# Incident management

**What is an incident ?** Incident is any interruption or disruption to normal IT services .

**IT services -** IT services is where you have the network services ,systems ,applications ,voice ,database as well as end user support related services

**Examples of Incidents** - Router down ,database down , Payroll service down and reported by users ,non IT or IT users

**Incident management** - Prime service of incident management is to restore the services as soon as possible to reduce the business impact and improve the productivity any IT services incident that need to be restored

**SLA** stands for service level agreement. It refers to a document that outlines a commitment between a service provider and a client, including details of the service, the standards the provider must adhere to, and the metrics to measure the performance.

**Incident management objectives -** 1)meeting SLA’s provided by the organization ,internal or external org i.e SLA’s set by client

2) client satisfaction

3) improvement in the business productivity

4)

**Inputs to Incident management -** phone call or web tool like snow ,hp service center ,BSM remedy or email etc , incident can come from client or supplier

**Incident management process activities -** depends from organization to organization

1)log

2)categorize

3)prioritize

4)diagnose

5) resolve and communication

Or

1)Identification

2)log

3)categorize

4)prioritize

5)diagnose the location of incident to right resolver group

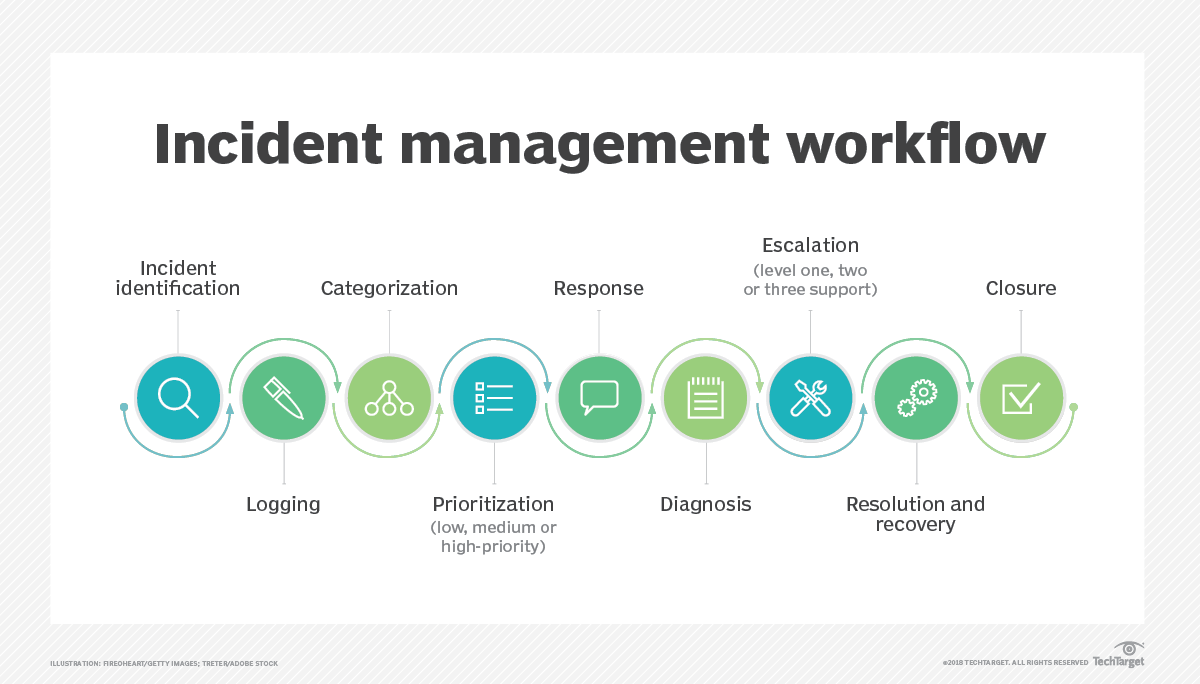
6) if not resolve then escalate

7)pushing people to restore

8) communicate to the user

9)update the knowledge base

10)close



**Scope of Incident management -** understand define scope of IT service in the organization

**SLM** -

**What is correlation of SLM & Incident management -**

Purpose of Service level management is to define SLA’s between service provider and client which is mutually agreed .It avoids penalty defined over SLA

**How escalation works in incident management -** 2 types

1. **Functional**

For example Server management team has L1 , L2 and L3

So for P4 - response time is 120 minutes and resolution time is 480 minutes

So we give 50% of time to L1 team for P4 incident

Remaining 50% of time given to L2 team

After 100%

Breached SLA’s will be given to L3 team ,

1. **Hierarchical**

Hierarchical escalation, also known as managerial escalation, is when an issue is passed to a more senior person or team within an organization based on their experience or seniority level. This can happen when a customer's needs aren't being met by an agent, or when the customer is unhappy with their response and wants to speak to someone with more authority or expertise. For example, if a customer asks for a refund or discount that an associate can't give, they may need to speak to a manager

