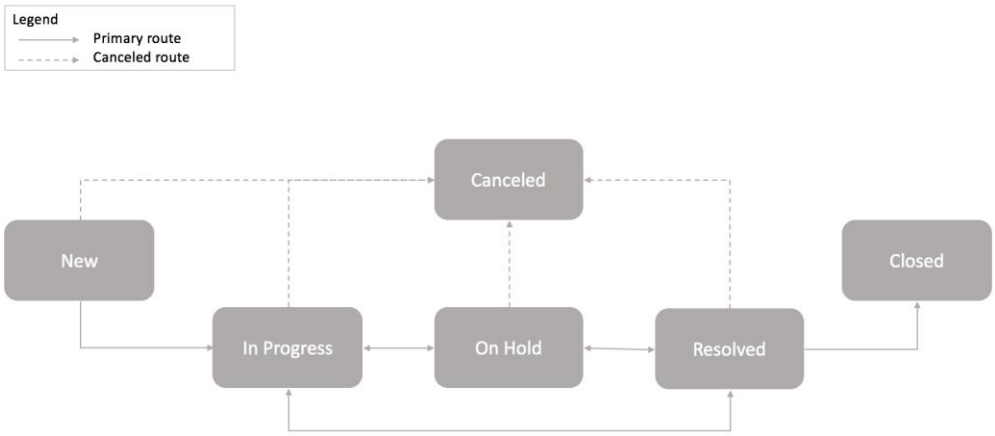
Life cycle of an Incident

Incident Management is responsible for managing the life cycle of incidents, from creation to closure.

The Incident Management process has many states, and each is vitally important to the success of the process and the quality of service delivered. The different states can be represented in a diagram as follows:



Incident states

State	Description
New	Incident is logged but not yet triaged.
In progress	Incident is assigned and is being investigated.
On Hold	The responsibility for the incident shifts temporarily to another entity to provide further information, evidence, or a resolution. When you select the **On Hold** option, the **On hold reason** choice list appears. If the **On hold reason** is **Awaiting Caller**, the **Additional comments** becomes mandatory. **Note:** If the caller updates the incident, the **On hold reason** field is cleared and the state of the incident is changed to **In Progress**. An email notification is sent to the user in the **Assigned to** field as well as to the users in the **Watch list**. An incident can be placed in the **On hold** state one or more times prior to being closed.
Resolved	A satisfactory fix is provided for the incident to ensure that it does not occur again.
Closed	Incident is marked **Closed** after it is in the **Resolved** state for a specific duration and it is confirmed that the incident is satisfactorily resolved.
Canceled	Incident was triaged but found to be a duplicate incident, an unnecessary incident, or not an incident at all.

Incident Management process

ServiceNow Incident Management supports the incident management process with the ability to identify and log incidents, classify and prioritize incidents, assign incidents to appropriate users or groups, escalate, resolve, and report incidents.

Any user can record an incident and track it until service is restored and the issue is resolved. Each incident is generated as a task record that contains pertinent information. Incidents can be assigned to appropriate service desk members, who resolve the task and document the investigation. After the incident is resolved, you can close the incident.

ServiceNow Incident Management supports the incident management process with the ability to identify and log incidents, classify and prioritize incidents, assign incidents to appropriate users or groups, escalate, resolve, and report incidents.

