ITIL v3 Incident Management Process

...restoring normal service operation as soon as possible
Content

• Key definitions
• Incident Lifecycle
• Purpose and Objectives
• Value to business
• Incident Priority
• Incident Priority and Target resolution times
• Major Incidents
• Escalations – Hierarchical & Functional
• Standard Incident Models
• Process Workflow
• Process Interfaces
• Information Management

• Challenges
• Risks
• Critical success factors (CSF)
• Key Performance Indicators (KPIs)
• Roles and Responsibilities
Key definitions

- **Incident**
  - unplanned interruption to an IT service
  - reduction in the quality of an IT service
  - failure of a CI that has not yet impacted an IT service
    - *(e.g. Redundant component failure)*

- **Service Request**
  - Formal request from a user for something to be provided.
    - ... *e.g. a request for information or advice; to reset a password; or to install a workstation for a new user*
    - ... *NOT a disruption to the agreed service*
    - ... *Request Fulfilment process. Manages lifecycle of Service Requests*

- **Workaround**
  - Method of bypassing an Incident or Problem (temporary fix).
  *It is not a permanent solution* but something that is used to get the service up and running till the real solution is found.*
Incidents have a Lifecycle!...

„Lifecycle is the series of changes that happen to a living creature/project/product/etc. over the course of its lifetime.”

Status codes indicate where Incidents are in relation to the lifecycle. E.g.:

- Open
- In progress
- Resolved
- Closed
- (Pending)

... Incident management is the process responsible for managing the lifecycle of all incidents.
Incident Management is like fire-fighting!
Purpose and objectives

Purpose

...restore normal service operation as quickly as possible

...minimize the adverse impact on business

...ensuring best possible levels of service quality and availability are maintained according to SLA’s

Objectives

• standardized methods and procedures
• increased visibility and better communication
• priorities aligned with business
• user satisfaction with the quality of IT services.
Value to business

- reducing service downtime
- reducing Incident impact to business
- aligning IT to business priority
- identify possible improvements to service
- identification of additional requirements (e.g. training, new service) as a result of handling multiple incidents.

* Value of IM is highly visible to the business. For this reason, IM is often one of the first processes to be implemented in Service Management projects.
Incident Priority

... assigned, to ensure that the support groups will pay the required attention to the incident.

... based on the Urgency and Impact.

\[
\text{IMPACT} + \text{URGENCY} = \text{PRIORITY}
\]

How much damage, if not fixed soon? How fast does it need to be fixed?
### Incident Priority & Timescales

- must be agreed for all incident-handling stages
- based upon the overall incident response and resolution targets within SLAs
- captured as targets within OLAs and Underpinning Contracts (UCs).
- support groups should be made aware of these timescales.
- Service Management tools automate and escalate as required

### Example of priority coding system:

<table>
<thead>
<tr>
<th>URGENCY</th>
<th>IMPACT</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Priority code</th>
<th>Description</th>
<th>Target Resolution Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical</td>
<td>1 hour</td>
</tr>
<tr>
<td>2</td>
<td>High</td>
<td>8 hours</td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
<td>24 hours</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>48 hours</td>
</tr>
<tr>
<td>5</td>
<td>Planning</td>
<td>Planned</td>
</tr>
</tbody>
</table>
Major Incidents

**Major Incident** = High Impact + High Urgency

... highest category of impact for an incident.
... results in significant disruption to the business.
... should have separate procedure

A separate procedure !!! (for major incidents)

... shorter timescales and greater urgency

... separate major incident team under the direct leadership of the incident manager

... Informing Management and Customer

... Service Desk ensures that all activities are recorded and users are kept fully informed of progress.
Functional and Hierarchical Escalation

**Escalation** is the mechanism that assists timely resolution of an Incident.

**Hierarchical Escalation**
...can take place at any moment during resolution.

Reasons might be:
- SLA threat
- Extra resources required
- Need to inform Higher management

**Functional Escalation**
... means involving more specialist personnel or access privileges to solve the incident. Departmental boundaries may be exceeded.
Standard Incident models

Standard Incident Models are designed and implemented for handling standard (reoccurring) incidents more efficiently.

