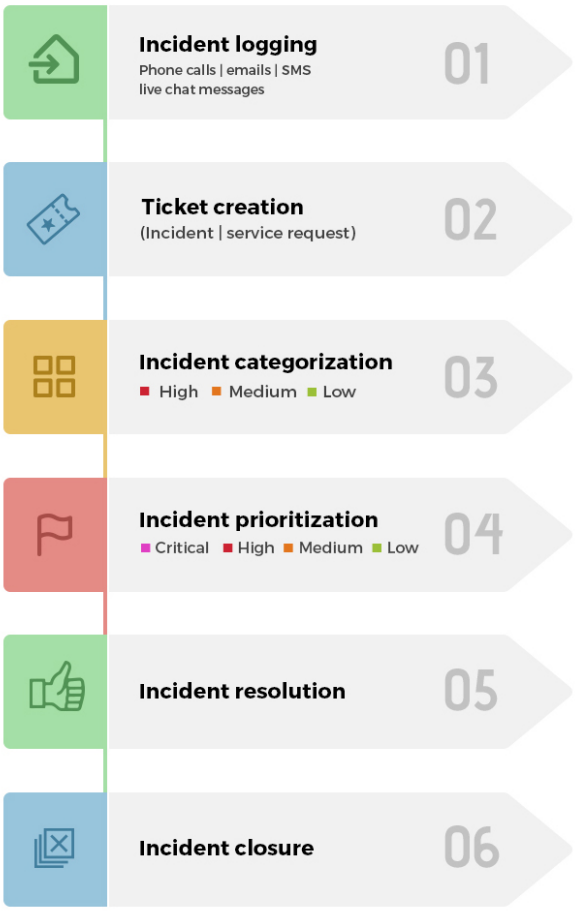
Incident management lifecycle 2021 2022

The incident management process can be summarized as follows:

- **Step 1 :** Incident logging.
- **Step 2 :** Incident categorization.
- **Step 3 :** Incident prioritization.
- **Step 4 :** Incident assignment.
- **Step 5 :** Task creation and management.
- **Step 6 :** SLA management and escalation.
- **Step 7 :** Incident resolution.
- **Step 8 :** Incident closure.



Incident management life cycle

These processes may be simple or complex based on the type of incident; they also may include several workflows and tasks in addition to the basic process described above.

- ### Incident logging

  An incident can be logged through phone calls, emails, SMS, web forms published on the self-service portal or via live chat messages.

- ### Incident categorization

  Incidents can be categorized and sub-categorized based on the area of IT or business that the incident causes a disruption in like network, hardware etc.

- ### Incident prioritization

  The priority of an incident can be determined as a function of its impact and urgency using a priority matrix. The impact of an incident denotes the degree of damage the issue will cause to the user or business. The urgency of an incident indicates the time within which the incident should be resolved. Based on the priority, incidents can be categorized as:

  - Critical
  - High
  - Medium
  - Low

- ### Incident routing and assignment

  Once the incident is categorized and prioritized, it gets automatically routed to a technician with the relevant expertise.

- ### Creating and managing tasks

  Based on the complexity of the incident, it can broke down into sub-activities or tasks. Tasks are typically created when an incident resolution requires the contribution of multiple technicians.

- **SLA management and escalation**

  While the incident is being processed, the technician needs to ensure the SLA is not breached. An SLA is the acceptable time within which an incident needs response (response SLA) or resolution (resolution SLA). SLAs can be assigned to incidents based on their parameters like category, requester, impact, urgency etc. In cases where an SLA is about to be breached or has already been breached, the incident can be escalated functionally or hierarchically to ensure that it is resolved at the earliest.

- **Incident resolution**

  An incident is considered resolved when the technician has come up with a temporary workaround or a permanent solution for the issue.

- **Incident closure**

  An incident can be closed once the issue is resolved and the user acknowledges the resolution and is satisfied with it.

Post-incident review

After an incident has been closed, it's good practice to document all the takeaways from that incident. This helps better prepare teams for future incidents and creates a more efficient incident management process. The post-incident review process can be broken down into various aspects, as shown below, and is particularly useful for major incidents.

Internal evaluation

- **Incident identification**
  - Who detected the incident and how?
  - How soon was the incident detected after it occurred?
  - Could the incident have been identified earlier?
  - Could any tools or technologies have aided in the prompt or pre-emptive detection of the incident?

- **Information flow and communication:**
  - How quickly were the stakeholders informed about the incident?
  - What channel was used for relaying notifications?
  - Were all the relevant stakeholders promptly updated with the latest information?
  - How easy was it to communicate with the end user(s) to gather information and keep them informed on the status of the ticket?
- **Structure**
  - How the incident response team was initially structured?
  - Was this structure adhered to throughout the incident management life cycle? If not, why? What changes had to be made to the structure?
  - Can the incident handling team be organized in a better way? If so, how?
- **Resource utilization**
  - What resources were employed to handle the incident?
  - Were those resources used to their optimal capacity?
  - How quickly were resources mobilized to handle the incident?
  - Could resource utilization be improved in the future?
- **Process**
  - How closely was the defined incident management process followed?
  - Were there any deviations in the incident management workflow and process?
  - Were the incident SLAs honoured? If not, which SLAs were breached? Why?
  - Was there adequate monitoring of the process being followed for handling the incident?
  - Could the process be improved to make it more efficient? If yes, how?
- **Reporting**
  - Were reports generated to analyse how the incident was handled?
  - What parameters were included in the reports?
  - Which parts of the incident life cycle were analysed?
  - Is there any room for improvement? If so, how can it be achieved?

External evaluation - End User surveys

Apart from the above factors, some end-user facing factors should also be evaluated. For this purpose, a post-closure survey is conducted to collect feedback from the end users affected by the incident. This survey should be used to gain insight in some key areas, like:

- How easy or difficult was it for the end user to report an incident?
- Was the first response from the IT team swift and prompt?
- Was the incident resolved in a timely manner?
- How satisfied is the end user with the resolution?

The key performance indicators for IT incident management

Metrics that drive important decisions are
termed key performance indicators (KPIs). Below are a few KPIs for effective IT incident management.

Average resolution time

The average time taken to resolve an incident.

Average initial response time

The average time taken to respond to each incident.

SLA compliance rate

The percentage of incidents resolved within an SLA.

First call resolution rate

Percentage of incidents resolved in the first call.

Number of repeat incidents

The number of identical incidents logged within a specific time frame.

Reopen rates

The percentage of resolved incidents that were reopened.

Incident backlog

The number of incidents that are pending in the queue without a resolution.

Percentage of major incidents

The number of major incidents compared to the total number of incidents.

Cost per ticket

The average expense pertaining to each ticket.

End user satisfaction rates

The number of end users or customers who were satisfied with the IT services delivered to them.