the investigation and resolution
- Assigns tasks to other teams to investigate and resolve the major incident
- Manages communications during the major incident to both business and IT stakeholders
- Conducts a review of the major incident once resolved

The Major Incident Manager is engaged in the process by changing the Assignment group field to the Major Incident Management group and the Assigned to field to the correct Major Incident Manager.

ServiceNow Role Required:

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

Incident Admin

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The incident management process owner can configure certain elements of the incident process that do not require the System Admin to do so.

Responsible for:

- Configuring incident properties
- Configuring major incident trigger rules

ServiceNow Role Required:

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 role of the Process Owner is usually a senior manager with the ability and authority to ensure the process is rolled out and used by all stakeholders.

Responsible for:

- Defining the overall mission of the process
- Establishing and communicating the process mission, goals, and objectives to all stakeholders
- Documenting and maintaining the process and procedures
- Resolving any cross-functional (departmental) issues
- Ensuring proper staffing and training for execution
- Directing the Incident Management roles
- Ensuring consistent execution of the process across the organization
- Monitoring, measuring, and reporting on the effectiveness of the process to senior management
- Continually improving the process

ServiceNow Role Required:

The **business_stakeholder** role can be used for incident process management. This role will gain additional capabilities in future releases.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

How incidents are initiated

Directly in ServiceNow - The Support Center Agent can create the incident directly because 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 of the portal where they can directly create a ticket. This would use a record producer to generate an incident record rather than exposing the full incident form to users that would not understand most of it.

Automatically via Integrations - Incidents can be automatically generated via external systems such as event monitoring.

Support Chat (Future Implementation) - A Service Agent can generate incidents using chat conversations with a user. The chat log is included in the Incident Activity Log and a link to the Incident and the user is set.

Inbound Email - Inbound emails can generate incident records. ServiceNow does not recommend this method since it cannot reliably collect enough information from the email to create an incident that can be worked on.

Walk Up Experience - An incident can be created using the Walk-Up interface when a user visits the onsite IT support location

© 2022 ServiceNow, Inc. All rights reserved.

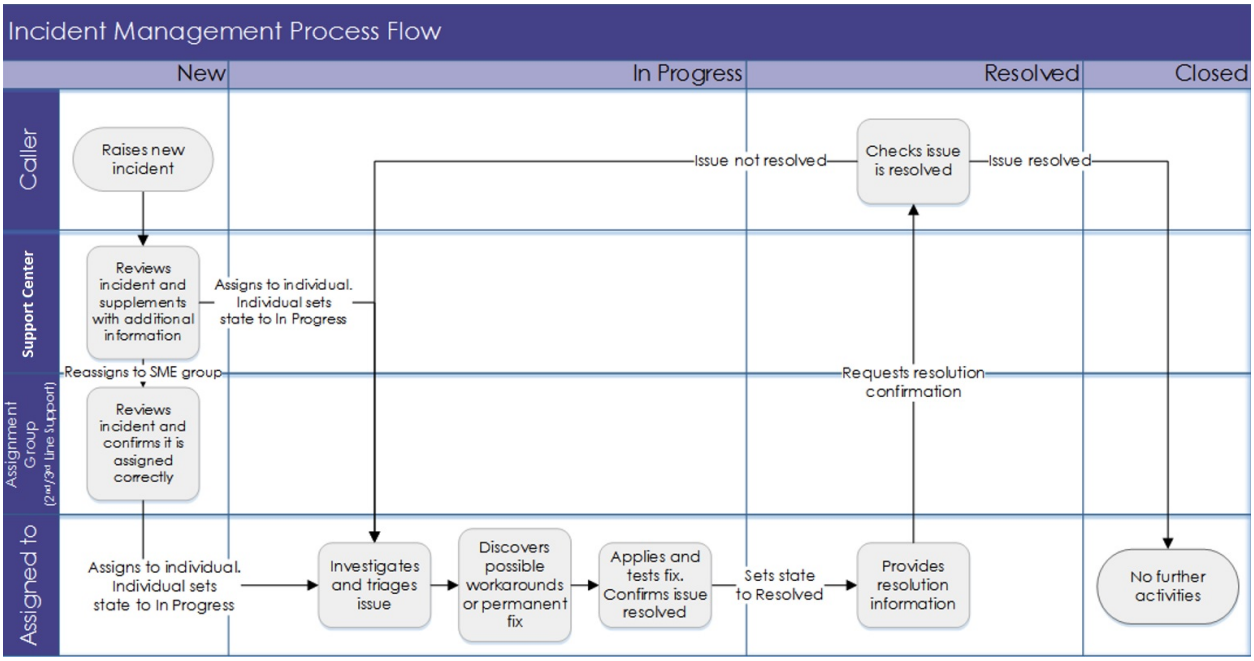
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Incident Management Lifecycle

States in any ServiceNow application serve a specific purpose. They are designed to make it clear where in a process a particular record currently resides and to display progress. States should represent a unique phase in a process where a specific set of related activities are grouped together designed to achieve a particular outcome to move to the next phase of the process. For example, in Incident Management the Resolved state should contain all activities required to understand what was done to resolve the incident. It would not be expected that resolution explanation activities would occur during other states. Out-of-the-box, Incident Management has the following state model:

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

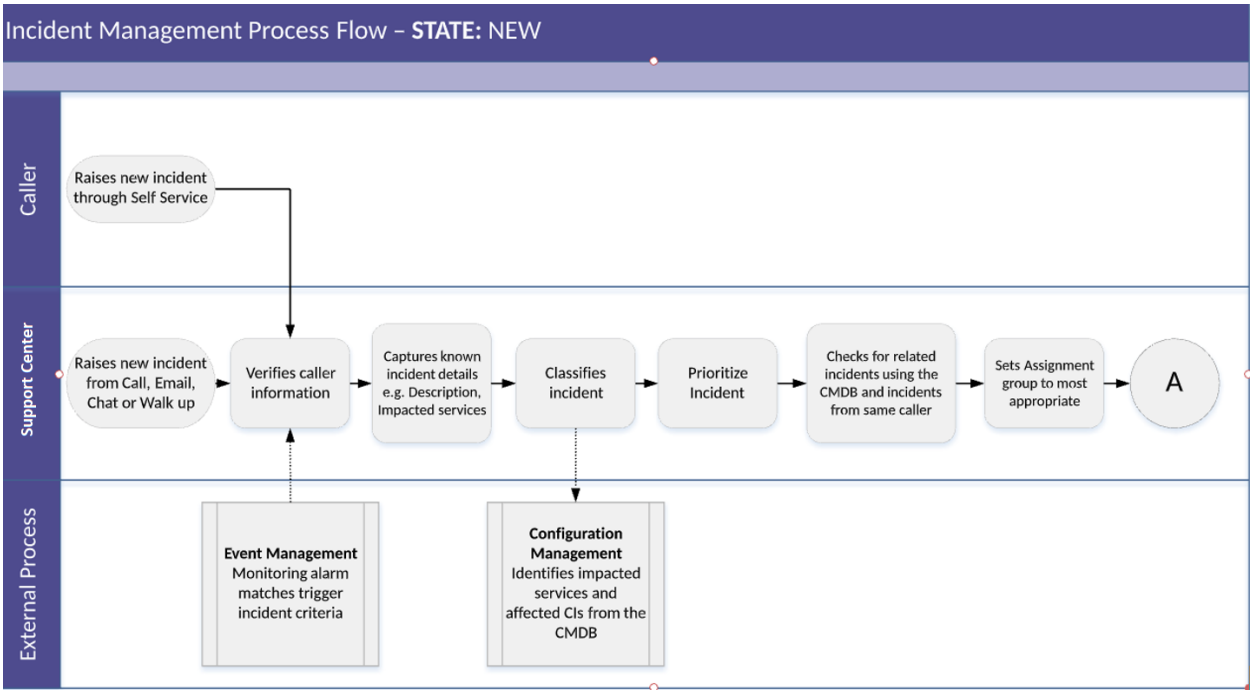
Process Overview



© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State: New



When an incident is first created, it is in a state of New. This is where the incident ticket is opened and all known information about the symptoms experienced is captured. Capturing sufficient and relevant details 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. It will be automatically assigned to the Support Center as the front line to review anything coming into the IT department for action.

The recommended mandatory fields are:

- Caller
- Service
- Configuration item
- Service Offering
- Contact type
- Impact
- Urgency
- Priority – this is automatically populated from the Impact + Urgency fields
- Assignment group
- Short description
- Description

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If the incident is raised through self-service or email it would only be expected for the end user to provide limited details:

- Caller
- Urgency
- Short description
- Description

Most of the remaining fields would not be known or understood by the end user. At this point, the Support Center Agent will review the information that has been provided and supplement it with further details.

Process Critical Attributes

There are several attributes captured in an incident that drive aspects of the process.

Establishing Priority

Incident prioritization typically drives the timeframe associated with the handling of the incident and the time to resolution. This will impact the Service Level Agreements that are associated with the incident. Priority is calculated through a combination of Impact and Urgency. Process owners will need to be clear on how they define the different levels of impact, urgency and the response/restoration timeframes associated with the resulting priorities. This will be used to define SLAs and ensure consistency across the process.

Impact is the affect that an incident has on business. For example, if the incident only impacts a single employee the impact is low in comparison to 500,000 paying customers with social media accounts.

Impact Ratings:

Category	Description
1 – High (H)	Statewide or multiple agencies affected, Entire agency.
2- Medium (M)	A work area, site, division, or unit is affected
3 – Low (L)	An individual is affected.

Urgency is the extent to which the incident's resolution can bear delay.

Urgency Ratings:

Category	Description
1 – High (H)	Service is down (no workaround/work stoppage).
2- Medium (M)	Service is degraded (work impaired/workaround/able to complete task).
3 – Low (L)	Non-vital Service is down or degraded (no workaround/work stoppage).