An Incident Model should include the following:
- steps required to handle the incident and their order
- Responsibilities
- Timescales and thresholds for completion
- Any escalation procedure
- Any evidence prevention activities

...Support tools can then be used to automate handling of standard incidents.
Process Workflow

From Event Mgmt -> Incident Identification -> Incident Logging -> Incident Categorisation

Service Request
- Yes: To Request Fulfilment
- No:
  - Incident Prioritisation
    - Major Incident?
      - Yes: Major Incident Procedure
      - No: Initial Diagnosis
        - Functional Escalation Needed?
          - Yes: Functional Escalation 2/3 Level
          - No:
            - Investigation & Diagnosis
            - Resolution & Recovery
            - Incident Closure
TRIGGERS: Incidents ... from Event Mgmt, from web interface, from Users, from suppliers, from technical Stuff

Incident Identification:

- Usually it’s unacceptable to wait until a user logs an incident
- Monitoring assures:
  - Early detection of Failure/potential failure
  - Quick start of Incident Management

* IDEAL SITUATION: Incident is resolved before it had an influence on users!
Incident Management

Process Workflow – Incident Logging

- **All incidents** must be
  - fully logged (INC. NO., DATE, TIME, OWNER, CONTACT...)
  - ... and date/time stamped;
  - Full historical record of all incidents must be maintained

... “Opportunity fixes” must also be logged !!! (ALL must be logged)

* Incident is logged  -> **Resolution time count starts** !
Categorization indicates the **type of incident** being logged

* Category is often related to team that will handle the incident from the Service Desk

* Categories are often multi-level. For Example:
  - Hardware – Server – Memory Board – Card Failure
  - Software – Application – Finance Suite – Purchase Order System

* It’s useful if incident and problem categories are alike
Process Workflow – Service Request?

- A part of categorisation will be to **check if it’s a Service Request**
  - If it is -> It will be transferred to Request Fulfilment process

*Requests are not incidents and should be handled differently*
Process Workflow – Incident Prioritization

- Prioritisation determines how the incident will be handled by support staff and by support tools

* Remember: **PRIORITY = Urgency + Impact (+ SLA)**

<table>
<thead>
<tr>
<th>URGENCY</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Low</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>Priority code</th>
<th>Description</th>
<th>Target Resolution Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>1</td>
<td>Critical</td>
<td>1 hours</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
<td>High</td>
<td>8 hours</td>
</tr>
<tr>
<td>Low</td>
<td>3</td>
<td>Medium</td>
<td>24 hours</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Low</td>
<td>48 hours</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Planning</td>
<td>Planned</td>
</tr>
</tbody>
</table>
**Incident Management**

Process Workflow – Major Incident?

- If priority indicates Major Incident it must be handled by following the Major Incident Procedure

*Staff must be familiar with the procedure!*
• Service Desk Analyst will determine with the user:
  - Full symptoms (what has gone wrong)
  - How to correct it?
    - Using:
      - Diagnostic scripts
      - Known Error information

If the incident is resolved -> it will be closed (after informing the user !!!)
Incident Management

Process Workflow – Functional Escalation

If the incident is NOT resolved -> it will be escalated (and user informed !!!)

- **FUNCTIONAL ESCALATION** (to the next level of support) occurs when:
  - Current level of support can’t resolve the incident
  - Current level of support has reached time scales for resolving the incident

* Ownership of the incident stays with the Service Desk!*
* Service Desk will track and monitor progress! *
If the incident is NOT resolved -> it will be escalated (and user informed !!!)

- **HIERARCHIC ESCALATION** (up the management chain) occurs when:
  - SLA breaches are threatened
  - Extra resources are needed to resolve the incident
  - Senior Management needs to be aware / approve the steps required

* May also be initiated by the customer / user if they see it necessary!
**Incident Management**

**Process Workflow – Investigation & Diagnosis**

- More detailed information might be collected on:
  - Exactly what has gone wrong
  - Understanding the chronological order of events
  - Confirming the full impact
  - Identifying events that may have triggered the incident
  - Knowledge searches
  - Previous incidents
  - Changes made

