ITIL – A guide to incident management

What is incident management?

- Incident management is a defined process for logging, recording and resolving incidents
- The aim of incident management is to restore the service to the customer as quickly as possible, often through a work around or temporary fixes, rather than through trying to find a permanent solution

What are the differences between incident management and problem management?

Problem management differs from incident management in that its main goal is the detection of the underlying causes of an incident and the best resolution and prevention. In many situations, the goals of problem management can be in direct conflict with the goals of incident management.

Deciding which approach to take requires careful consideration. A sensible approach would be to restore the service as quickly as possible (incident management), but ensuring that all details are recorded. This will enable problem management to continue once a workaround has been implemented.

Discipline is required, as the idea that the incident is fixed is likely to prevail. However, the incident may well appear again if the resolution to the problem is not found.

Incident versus problem

An incident is where an error occurs: something doesn't work the way it is expected.

This is often described as:

- a fault
- an error
- it doesn't work!
- a problem

but the ITIL term used with is an *incident*.

A problem (is different) and can be:

- the occurrence of the same incident many times
- an incident that affects many users
- the result of network diagnostics revealing that some systems are not operating
- in the expected way

A problem can exist without having immediate impact on the users, whereas incidents are usually more visible and the impact on the user is more immediate.

Examples of incidents

User experienced incidents

Application

- Service not available (this could be due to either the network or the application, but at first the user will not be able to determine which)
- Error message when trying to access the application
- Application bug or query preventing the user from working
- Disk space full
- Technical incident

Hardware

- System down
- Printer not printing
- New hardware, such as scanner, printer or digital camera, not working
- Technical incident

Technical incidents

Technical incidents can occur without the user being aware of them. There may be a slower response on the network or on individual workstations but, if this is a gradual decline, the user may not notice.

Technicians using diagnostics or proactive monitoring usually spot technical incidents. If a technical incident is not resolved, the impact can affect many users for a long time.

In time, experienced users and the service desk will spot these Incidents before the impact affects most users.

Examples of technical incidents:

- Disk space nearly full (this will affect users only when it is completely full)
- Network card intermittent fault – sometimes it appears that the user cannot connect to the network, but on a second attempt the connection works. Replacing the card before it stops working completely provides more benefit to the users
- Monitor flickering – it is more troublesome in some applications than others
- Although the flicker may be easy to live with or ignore, the monitor will not usually last more than a few weeks in this state

Why use incident management?

There are major benefits to be gained by implementing an incident management process:

- improved information to customers/users on aspects of service quality
- improved information on the reliability of equipment
- better staff confidence that a process exists to keep IT services working
- certainty that incidents logged will be addressed and not forgotten
- reduction of the impact of incidents on the business/organisation
- resolving the Incident first rather than the problem, which will help in keeping the service available (but beware of too many quick fixes that problem management does not ultimately resolve)
- working with knowledge about the configuration and any changes made, which will enable you to identify the cause of incidents quickly
- improved monitoring and ability to interpret the reports, which will help to identify Incidents before they have an impact

What happens if incident management is not used?

Failing to implement incident management may result in:

- no one managing and escalating incidents
- unnecessary severity of incidents and increased likelihood of impact on other areas (for instance, a full disk will prevent printing, saving work and copying files)
- technicians being asked to do routine tasks such as clear paper jams, repair a *broken* monitor that has merely had the power disconnected, or fix a disk error when a floppy disk was left in during reboot
- specialist support staff being subject to constant interruption, making them less effective
- other staff being disrupted as people ask their colleagues for advice
- frequent reassessment of incidents from first principles rather than referring to existing solutions, such as the knowledge database
- lack of coordinated management information
- forgotten, incorrectly handled, or badly managed incidents

Issues with deciding on an incident management process

Be prepared to overcome:

- absence of visible management or staff commitment, resulting in non-availability of resources for implementation
- lack of clarity about the business/organisation's needs
- out of date working practices
- poorly defined objectives, goals and responsibilities
- absence of knowledge for resolving incidents
- inadequate staff training
- resistance to change

Who uses incident management?

Any organisation that needs to understand its technical support requirements should start with implementing a service desk, closely followed by a defined incident management process.