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

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

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

Target Response and Resolution Times

Priority	Description	Target Response Time*	Target Resolution Time
1	Critical	Immediate or less than 15 minutes	Less than 4 hours
2	High	Immediate or less than 15 minutes	Less than 8 hours
3	Moderate	4 Hours or less	2 business days
4	Low	1 business day	1 week

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. For example, an online banking service would be considered critical to a financial organization. If this CI is related to the incident the priority can be automatically set to Critical as a result. This ensures a more accurate and consistent prioritization of incidents, as the determination of impact and urgency can be a subjective call.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Categories/Business Services & CIs

The Category field is intended to be used to identify what is being impacted by the incident; however, it is only recommended to be used where the CMDB (Configuration Management Databases) is not yet in use or is extremely immature.

The CMDB (CI fields) is also used to identify what is being impacted by the incident. It offers significantly enhanced data than what could be made available in a choice list. The Category field should be replaced by the Business service and Configuration item field/related lists to maximize the benefits of the platform and to allow better interaction across the various ITSM processes. Business Service CI is available across all ITSM processes and therefore it must be related to an incident to provide true insight into the performance and health of the service. By using categories, the data is limited to the incident management process only and does not provide value beyond that.

Incident Assignment

The Support Center Agent may already be aware of the correct group to assign the incident to and at this point would reassign it to that group. If automated assignment is in place this will also occur here usually once the Business service or CI are populated. The new assignment group will review the incident that arrived in their work list and assign it to an individual to focus on. Once that individual begins working on the incident, they will manually set to the state field to In Progress. This will then stop the clock on any response SLAs that may be running as this is responding.

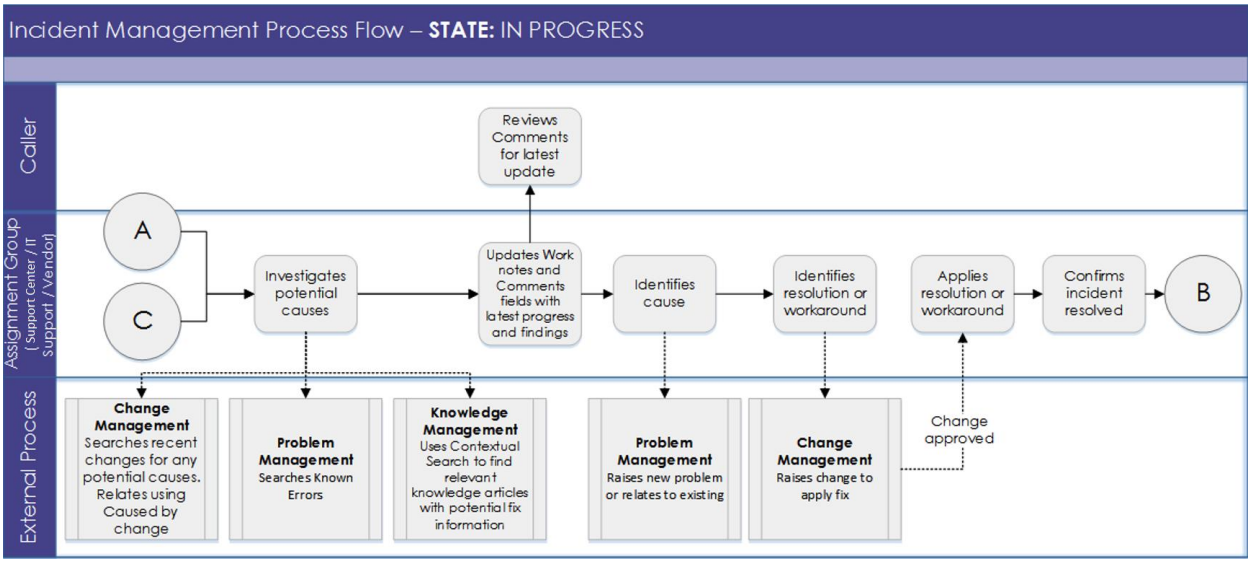
Alternatively, the Agent may need to begin some investigation and triage. At this point, they will assign the incident to themselves using the Assigned to field and set the state field to In Progress.

It is mandatory to assign an individual to the incident for it to move to In Progress. This is so that anyone wanting to get an update/discuss the issue will know who is responsible for it.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State: In Progress



The incident is now actively being worked on. In Progress state covers many different activities that are required to resolve the issue. This will begin with investigation and triaging by the Assigned-to individual to establish what the cause might be and/or how to fix it. It is possible to use the Contextual Search feature to display knowledge articles within the incident that match or are like the Short description entered. This allows the Assigned to individual to easily locate any published information that may provide them with help in resolving the issue. They may also refer to similar incidents and problem records.

The individual may subsequently reassign the incident to another assignment group or individual if they discover that there is a better-suited group/individual to deal with the issue. This is done by updating the Assignment group and Assigned to fields and may involve passing the incident to 2nd or 3rd line subject matter experts. An email notification will be sent to the new assignees to make them aware they are now responsible.