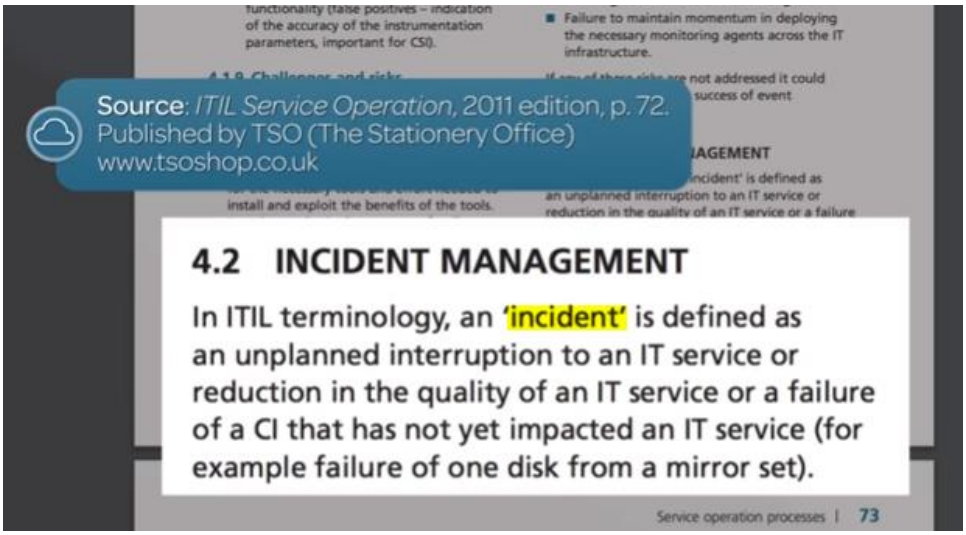
Any user can record an incident and track it until service is restored and the issue is resolved. Each incident is generated as a task record that contains pertinent information. Incidents can be assigned to appropriate service desk members, who resolve the task and document the investigation. After the incident is resolved, you can close the incident.

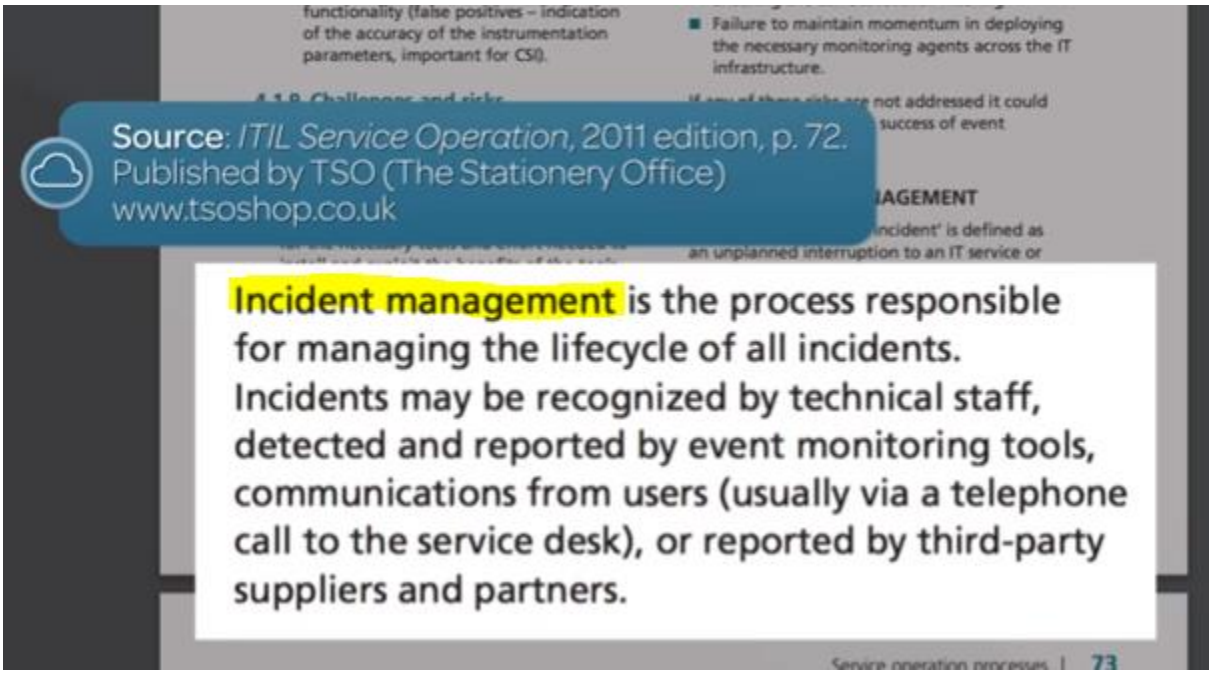
ServiceNow Incident Management process follows these steps:

1. Incident identification
2. Incident logging
    - Incident categorization
    - Incident prioritization
3. Incident response
    - Initial diagnosis
    - Incident escalation
    - Investigation and diagnosis
    - Resolution and recovery
    - Incident closure

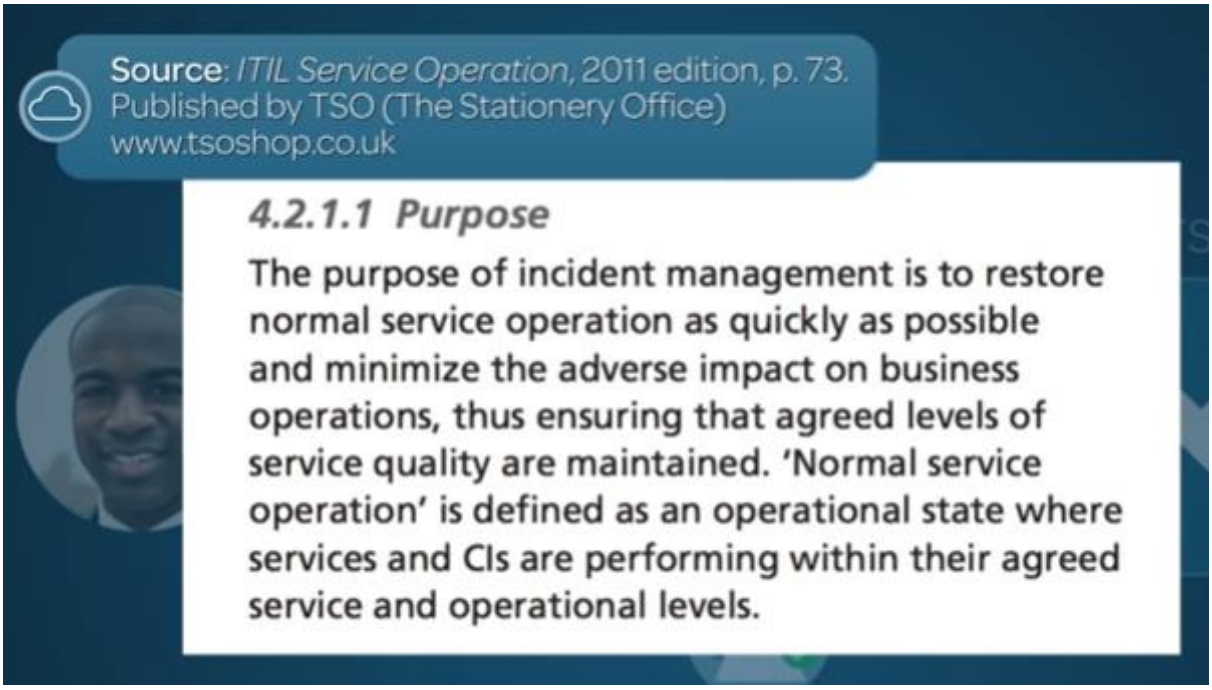

Users create incidents to report an interruption or reduction in the quality of an IT service, for example email.


Error
Incidents are also used to notify IT of local hardware or software issues...