It will help to channel all incidents through a single point of contact (service desk) so that someone is responsible for following them through to a speedy resolution. Most organisations that rely on IT services need to know how their ICT systems/IT services are functioning, what is failing and how long systems are unavailable. The reports produced in the process of incident management focus on the performance of equipment, and not on the technical issues that created the incidents.

How incident management works

Incident management is about understanding the incident life cycle and the actions to take at each stage.

Incident process

Inputs to the incident process

- Incident details logged at the service desk
- Configuration details from the configuration management database
- Output from problem management and known errors
- Resolution details from other incidents
- Responses to requests for change

Output from the incident process

- Incident resolution and closure
- Updated incident record and call log
- Methods for work arounds
- Communication with the user
- Requests for change
- Management information (reports)
- Input to the problem management process

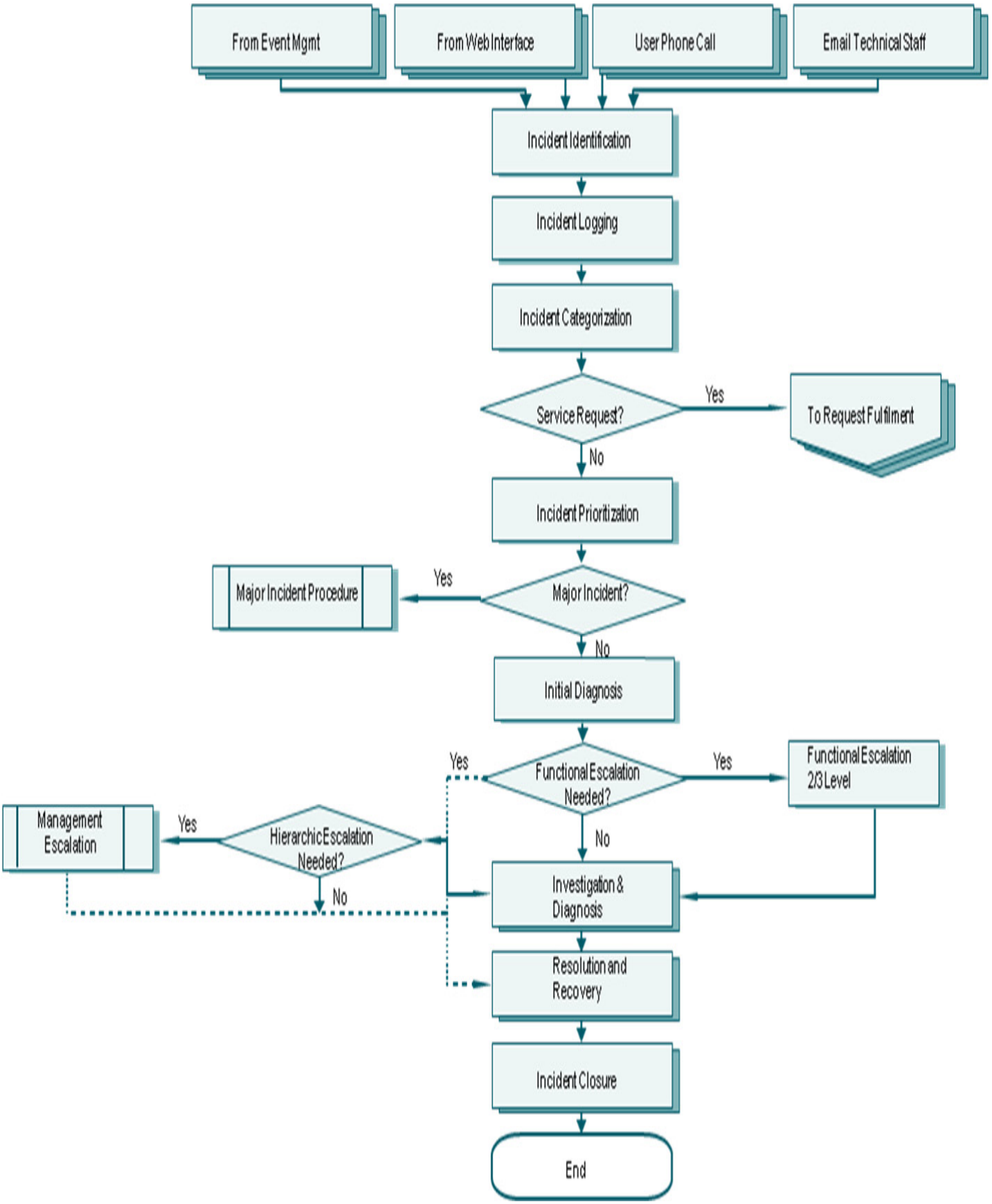
Activities of the incident process

- Incident detection and recording
- Initial user support by the single point of contact (service desk)
- Investigation and diagnosis
- Resolution and recovery of service
- Incident closure
- Incident ownership, monitoring, and communication