It is possible for the incident to be reassigned multiple times while it is In Progress as different teams may need to be involved. When reassigning an incident, it is mandatory to enter a Work note to explain why the incident is being assigned to the new group or individual and what is expected of them. Reassigning an incident will not reset SLAs attached to the incident unless the SLA is specifically tracking reassignment only. Therefore, if an SLA only has 1 hour remaining before it will breach and is then reassigned the new team will still only have 1 hour before the SLA will breach.

Throughout this time the Work notes field is used to make journal style updates to the incident capturing what actions have been taken and what has been learnt. If an update needs to be provided to the original caller this can be done using the Additional Comments field.

When a fix is identified by the investigation, the assigned to individual will apply the fix to resolve the issue. This may be in the form of a workaround rather than a permanent solution. A change request is raised to apply the fix, and this is related to the incident in the Change Request field. If the incident is purely waiting for the change to be implemented and no other activities are

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

occurring, the State field can be changed to On Hold with an On Hold reason of Awaiting Change.

During investigation, it may be discovered that a change was the cause of the issue. If this is the case, the change in question can be related to the incident using the Caused by Change field.

Once the fix or workaround is applied, the Assigned to individual will test to see if the issue is resolved. If they believe it is, they will change the state field to Resolved or click the Resolve button.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State: On Hold

The On Hold state is used to indicate where an incident is not yet resolved but is temporarily not being worked while waiting for further action to occur outside of the control of the Assigned to individual.

There is a separate On Hold reason field to determine why the incident is on hold. This is a choice list so that process owners can only include those reasons which they determine legitimate for pausing an incident therefore guiding the users of the process to follow it correctly.

The incident is put into On Hold state by changing the State field. The On Hold reason field becomes mandatory at this point with the following choices:

- Awaiting Caller
- Awaiting Change
- ~~Awaiting Problem~~ (do not use)
- Awaiting Vendor

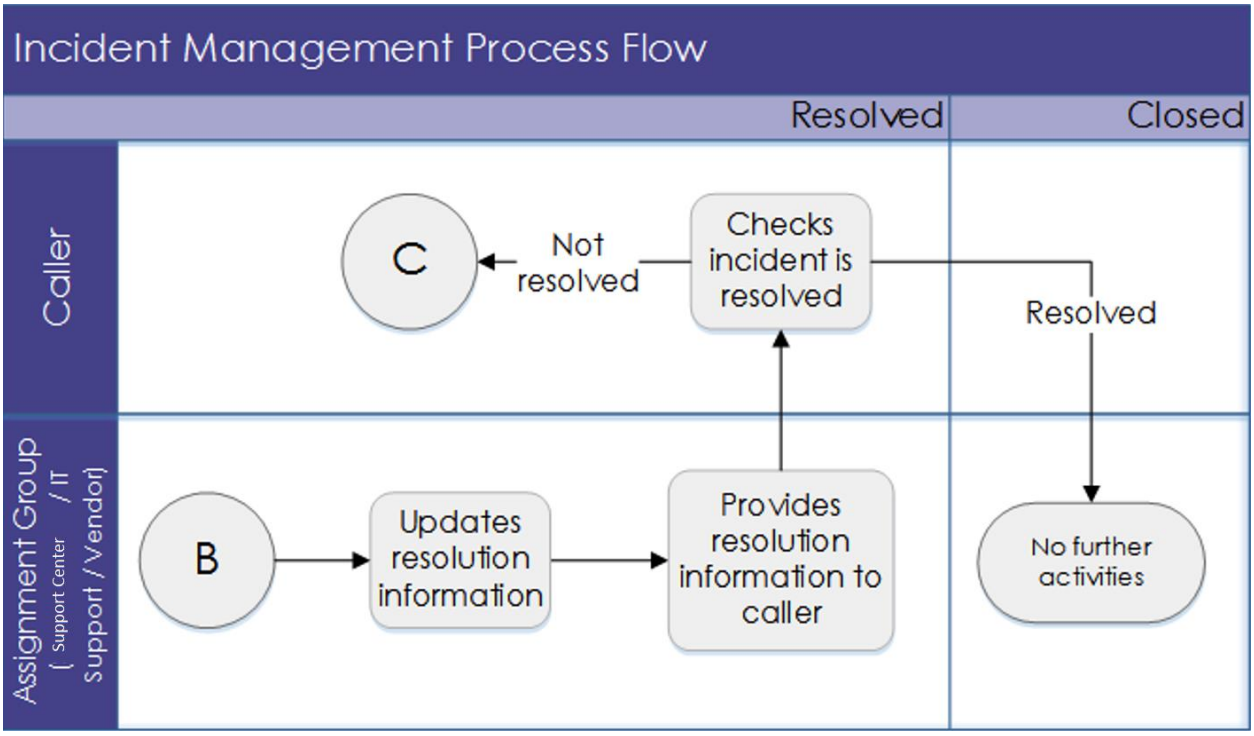
ServiceNow recommends removing Awaiting Problem from the choices. Resolving an incident should never be dependent on a problem.