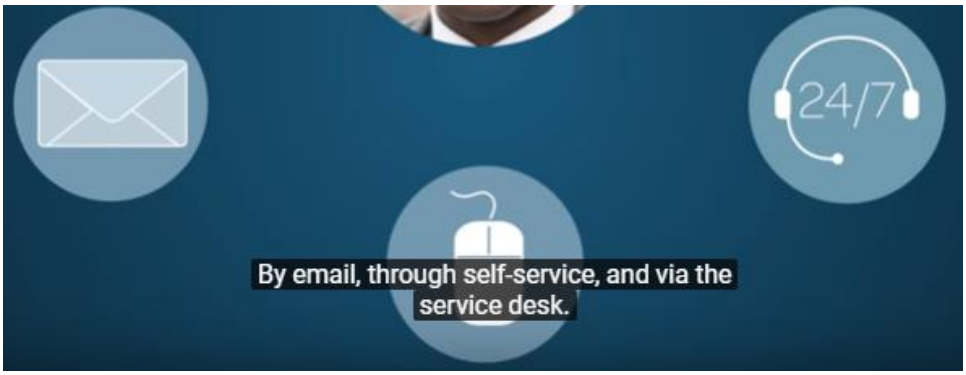

Source: ITIL Service Operation, 2011 edition, p. 72.
Published by TSO (The Stationery Office)
www.tsoshop.co.uk
4.2 INCIDENT MANAGEMENT
In ITIL terminology, an 'incident' is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a CI that has not yet impacted an IT service (for example failure of one disk from a mirror set).
Service operation processes | 73


Source: ITIL Service Operation, 2011 edition, p. 72.
Published by TSO (The Stationery Office)
www.tsoshop.co.uk
Incident management is the process responsible for managing the lifecycle of all incidents. Incidents may be recognized by technical staff, detected and reported by event monitoring tools, communications from users (usually via a telephone call to the service desk), or reported by third-party suppliers and partners.

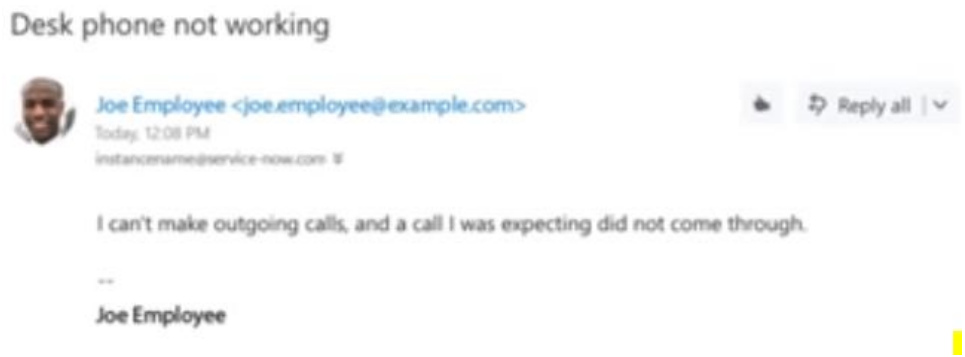

ITSM
Incident management is the IT service management,
or ITSM, process aimed at restoring normal service operation as quickly as possible...


Source: ITIL Service Operation, 2011 edition, p. 73.
Published by TSO (The Stationery Office)
www.tsoshop.co.uk
4.2.1.1 Purpose
The purpose of incident management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained. 'Normal service operation' is defined as an operational state where services and CIs are performing within their agreed service and operational levels.

There are several ways a user can report an incident. For example:



EMAIL:



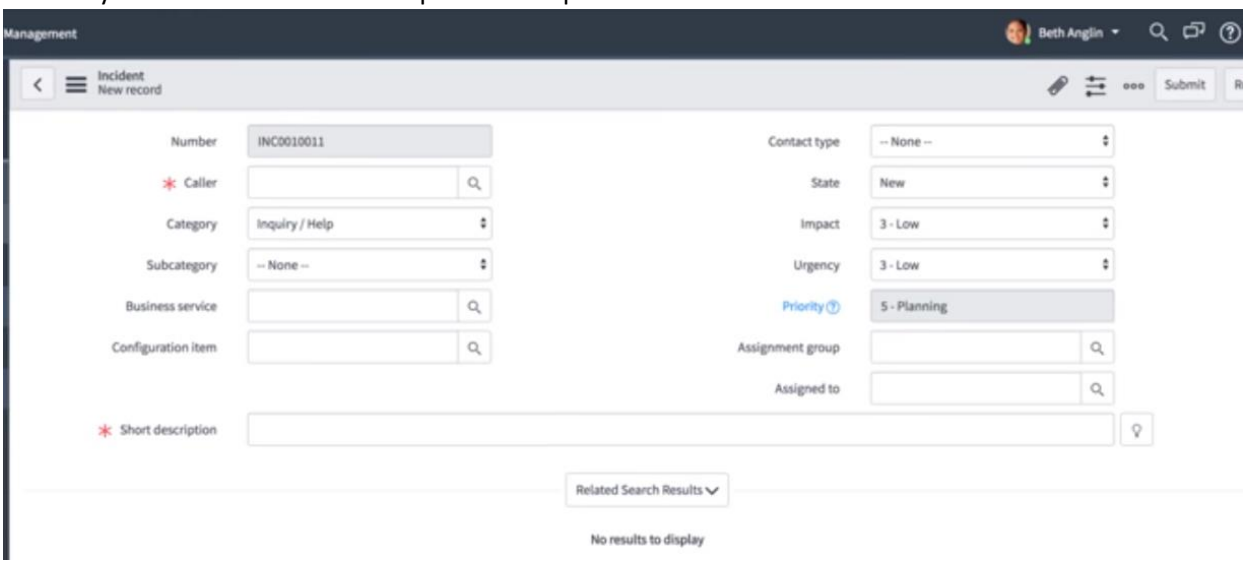
Users can create incidents by email, using the email address issued to their instance.

When users send an email message to the respective address, and incident record is automatically inserted into the system.

SELF-SERVICE:

Another way for users to create incidents is through the self-service homepage (ie, the Service Catalog).

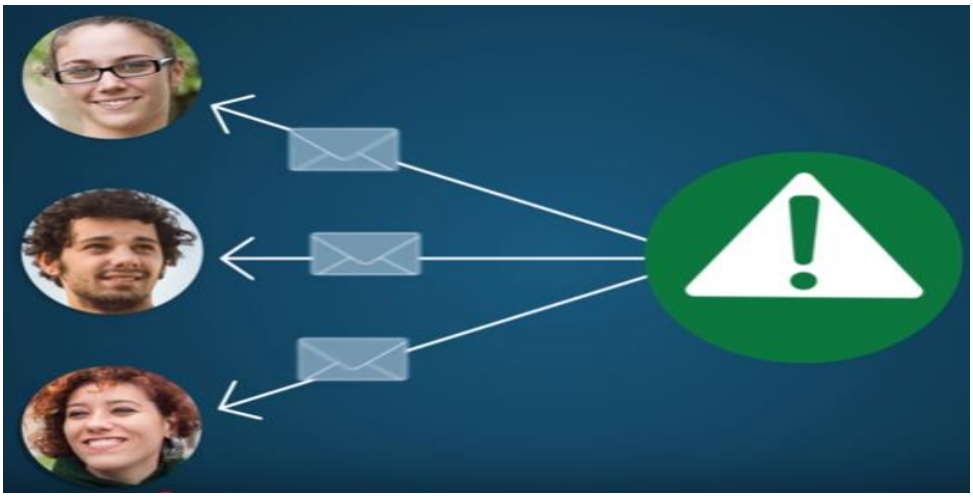
An IT Service Desk staff member or administrator can submit a new incident on behalf of the end user who may have contacted them via phone or in person:



After an incident is submitted, it is assigned to a Group and/or User based on Assignment Rules:

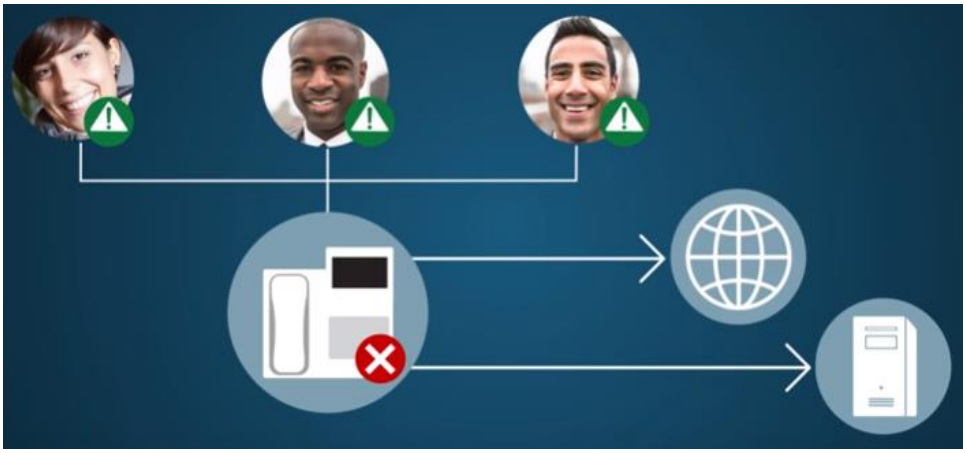
Proven practice is for incidents to be automatically assigned to groups, but not a user:

Notifications are sent to the Group Members if configured in the system:

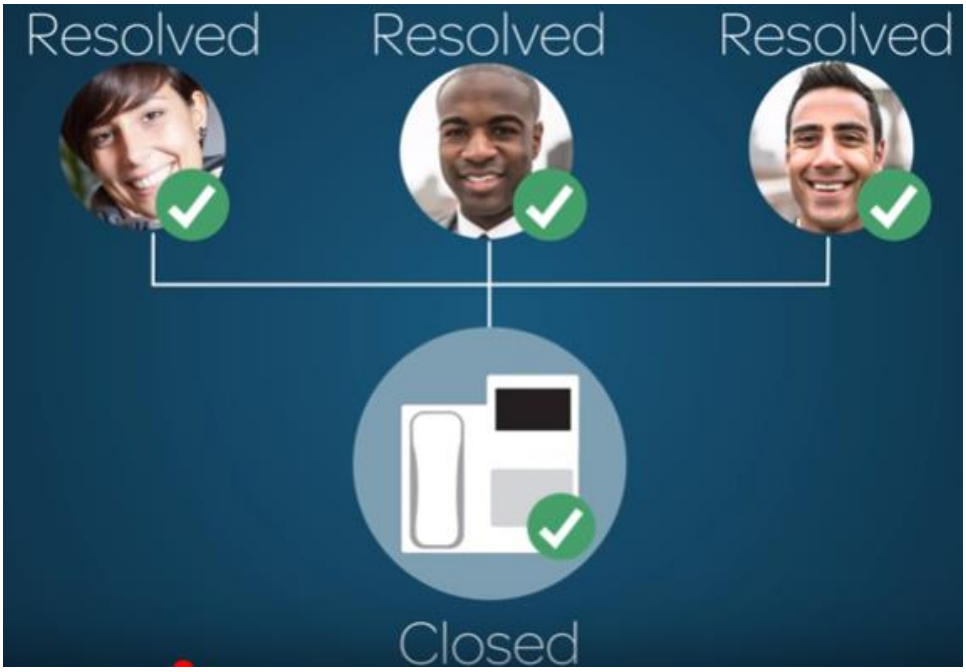


Depending on the ITSM process you've implemented, you might need to create a problem or change request related to the incident.

PROBLEM: For example, multiple report issues with desk phones:



...these incidents all point to the root cause, which could either be the network or IP phone server.



...when the problem is closed, all the related incidents are resolved.

CHANGE REQUEST: If the incident exposed a problem with the IT infrastructure that requires a change...

...you may need to create a Change Request:

...for example, the IP Phone Server might require a Software patch or a new Network card.