

# ITIL – Dealing with major incidents

## Understanding a major incident

### What is a major incident?

Major incidents are those for which the degree of impact on the business/organisation is extreme. Incidents for which the timescale of disruption – to even a relatively small percentage of users – becomes excessive should also be regarded as major incidents. It is possible to define some of these major incidents, but most will be prioritised as they happen based on impact and urgency. Usually Priority 1 is set aside for these types of incident.

A separate procedure, with shorter timescales and greater urgency, must be used for major incidents. A definition of what constitutes a major incident must be agreed and ideally mapped on to the overall incident prioritisation system.

Where necessary, the major incident procedure should include the dynamic establishment of a separate Major Incident Team, under the direct leadership of the Incident Manager, formulated to concentrate on this incident alone, and to ensure that adequate resources and focus are provided for finding a fast resolution. If the Service Desk Manager is also fulfilling the role of Incident Manager (which is the situation in some businesses and organisations), then a separate person may need to be designated to lead the major incident investigation team – so as to avoid conflict of time or priorities – but should ultimately report back to the Incident Manager.

If the cause of the incident needs to be investigated at the same time, then the Problem Manager will be involved as well, but the Incident Manager must ensure that service restoration and underlying cause are kept separate. Throughout, the service desk will ensure that all activities are recorded and users are kept fully informed of progress. Communication is a hugely important activity in handling major incidents.

The Problem Manager should in these circumstances be notified (if not already aware) and should arrange a formal meeting with interested parties (or regular meetings if necessary). These should be attended by all key in house support staff, vendor support staff and IT services management, with the purpose of reviewing progress and determining the best course of action. The service desk representative should attend these meetings and ensure that a record of actions/decisions is maintained, ideally as part of the overall incident record as major incidents are still logged in the same way as all other incidents (it is only the priority and management of the incident which is different).

If no Problem Manager or Problem Process Owner is currently in place, an Incident Management Executive and Major Incident Team could take on the activities described above.

### Example major incident procedure

A procedure should be in place to manage all aspects of a major incident, including resources and communication. It should describe how the business/organisation handles major incidents from receiving notification of a potential major incident, through the investigation process itself and to the delivery of a final report.

A related procedure describing the process of reviewing the major incident policy and procedure also needs to be in place.

Some of the areas to be covered in the major incident policy and procedure are:

- Purpose
- Scope
- Definition
- Policy
- Roles and responsibilities
- Other considerations

#### Purpose

Describe the purpose of the major incident policy and procedure.

For example:

*“This procedure and related policies have been put in place to document the business/organisation’s requirements and arrangements for responding to and investigating major incidents.”*

## Scope

Document the exact scope of the major incident procedure and policy.

For example:

*“This procedure and related policies apply to all Incidents that, due to their status of impact or urgency to the business/organisation, have been prioritised as a major incident.”*

## Definition

A major incident is defined as an event which has significant impact or urgency for the business/organisation and which demands a response beyond the routine incident management process.

A major incident will be an Incident that is either defined in the major incident procedure or which:

- may either cause, or have the potential to cause, impact on business critical services or systems (which can be named in the major incident procedure);
- or be an incident that has significant impact on reputation, legal compliance, regulation or security of the business/organisation.

## Policy

The business/organisation’s policy is to have an effective and efficient system for responding to major incidents, which is appropriate to the individual circumstances.

The requirements are:

- to provide an effective communication system across the business/organisation during a major incident
- to ensure that an appropriate Incident Manager/Major Incident Team/Management Group are in place to manage a major incident
- that there are in place appropriate arrangements to ensure that major incidents are notified promptly to appropriate management and technical groups, so that the appropriate resources are made available
- to conduct major incident investigations and to contribute to the business/organisation’s knowledge of the causes of incidents
- to provide timely information about the causes of incidents and any relevant findings from investigations
- to conduct a review of each major incident once service has been restored and, in line with problem management, to look at root cause and options for a permanent solution to prevent the same major incident happening again
- to conduct reviews of major incident investigation policy and procedure, independent of the major incident investigation, and to report on them (any lessons to be learned from the policy and procedure review will be considered, and appropriate action taken to ensure any improvements to existing arrangements are implemented within a specified timescale)

## Roles and responsibilities

The following roles and responsibilities need to be defined for managing major incidents:

- The Incident Manager
- The Problem Manager
- If no Problem Manager exists, the role of Root Cause Analyst
- Major Incident Investigation Board
- Investigation Team/investigation resources (technical staff)
- The service desk
- Service level managers/IT account managers
- Any other relevant groups who will act as part of the Major Incident Team

### **Other considerations**

The following also need to be considered for managing major incidents:

- Knowledge transfer
- Changes to appropriate documentation
- Changes to appropriate processes