

# Table of Contents

Incident Management Plan Template ..... 3

Incident Management Plan Template ..... 4

*Table of Contents* ..... 4

*Purpose* ..... 5

*Scope* ..... 5

*Incident Management Policy* ..... 5

*Roles and Responsibilities* ..... 5

*Incident Classification* ..... 5

*Incident Response Procedures* ..... 5

6.1 Identification ..... 5

6.2 Logging ..... 5

6.3 Investigation and Diagnosis ..... 5

6.4 Resolution and Recovery ..... 5

*Communication Plan* ..... 5

*Documentation and Reporting* ..... 6

*Post-Incident Review* ..... 6

*Training and Awareness* ..... 6

*Continuous Improvement* ..... 6



# Incident Management Plan Template

## What is Incident Management Plan Template?

An Incident Management Plan Template is a structured framework designed to guide organizations in effectively managing and responding to incidents that disrupt normal operations, thereby minimizing their impact on business continuity. As emphasized in best practices such as TOGAF (The Open Group Architecture Framework), this template provides a blueprint that encompasses the identification, categorization, prioritization, and resolution of incidents, ensuring a systematic approach to incident handling. It typically includes key components such as roles and responsibilities, incident escalation procedures, communication plans, resource management, and post-incident review processes. By leveraging such a template, enterprise architects and project managers can ensure that their organizations are well-prepared to respond to incidents, maintain operational resilience, and continuously improve their incident response strategies through lessons learned.

[template](#)

Copied!



### AI Prompt: Incident Management Plan Template

Imagine you are an IT Service Manager at a large organization, tasked with developing a comprehensive [Incident Management Plan Template] to enhance your team's response to incidents and minimize downtime. Your request is to generate a detailed and practical template that includes sections such as [Incident Identification], [Categorization], [Prioritization], and [Resolution], ensuring it is tailored for a medium-sized enterprise with a complex infrastructure. For example, an effective template might specify procedures for escalating incidents based on their impact on business services, along with a clear communication strategy for stakeholders. As you refine the content, consider adjustments for different industries, such as healthcare or finance, to ensure versatility. The expected output is a clear, structured, and user-friendly template that can be readily adopted and customized by any IT team, enhancing their incident response capabilities while also including tips for regular reviews and continuous improvement. As a bonus, provide some insights on common pitfalls to avoid when implementing an incident management framework to foster a more resilient organizational culture.

[Learn more ...](#)



[Try prompt on ...](#)



# Incident Management Plan Template

## Table of Contents

1. [Purpose](#)
2. [Scope](#)
3. [Incident Management Policy](#)
4. [Roles and Responsibilities](#)
5. [Incident Classification](#)
6. [Incident Response Procedures](#)
  - [6.1 Identification](#)
  - [6.2 Logging](#)
  - [6.3 Investigation and Diagnosis](#)
  - [6.4 Resolution and Recovery](#)
7. [Communication Plan](#)
8. [Documentation and Reporting](#)
9. [Post-Incident Review](#)
10. [Training and Awareness](#)
11. [Continuous Improvement](#)

## Purpose

The purpose of this Incident Management Plan is to provide a structured approach to managing incidents to minimize their impact on the business and ensure timely restoration of services.

## Scope

This plan applies to all incidents affecting the enterprise's operations, including but not limited to IT services, security incidents, and service interruptions.

## Incident Management Policy

- Outline the organization's commitment to effective incident management.
- Define the goals and objectives of the incident management process.

## Roles and Responsibilities

- **Incident Manager:** Oversees the incident management process.
- **Support Teams:** Responsible for resolving incidents.
- **Communications Officer:** Manages communication with stakeholders.

## Incident Classification

- Define categories of incidents (e.g., critical, high, medium, low).
- Criteria for each classification.

## Incident Response Procedures

### 6.1 Identification

- Procedures for identifying incidents, including monitoring and alerting mechanisms.

### 6.2 Logging

- Detailed logging process for recording incidents as they occur.

### 6.3 Investigation and Diagnosis

- Steps for investigating incidents to determine the root cause.

### 6.4 Resolution and Recovery

- Procedures for resolving incidents and restoring services.

## Communication Plan

- Outline how information regarding incidents will be communicated to stakeholders and affected parties.
- Define channels and frequency of communication.

## Documentation and Reporting

- Procedures for documenting incidents and maintaining logs.
- Reporting requirements for incidents (e.g., metrics, summaries).

## Post-Incident Review

- Define the process for conducting a post-incident review.
- Outline the criteria for evaluating incident responses and outcomes.

## Training and Awareness

- Plan for training staff on incident management procedures.
- Promote awareness of the incident management process.

## Continuous Improvement

- Methods for reviewing and improving the incident management process.
- Regular updates to the incident management plan based on lessons learned.



Export as PDF

### Related:

- [Architecture](#)
- [Architecture Templates](#)

### External links:

- TBD

### Search this topic on ...





From:  
<https://almbok.com/> - **ALMBoK.com**

Permanent link:  
[https://almbok.com/architecture/templates/incident\\_management\\_plan\\_template](https://almbok.com/architecture/templates/incident_management_plan_template)

Last update: **2024/11/04 10:41**