The Service Level Management product will make heavy use of this state since putting something on hold (Awaiting Caller) will typically act as the pause condition for all SLAs.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State: Resolved



To move the State to Resolved, the Assigned to individual will need to give some further details to explain what the problem was and how it was fixed. The mandatory fields are:

- Resolution code
- Resolution notes

The Resolution codes field is a choice list focused on the nature of the resolution provided, for example, whether a workaround was provided or a permanent fix. They are not intended to explain how the incident was resolved.

Resolution notes is a free text field intended to describe what the issue was and how it was resolved. This is deliberately not held as a category or choice list solution. Experience shows that there tends to be many possible codes. These would have to be filtered based on the CI related to the incident. If this filter was not applied, then the resolver would have so many options the choices would be overwhelming, and the chance of correct data being selected becomes significantly reduced resulting in the data no longer offering value.

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.

Requiring codes to track what the issue was and how it was fixed should only be done where there is a clear business benefit to be achieved.

Once the resolution information is provided the Caller is notified that the Assigned to individual believes they have resolved the issue.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Caller has 7 days to disagree with this. They will be sent an email notification to advise them which provides a link back to the incident if they disagree. In the incident they will click the Reopen Incident button which will require them to enter an Additional comment explaining why they believe the incident is not yet resolved. This will set the State field back to In Progress and clear the Resolution code and notes. The Assigned to individual will receive a notification containing the Additional comments from the Caller.

If the Caller does not contest the resolution, they do not need to take any action. The incident will remain as Resolved for 7 days. After that time, the State field is automatically updated to Closed.

State: Closed

No activities take place at this state. Should the incident reoccur a new Incident record must be raised. Once an incident is closed, it cannot be reopened.

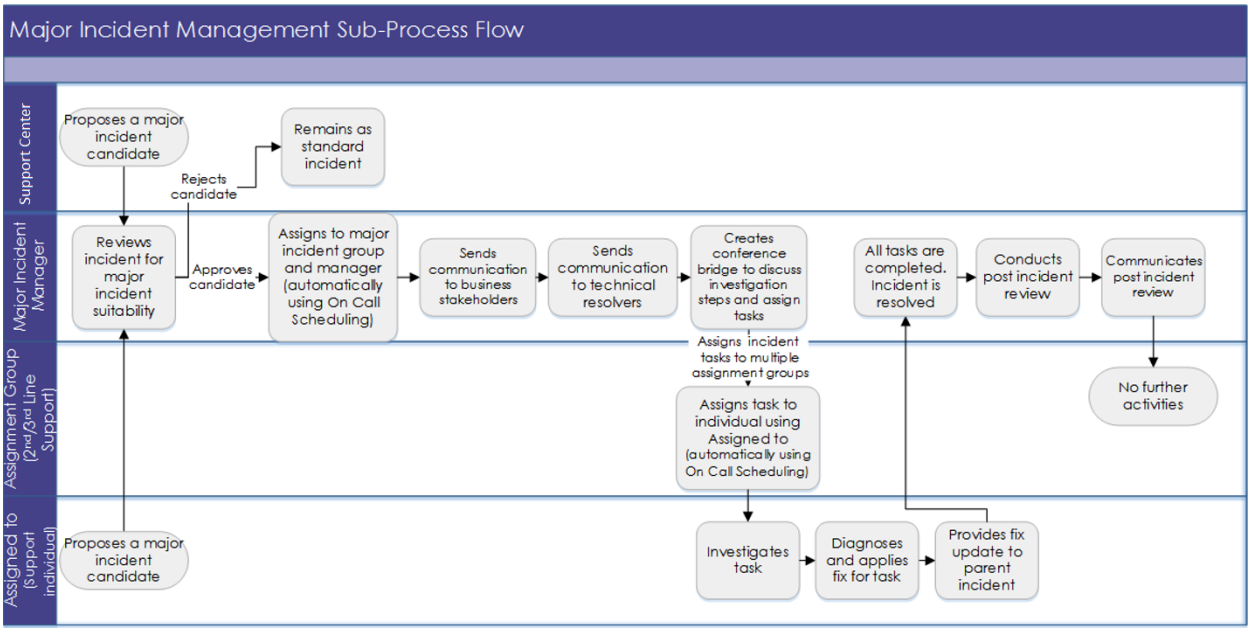
State: Canceled

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

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Major Incident Management



Major incidents are managed as a sub process occurring within Incident Management where the impact of the incident is considered to have a particularly strong impact on the business such that additional activities must be undertaken to ensure the impact is reduced or removed as quickly as possible.

Major incidents are coordinated by a single individual (Incident Manager) who will manage the situation through to resolution. The Incident Manager can use incident tasks to allow multiple support groups and users to work on the resolution concurrently. Incident Managers use the Major Incident Workbench to communicate regular updates on the progress of the incident through the lifecycle. When the incident has been resolved, the Incident Manager can conduct a review of the incident and any follow-up activities.

Incident Candidates

Users of the incident process may consider a particular incident to require the major process however they cannot automatically promote an incident into this process since it will trigger several actions and activities in other teams that they may not be aware of. Incidents are initially proposed as a Major Incident Candidate so that Incident Managers can confirm this process should be followed. There are 3 possible ways to do this:

1. Automatically via predefined trigger criteria
2. Manually from an existing incident
3. Manually where no incident currently exists

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Trigger Criteria

Major incident candidates can be automatically proposed based on pre-defined criteria. When these criteria are met, the incident is immediately proposed as a candidate.