1. **Hierarchical Escalation:**
   * Definition: Hierarchical escalation refers to the process of passing an issue or incident up the organizational hierarchy based on the level of expertise or seniority.
   * Key Points:
     + Flow: Issues move from junior staff to more experienced or specialized team members.
     + Purpose: Ensures that the right expertise is involved in resolving complex problems.
     + Examples: When a junior developer escalates a critical bug to a senior developer or when a customer service representative passes a challenging customer issue to a supervisor.
     + Advantages: Utilizes specialized knowledge, maintains efficiency, and provides better support.
     + Challenges: Can lead to slower decision-making and reduced empowerment of frontline staff.
     + **Visual Representation**:

Junior Developer → Senior Developer

Customer Service Rep → Supervisor

1. **Functional Escalation:**
   * **Definition**: Functional escalation involves routing an issue to a specialized team or department based on the specific function or domain related to the problem.
   * **Key Points**:
     + **Flow**: Issues move horizontally across functional areas (e.g., from development to testing, from IT support to network engineering).
     + **Purpose**: Ensures that issues are handled by experts in the relevant domain.
     + **Examples**: Escalating a database-related issue to the database administration team or forwarding a security incident to the cybersecurity team.
     + **Advantages**: Efficiently addresses domain-specific challenges.
     + **Challenges**: Requires effective communication between functions and clear handoffs.
     + **Visual representation** 
       1. Development Team → Testing Team
       2. IT Support → Network Engineering

Remember that both hierarchical and functional escalation play crucial roles in incident management, ensuring that the right people with the right expertise are involved in resolving issues within an organization.

**Give me some Incident management process improvement -**

**Incident management L1,L2 & L3-**

In the context of incident management, the terms L1, L2, and L3 refer to different levels or tiers of technical support. Let’s break down what each level entails:

1. **L1 (Level 1) Support:**
   * Role: L1 support is the initial point of contact for users experiencing technical issues. It’s often provided by the user help desk.
   * Responsibilities:
     + Issue Screening: L1 personnel screen incoming issues, gather relevant information, and assess the severity.
     + Basic Troubleshooting: They handle straightforward issues that can be resolved using predefined procedures or knowledge bases.
     + User Assistance: L1 support assists users with common problems, such as password resets, software installations, and basic configuration.
   * [Example: If a user can’t log in to their email account, L1 support would guide them through the steps to reset their](https://www.infosys.com/digital/insights/Documents/application-maintenance-support.pdf) password
2. **L2 (Level 2) Support:**
   * Role: L2 support comes into play when issues are more complex or require deeper technical expertise.
   * Responsibilities:
     + Advanced Troubleshooting: L2 personnel analyze incidents that couldn’t be resolved at L1. They use technical knowledge to diagnose and address issues.
     + Configuration and Workarounds: L2 may perform basic configuration changes within applications or suggest workarounds.
     + Interaction with Other Teams: If necessary, L2 collaborates with other teams (e.g., development, network) to resolve incidents.
   * Example: Suppose an application is crashing due to a specific configuration. [L2 would investigate and make necessary adjustments1](https://www.infosys.com/digital/insights/Documents/application-maintenance-support.pdf).
3. **L3 (Level 3) Support:**
   * Role: L3 support handles the most complex and critical incidents.
   * Responsibilities:
     + Code Changes and Custom Solutions: L3 personnel deal with incidents that require code modifications, custom solutions, or deep system understanding.
     + Root Cause Analysis: They identify underlying causes and address systemic issues.
     + Escalation Point: L3 serves as an escalation point for unresolved L2 incidents.
   * [Example: If an application bug requires code changes or database adjustments, L3 support would handle it1](https://www.infosys.com/digital/insights/Documents/application-maintenance-support.pdf).

Remember that these levels are part of a structured approach to IT support, allowing organizations to efficiently address user needs and maintain high-quality service.

[Each level builds upon the previous one, ensuring a comprehensive support system](https://www.infosys.com/digital/insights/Documents/application-maintenance-support.pdf)

**Incident management KPI’s -**

A KPI is a specific metric used to evaluate performance. It provides a clear, measurable way to assess progress toward strategic, financial, or operational goals.

* **Purpose of KPIs:**
  + **Strategic Decision-Making**: KPIs allow management to make informed decisions by succinctly communicating results.
  + **Focus and Improvemen**t: They create a basis for decision-making and help focus attention on what matters most.
  + **Performance Evaluation**: KPIs gauge output against targets, objectives, or industry peers.
* **Categories of KPIs:**
  + **Strategic KPIs**: High-level indicators used by executives. Examples include return on investment (ROI), profit margin, and total company revenue.
  + **Operational KPIs**: Analyze processes, segments, or geographical locations month over month (or even day over day). Used by managing staff to address questions derived from strategic KPIs.
  + **Customer-Focused KPIs**: Measure per-customer efficiency, satisfaction, and retention.
  + [**Process-Focused KPIs**: Monitor operational performance across the organization](https://www.investopedia.com/terms/k/kpi.asp)

Number of incidents resolved within SLA’s

Number of incidents breached/violated SLA’s

**Incident management -** placeholder for next items

**Incident management -** placeholder for next items