Define what needs to be done to implement incident management

- Before identifying your needs, consider what you want to achieve
- This is an opportunity to re-evaluate the way you have, to date, approached and fixed incidents. Rethink current processes and activities
- Understand the difference between incident management and problem management
- Technical staff will always try to solve the cause of a problem. Their way of thinking needs to change so that they approach it with incident management before problem management
- Choose which areas to improve and which processes to remove
- You need to sell the idea to the other staff, so make it appeal to yourself first

Implementing incident management



Roles and functions in the incident process

Service desk role in incident management

Service desk responsibilities include:

- logging the incident in the call log
- performing the initial Incident diagnostics
- requesting technician support when required
- owning, monitoring and communicating
- updating records (call log, incident sheet) with the resolution
- closing incidents
- progressing any follow up action (for example, following through into problem management)

Technical support role in incident management

The technician's role in incident management has the same focus – to restore the service as soon as possible. The technician will keep the service desk informed at all stages.

Other roles

Additional first line support groups, such as configuration management or change management specialists should be consulted.

Second and third line support groups, including specialist support groups and external suppliers should be consulted as necessary.

Users should keep the service desk informed of any further changes to the state of the affected equipment (sometimes computers start working again when different incidents are resolved).

Prepare to implement incident management

- Implement the service desk first
- Decide how incident management will interface with the service desk
- Decide who will take on the responsibility of incident management
- Make sure that management commitment, budget and resource is made available before you consider setting up incident management
- Ensure that the proposed solution aligns with your business/organisation's strategy and vision
- Define clear objectives and deliverables
- Involve and consult IT staff
- Sell the benefits to the support staff – implementing incident management will need a change of behaviour from IT staff as well as users
- Plan the incident management process training
- Service desk training is the first priority
- Incident management training – who, when
- Decide what to measure and report
- Before making changes, you must understand the levels of service you are currently providing with the current resources available
- Produce a report on the number of calls currently logged, the time taken to resolve them and the time the equipment is unavailable – this is your baseline
- Set targets for a manageable number of objectives for the effectiveness of incident management

- Decide what incident management reports are required
- Ensure that the incident management process is regularly reviewed

Incident management post implementation review

It is the users' perception rather than availability statistics or transaction rates that, in the end, defines whether the service is meeting their needs.

User satisfaction analysis and surveys

Satisfaction surveys are an excellent method of monitoring user perception and expectation and can be used as a powerful marketing tool. However, to ensure success you should address several key points:

- Decide on the scope of the survey
- Decide on the target audience
- Clearly define the questions
- Make the survey easy to complete
- Conduct the survey regularly
- Make sure that your users understand the benefits
- Publish the results
- Follow through on survey results
- Translate survey results into actions

Measurements

- Do not set targets that cannot be measured
- Ensure that users are aware of what you are doing, and why
- Establish a baseline before discussing formal Service Level Agreements (SLAs) with customers
- Maintain measurements of what is necessary and viable. For instance, if your staff think that they need feedback on response times, then measure them

Incident management reports

There should already be reports produced by the service desk on the number of incidents logged each week. Expand on the information in those reports to decide whether your new approach to incident management is effective. For example:

- In addition to recording the number of incidents logged each week, compare the numbers to incidents logged prior to implementing incident management
- Show the average length of time taken to resolve incidents before and after implementing incident management
- Where possible, show the types of incident reported
- Show the percentage of incidents handled within the agreed response time
- Show the percentage of incidents closed by the service desk without the need for contacting technical support
- Show the number and percentage of incidents resolved remotely, without the need for a visit

Reports are used to summarise in non-technical language and to show where improvements could be made. Often the improvements require expenditure, so having reports to back up your suggestions can prove invaluable.