* All actions and findings must be recorded!
* As much actions as possible should be performed in parallel to save time
When the resolution has been identified it should be applied and tested.
If satisfactory a time / date stamp is recorded as this is the end of downtime.
The incident record must be updated with the details of actions taken.
The incident should be returned to the Service Desk for closure action.
Before closing the incident the SD Analyst must:

- Make sure the user is informed and happy with the solution
- The assigned incident category is the correct one (if not, correct it)
- The incident documentation is complete

- If there is indication the incident might recur, a Problem record should be raised

* The Incident is closed by Service Desk!
* Re-opening incidents – strict rules must exist for this action !!!
Incident Management

Process Interfaces

- **Event Mgmt**: Event can (automatically) raise incident
- **Request Fulfilment**: Request handling can also be handled by IM process
- **Problem Management**: Incidents (repeated) often point to problems
  - Solving the problems should reduce the number of incidents
- **Asset & Configuration Mgmt**: Provides data used to identify and progress incidents
  - IM assists in verification of CMS
- **Change Management**: Changes are often reasons why incidents occur
  - Incidents can lead to changes required for resolutions/workarounds
Process Interfaces – cont.

- **Service Level Management**
  - IM must restore service as agreed in SLAs – thus, targets for IM are determined considering SLM and vice-versa

- **Service Catalogue Management**
  - Service Desk will consult Service Catalogue in handling incidents

- **Capacity Management**
  - IM may trigger monitoring of a system or service performed by Capacity Management
  - Workarounds used by Incident Management can come from Capacity Management

- **Availability Management**
  - Incident data is important in determining availability.

- ...
Involvement in Information Management

Incident Record
• Reference Number
• CI Impacted
• Dates and Times
• Originator
• Affected users
• Symptoms
• Category, Priority
• Actions Taken
• Relationships
• Closure details
Incident Management

Challenges

- Ability to detect incidents as early as possible.
- Convincing all staff that **ALL incidents must be logged**.
- Making information available about known errors to ensure staff learn from previous incidents.
- Configuration Management System integration
- Integration into the Service Level Management processes in order to correctly assess the impact and priority of incidents, and
- Defining escalation procedures.
Incident Management

Risks

- Incidents not being handled in appropriate timescales
- Insufficient incident backlog
- Poor information availability (for resolving/escalating...)
- Mismatch in objectives/expectations for Incident Management

...due to a lack of or inappropriate training?
...due to inadequate support tools?
...due to lack of support tools integration?
...due to poorly-aligned or non-existent OLAs or UCs...SLAs?

....due to ...... ?
Critical Success Factors (CSF) & Key performance Indicators (KPI)

**CSF Resolve incidents as quickly as possible minimizing impacts to the business**
- **KPI** Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code
- **KPI** Breakdown of incidents at each stage (e.g. logged, work in progress, closed etc.)
- **KPI** Percentage of incidents closed by the service desk without reference to other levels of support (often referred to as ‘first point of contact’)
- **KPI** Number and percentage of incidents resolved remotely, without the need for a visit

**CSF Maintain quality of IT services**
- **KPI** Total numbers of incidents (as a control measure)
- **KPI** Size of current incident backlog for each IT service
- **KPI** Number and percentage of major incidents for each IT service

**CSF Maintain user satisfaction with IT services**
- **KPI** Average user/customer survey score (total and by question category)
- **KPI** Percentage of satisfaction surveys answered versus total number of satisfaction surveys sent
Incident Management

**Roles**

**IM Process Owner** - accountable for the process

- Developing and maintaining IM process and procedures (driving efficiency and effectiveness)
- Managing the work of incident support staff (first- and second-line)
- Managing Major Incidents
- Monitoring the effectiveness of IM ...recommending improvement
- Developing and maintaining the IM systems
- Producing management information

**Incident Manager** ...manages the work of Incident Support Staff

- Identifying, logging, categorizing, prioritizing, diagnosing, resolving/escalating and closing an incident.

**1st line support** *(normally the Service Desk)*

- Investigate, diagnose, resolve (recover) an incident.

**2nd line support** *(generally Technical/Application Management)*

- Investigate, diagnose, resolve (recover) an incident.

**3rd line support** *(External experts or Internal ones)*

- Investigate, diagnose, resolve (recover) an incident.
ITIL v3 Incident Management Process

...restoring normal service operation as soon as possible