Users can manually propose a candidate from an existing incident by selecting the Propose Major Incident choice in the context menu. If an incident does not already exist, a candidate can be proposed directly from the left navigation menu using the Create Major Incident Candidate option.

Major Incident Managers can create a major incident without the need for a candidate by using the Create Major Incident link in the left navigation menu.

Once the candidate is proposed this allows a new form section called Major Incident to be displayed on the incident record.

This section includes additional fields related to major incidents. The user proposing the candidate should now populate the Business impact and Probable cause if they have any information relating to these subjects.

All proposed candidates are now reviewed by an Incident Manager. They can be accepted or rejected by choosing the relevant option in the context menu. Once the candidate is promoted to a major incident, the Major incident state field is automatically updated to Accepted and the Assignment group field is changed to the Major Incident Management group if it was previously empty. It is expected that the Major Incident Manager reviewing the candidate would manually reassign it to the correct incident management group if it were previously assigned.

During the major incident, the Major Incident Manager can log specific actions taken in the main incident record by entering notes into the Actions taken journal field. This allows these notes to be identified independently of any general notes that were added.

Incident Tasks

The incident will now remain assigned to the Major Incident Management group for the remainder of the lifecycle. The Major Incident Manager will need to designate actions and activities to other groups and individuals as part of the process of investigating and resolving the incident. This is achieved by creating individual incident tasks from the Incident Tasks related list only available on 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 is primarily used to coordinate communication activities.

Incident Communications

The Communication tab within the Workbench has a set of predefined communications tasks to be carried out. These tasks use the Incident Communication feature and are created as the task is initiated from the Workbench. The Incident Manager will need to populate the content of the task and assign it to the relevant individual for action.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the tasks are closed this is reflected in the Workbench.

Conference Calls

The Conference tab is only displayed if the Notify plugin has been purchased and enabled. Conference calls can be directly initiated from this tab.

On-Call Scheduling

On-call scheduling provides a way to determine which member of a user group is available to complete a task. For example, to find the right person to assign an incident.

On-call scheduling also helps you to determine who is the current primary contact for a task, and to escalate notifications for a group.

Major Incident Reviews

Once the major incident has been resolved, the Incident Manager will review what happened. This usually involves understanding the root cause and concluding whether any steps can be taken to avoid the situation reoccurring. Lessons learned can be captured here. The review is conducted when the incident is in Resolved state. If the review is comprehensive, incident tasks can be created and assigned. Once the review is complete, the incident can be closed.

Managing all Major Incidents

Major Incident Managers can keep track of all major incidents through using the Major Incident Overview dashboard.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Parent and Child Incidents

Where an incident is causing a widespread impact, this will be evident with several records being raised by different Callers for the same issue. Although these incidents are reporting the same thing and might be considered duplicates of each other it is good to capture each instance where the impact has been experienced so that the size of impact can be more easily determined.

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

Handling Ad Hoc Questions/Help

Where a caller has an ad hoc question or request for help that does not involve an issue this may be captured using the Interaction feature. This allows the question to be handled without having to log an incident or create a service request for the purpose.

It is not recommended to create a catalog item in the Service Catalog for this purpose since the structure of requests, requested items and catalog tasks is over complex for this need. If the process owner does not wish to use the Interaction feature, an incident record is used to capture this interaction. If the Category field is in use the Inquiry / Help choice should be selected to distinguish this from a true incident. If the Category field is not in use a new field will be required to determine this.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Other Processes

Change Management

For many incidents, the solution will require work on a service, hardware, or software. Conducting this work will require a change record to be raised. This is done by selecting the Create Normal Change or Create Emergency Change option in the context menu.

Emergency changes typically require an incident record to be related to prove that they are urgent enough to bypass the full process and lead times. This can also be done from the change record by 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 link the chain of events together. This can be done using the Incidents Caused by Change related list.

Problem Management

Problem Management is the subsequent process for incidents that require further investigation of the root cause. Problem records can be generated directly from the incident record and will copy over key data. This is done using the Create Problem option in the context menu.

There could be many incidents associated with a single problem and the higher the number of incidents the clearer the scale of impact becomes. It may be that when the problem was first encountered the number of associated incidents was low and so it was decided not to pursue a permanent fix. However, as the number increases and the impact widens that decision may be reviewed. Multiple incidents can be added to the problem using the Incidents related list.

If a workaround exists for the problem this can be logged into the problem record in the Workaround field and automatically pushed into all associated incident records using the Communicate Workaround related link.

Once the problem has been 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, but also contains details of the infrastructure vital to efficient call handling.

