Incident Management Workflow and ITIL Basics

Faraazuddin Syed

Aspiring IT Professional

30/09/2025

Edition 1

Table of Contents

Understanding the ITIL service lifecycle

What is the ITIL service lifecycle?

- The method for implementing the best practices outlined in the ITIL framework. With the service lifecycle, the need for coordination is emphasized.

- This method includes factors like service strategy, design, transfer, operation, and continuous improvement. They are strategic.

1. Service Strategy

This explains how IT services will be used to meet business objectives, it also demonstrates how these services will support a company's overall business strategy. The goal is to establish a service provider's perspective, position, plan, and patterns.

2. Service Design

At this point, the service strategy is converted into a tactical plan to achieve an IT department's goals. To make sure services provide value to a business, they must be created with a business need and aim in mind. The benefit of this stage is primarily reducing the total cost of ownership (TCO), enhancing quality, dependability, and performance. It improves IT governance, efficiency, and service management procedures.

3. Service Transition

At this stage, the tactical plan is being put into operation, and the service transition stage will improve decision making and service management. It makes sure that new, updated, or discontinued services match the previously agreed upon terms in the design and strategy stages.

It helps estimate the costs of the service timeline, improve the number of successful changes, reduce time and amount of effort, and improves the expectations of stakeholders.

4. Service Operation

Gives value to an organization using technology on a regular basis. It aims to guarantee that essential services are supplied quickly and effectively to customers. Helps in the improvement of services by consistently doing periodic tasks. In this section there are five key processes:

1. Event Management, which refers to the process of managing an event over its entire life cycle.

2. Incident Management, which refers to effectively restoring disrupted services by bringing them to normal operating level.

3. Problem Management, which refers to determining the root cause of numerous incidents and taking action.

4. Request fulfillment, which involves handling service requests, which are small, low-risk changes.

5. Access Management, which is concerned with allowing only authorized users to access a service.

5. Continual Service Improvement

These are procedures that use quality management approaches to improve each phase of the IT service management process. They involve:

1. Service Review, to evaluate the infrastructure and business services on a regular basis.

2. Process evaluation, to conduct frequent evaluations of IT procedures.

3. Defining CSI initiatives, which identify specific initiatives aimed at improving services and processes.

4. Monitoring CSI initiatives, which check the improvement initiatives and verify that they are proceeding per their plan.

Understand Incident Management Workflow

An incident is an event that requires an emergency response, every incident is an event, but not every event is an incident.

What is Incident Management?

A process used by development and IT teams to respond to disruptions and restore services to an operational state. It is a fire drill, but for IT issues. The goal is to minimise impact, and maximize productivity.

- Boosts efficiency
- Improves service quality
- Prioritizes issues
- Reduces downtime
- Learn and prevent issues

1. Logging

Logging the issue helps understand the urgency and impact of the issue.

2. Categorization

At this stage, a service desk technician reads the report / log, and categorizes the incident. This is important because it helps determine whether a range of incidents is actually a problem or not.

3. Prioritization

Now, technicians need to decide how urgent the issue is. Priority is determined by impact.

4. Diagnosis and Escalation

This involves hands-on dealing of the incident, and can involve attempting a few quick fixes, if it is not possible to fix it immediately, all findings are logged, and the issue is escalated to other specialized teams.

5. Investigation and Diagnosis

At this stage, a more specialized team takes over the incident, they review the notes and dig deeper, if it is still not possible to be fixed, the issue is escalated further. This process continues until a fix is found.

6. Resolution and Recovery

Here, the issue is solved, and the technician records the issue, the fix, and writes technical documentation.

7. Closure

The technicians verify that the incident is solved and close the ticket.

Incident Management Tools

Tools such as incident trackers, chatrooms, video chat, real time monitoring and alert systems, documentation tools, and status pages are all used in incident management.