

INCIDENT MANAGEMENT

Incident Management

The goal of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.

'Real World' definition of Incident Management:

IM is the way that the Service Desk puts out the 'daily fires'.

Inputs for Incident Management *mostly come from users*, but can have other sources as well like management Information or Detection Systems.

Incidents and Service Requests are formally managed through a staged process to conclusion.

This process is referred to as the "**Incident Management Lifecycle**". The objective of the Incident Management Lifecycle is to restore the service as quickly as possible to meet Service Level Agreements. The process is primarily aimed at the user level.



INCIDENT MANAGEMENT

Mission Statement

ITIL defines an incident as "any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of service."

Process Goals



- Incident detection and recording
- Classification and initial support
- Investigation and diagnosis
- Resolution and recovery
- Incident closure

Success Factor



- Maintaining IT Service Quality
- Maintaining Customer Satisfaction
- Resolving Incidents Within Established Service Times

Performance



- Number of incidents logged
- Number of incidents resolved
- Number of incidents escalated
- Average time to restore service from point of first call

Incidents, problems and known errors



Activities of the Incident Management process:

Usually as part of the wider management process in private organizations, incident management is followed by **post-incident analysis** where it is determined why the incident happened despite precautions and controls. This information is then used as feedback to further develop the security policy and/or its practical implementation.

Incidents, problems and known errors

Incidents may match with existing 'Known Problems' (without a known root cause) or 'Known Errors' (with a root cause) under the control of Problem Management and registered in the Known Error Database (KeDB). Where existing work-arounds have been developed, it is suggested that accessing these will allow the Service Desk to provide a quick first-line fix.

Where an incident is **not** the result of a **Known Problem** or **Known Error**, it may either be an isolated or individual occurrence or may (once the initial issue has been addressed) require that Problem Management become involved, possibly resulting in a new problem record being raised.

Incident management processes

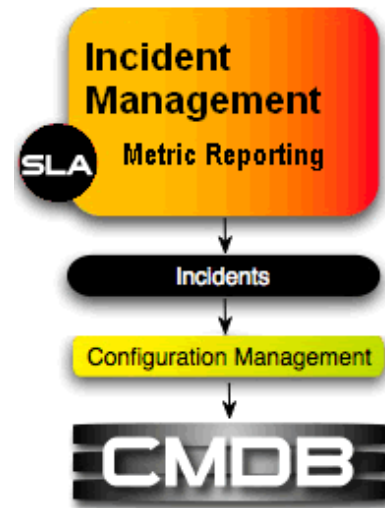
The main incident management processes are the following:

- Incident detection and recording
- Classification and initial support
- Investigation and diagnosis
- Resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking and communication

Incidents should be classified as they are recorded, **Examples of incidents by classification are:**

- **Application**
 - service not available
 - application bug
 - disk-usage threshold exceeded
- **Hardware**
 - system-down
 - automatic alert
 - printer not printing

ESS software streamlines collection and management of incident information at any organizational level or across the enterprise.



SOFTWARE FOR BETTER BUSINESS

© 2010, Westover Consulting, Ltd.

© 2010, Buoyant Solutions, Inc.

Remedy, a BMC Software Company

Remedy, the Remedy logo and all other Remedy product or service names and registered trademarks are trademarks of BMC Software, Inc.

Enterprise Service Suite @ Work™, ESS@ Work™, XtremeAIR™ are trademarks of Westover Consulting, Ltd. and Buoyant Solutions, Inc.

FOR MORE INFORMATION GO TO [HTTP://WWW.BUOYANTSOLUTIONS.NET](http://www.buoyantsolutions.net)