The CMDB is used within the incident management process by relating Configuration Items including Business Services to the incident. This allows Dependency Views to be used which 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 is available using the Contextual Search feature embedded into the incident record and record producers to display relevant knowledge articles as the incident is being created. Contextual Search will use text entered in the Short description fields or other text fields to search for close matches in the knowledge base and display these on the screen.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Service Level Management

Service Level Management defines measurable responses to service disruptions. Incident Management will provide historical data that enables the review of service level agreements (SLAs) objectively and regularly. SLM defines the acceptable levels of service within which Incident Management works, including:

- Incident response times
- Impact definitions
- Target fix times
- Service definitions
- Rules for requesting services

User Experience

Mobile platforms and Virtual technology can have a positive impact on how end users interact with the end-to-end process and ultimately how the entire user experience is perceived. Consider which touchpoint in the process can leverage the mobile platform to minimize delays in the process. Tasks such as Create an incident, Details of incident, Chat can all be performed on mobile devices. Consider also how Virtual Agent can be deployed to assist users in common actions and tracking progress.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Process Governance

Measurement

Key Performance Indicators (KPIs) evaluate the success of a particular activity toward meeting the critical success factors. Successfully managing KPIs can be either through repeatedly meeting an objective (maintain) or by making progress toward an objective (increase/decrease). The Benchmarks feature gives you instant visibility into your key performance indicators (KPIs) and trends, as well as comparative insight relative to industry averages of your peers. You can contrast the performance of your organization with recognized industry standards and view a side-by-side comparison of performance with global benchmarks. Benchmark 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

- Provide information on the effectiveness of the process and the impact of continuous improvement efforts
- Are best represented as trend lines and tracked over time
- Monitored by the Process Owner

Item	Purpose
Reassignment count	Count of the total number of times the Assignment Group field is changed to understand how quick/easy it is for the incident to get to the right group for resolution
Resolved on first assignment	% Of incidents resolved by the first line or first person to be assigned to the ticket. This helps to understand how well the Support Center can handle incidents without reassigning to a more costly resource to resolve
Resolved within SLA/OLA	% Of incidents resolved within SLA/OLA helps to understand whether the SLA/OLA are unachievable and need a review or whether there is an issue with operational practices

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

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 Support Center and Incident Management team.

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 a quick view of incidents that need immediate attention to prevent further degradation of resolution time.
List of incidents reactivated from caller feedback	Provides a quick view of incidents that need immediate attention to meet resolution target and customer satisfaction.

Reports and Homepages

There are numerous default reports available in ServiceNow that can be used to generate charts, be published to a URL, or can be scheduled to be run and distributed at regular intervals. Users 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 records that exist in ServiceNow tables.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Appendix A: RACI Matrix

Roles are responsible for performing specific process activities. A RACI diagram visually indicates these responsibilities. The following guidelines are used in defining the RACI model for each process step throughout the document.

- **Responsible (R)** = The person responsible for the task or deliverable.
- **Accountable (A)** = The person accountable and makes the final decision and has ultimate ownership.
- **Consulted (C)** = The person/persons who must be consulted and provide guidance before a decision is made or action is taken.
- **Informed (I)** = The person/persons who must be informed on decisions that have been made or actions taken; they may be dependent on outcomes and must be kept updated on progress.

Phase	Deliverable/Task	Incident Reporter	Support Center	Incident Process Manager	Incident Response Technician(s)	Incident or Service Owners
Incident Identification	Detect/discover incident.	**R/A**	**I**		**I/R**	
	Event monitoring/auto-generates ticket.		**I**		**I**	**I**
Incident Logging	Record incident	**R**	**R**	**I**	**R**	**A**
	Document incident information.		**R/A**	**I**	**I/R**	
	Document steps to reproduce incident.	**R**	**R**	**I**	**R/A**	
	Document incident reporter information.	**R**	**R/A**	**I**	**I**	
	Create summary description of incident.	**R**	**R/A**	**I**	**I**	
	Unique identifier – case number assigned.	**I**	**I**	**I**	**I**	**I**
Incident Categorization & Prioritization	Incident Classification	**C**	**R**	**C**	**I/R**	**A/C**
	Initial Support & Diagnosis.		**R/A**	**I**	**R**	**I**

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

	Validate incident meets criteria (for an incident and priority).		**R**		**I/R**	**A**
	Assign or reassign incident priority.		**R/A**		**R**	**I/C**
	Assign incident.		**R/A**		**I/R**	**R**
	Incident Response, draft communications for Service Alerts.				**C/I**	**R/A**
Phase	**Deliverable/Task**	**Incident Reporter**	**Support Center**	**Incident Process Manager**	**Incident Response Technician(s)**	**Incident or Service Owners**
Incident Categorization & Prioritization	Send and post Service Alert.		**R**	**I**	**I/C**	**R/A**
Escalation	Reserve room for incident command center, if needed.				**I**	**R/A**
	Identify resources - people, equipment, technology, information.				**R**	**R/A**
	Make staff resources available and/or joining staff to the existing Critical & Major Incident TEAMS channel				**I/C**	**R/A**
	Coordinate resources.				**I**	**R/A**
	Obtain additional information to assist diagnosing and resolving incident.				**R**	**A**
	Incident kickoff meeting.			**I**	**R**	**R/A**
	Communicate incident priority.		**I**		**I/R**	**R/A**
	Reinforce urgency and priority.	**I**	**I**		**R**	**R/A**
	Manage internal communication.		**I**		**C**	**R/A**
	Manage external communication, by		**I**		**C**	**R/A**

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

	updating Service Alerts regularly.					
	Provide customer (incident reporter or business owner) communication and status.		**I/A**		**C**	**R/A**
Investigation & Diagnosis	Develop Action Plan.				**R/A**	**I/C**
	Lead and facilitate cross-team investigation and diagnosis.				**R**	**R/A**
	Monitor progress towards service restoration.			**I**	**R**	**I/A**
Phase	**Deliverable/Task**	**Incident Reporter**	**Support Center**	**Incident Process Manager**	**Incident Response Technician(s)**	**Incident or Service Owners**
Investigation & Diagnosis	Reconvene incident response team as needed.				**C**	**R/A**
	Investigate technology, processes, data and any changes.			**I**	**R/A**	**I**
	Perform analysis to determine level of effort to address incident.			**I**	**R/A**	**I**
	Provide data, information, analysis, and ideas.				**R/A**	**C**
	Analyze and diagnose to determine problem and resolution.				**R/A**	**I**
	Perform steps to reproduce incident.			**I**	**R/A**	
	Remove barriers that inhibit diagnosis and service restoration.				**I**	**R/A**
Resolution & Recovery	Identify and test possible solution, or work-around if needed.				**R**	**A**

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

	Coordinate with Change Management to implement solution.				**R**	**A**
	Deploy solution to restore service; confirm recovery; validate service restored.		**I**		**R**	**A**
	Document trouble-shooting steps and resolution.				**R**	**A**
Incident Closure	Review case - ensure correct category, priority, closure date, and other critical information.				**R**	**A**
	Communicate: Service restored Service Alert & Gov Delivery, notify customers of ticket closure.		**R**		**R**	**A/R**
Phase	**Deliverable/Task**	**Incident Reporter**	**Support Center**	**Incident Process Manager**	**Incident Response Technician(s)**	**Incident or Service Owners**
Incident Closure	Determine reason for outage, update Alert on support website.		**R/I**		**R**	**A**
	Retrospective and Root Cause Analysis.				**R**	**R/A**
	Reopen ticket if incident reoccurs.	**R**	**R**	**I**	**R**	**A**

Appendix B: Roles and Responsibilities

ROLE	STEPS
SUPPORT CENTER, SERVICE OWNER, TECHNICIANS	1. **Major Incident Identification** a. Following urgency and impact assessment, the incident is given a Priority 1, 2, or 3. Incident assessment and priority is validated.
TECHNICIANS, INCIDENT PROCESS MANAGER, SERVICE OWNER,	2. **Escalation** a. **Notification**– initial notifications (Service Alert) will be sent to appropriate managers, support teams including Support Center,

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TECHNICAL LEADS, SUPPORT CENTER	and customers. This will include all essential information to keep others informed and begin resolution. b. **Engagement** – All appropriate roles will be engaged immediately, including: i. Vendors (if applicable). ii. WaTech Communications (if it has the possibility of generating calls to the Governor from constituents or generating media attention). c. **Major Incident Command Room** will be established in a conference room or via Skype. d. **Priority 1, 2, or 3** is confirmed – confirm urgency, business impact, and target resolution. e. **Status and informational** updates will be sent to internal management and business owners as information is available. f. **Service Alerts** will provide customers with vital information. These will be sent and posted on the WaTech Support site. Updates to the site should be timely and a 'service restored' should be sent as soon as possible. [Refer to Service Alert process for additional process and expectations details].
SERVICE OWNER TECHNICIANS	3. **Investigation & Diagnosis** a. Facilitate technicians problem-solving. b. Review incident information. c. Perform analysis to identify the problem. d. Provide appropriate relevant information to assist team analysis (e.g. diagrams, data, environment, information, changes). e. Develop Action Plan for diagnosing problem and restoring service. f. Follow through with all action items.
SERVICE OWNER TECHNICIANS SUPPORT CENTER	**4. Resolution & Recovery** a. Develop next steps in Action Plan for restoring service. b. Identify a work-around where necessary. c. Identify a root cause when possible up front. d. Test and validate the fix. e. Deploy solution. f. Restore service. g. Validate restoration. h. Confirm with customer(s) that service is restored. i. Document trouble-shooting steps and resolution.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TECHNICIANS **SERVICE OWNER** **SUPPORT CENTER**	**5. Closure** a. Review ticket to ensure correct service, category, priority, and other critical information is documented. b. Notify customers of ticket closure. c. Update RFO on service alert post to support.watech.wa.gov. d. Final communications – customers, internal management, and business owners as needed. e. Close ticket - set an accurate closure date/time for incident end. f. Assess resolution for knowledge base article. g. Add knowledge base article. h. If further resolution is needed, ensure it will be managed by the appropriate technical team.
SERVICE OWNER **TECHNICIANS**	**6. Conduct Root Cause Analysis** activity, if root cause was not identified in the process of restoring service.

© 2022 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.