ITIL – Incident management: Key Performance Indicators (KPIs) and reports

KPIs and reports for incident management

Requirements for reports, KPIs and Metrics will be different for each business/organisation so this document only covers key topics. It serves as a guide on suitable KPIs and reports for management, suggesting measures that would be meaningful for the incident management process. A range of metrics that can be used are documented. Technology metrics must be heavily supplemented with non-technical and business focused metrics/KPIs/measures.

KPIs

Continuous improvement requires that each process needs to have a plan about *how* and *when* to measure performance. While there can be no set guidelines for the timing of reviews; the *how* question can be answered with metrics and measurements.

With regard to timing of reviews, factors such as resource availability, cost and *nuisance factor* need to be taken into account. Many initiatives begin with good intentions to do regular reviews, but these fall away very rapidly. This is why the Process Owner must follow through on assessments, meetings and reviews, etc. If the Process Manager feels that reviews are too seldom or too often then the schedule should be changed to reflect that.

Establishing SMART metrics is a key part of good process management.

SMART is an acronym for:

Specific
Measurable
Achievable
Realistic
Time driven

Metrics help to ensure that the process in question is running effectively and efficiently.

The metrics in the following table should be considered.

Key Performance Indicator/Metric
Using data from the Configuration Management Database (CMDB) to indicate any particular configuration items that are experiencing recurring incidents.
The number of incidents logged. These can be broken down by the following: ■ Number of incidents per priority, impact, urgency ■ Number of incidents per type and category ■ Number of incidents per person (i.e. top ten incidents per user) ■ Number of incidents per configuration item type (i.e. top ten infrastructure incidents) ■ Number of incidents per service ■ Number of incidents per business/organisational area

Key Performance Indicator/Metric
The average time to achieve incident resolution. This can be broken down by the following: ■ Type ■ Category ■ Priority, impact, urgency ■ Service
The percentage of incidents handled within the agreed Service Level Agreements for that type of incident or configuration item.
The average cost per incident.
The percentage of incidents resolved at first line support that meet the Service Level Agreement.
The percentage of Incidents resolved by group: ■ Service desk ■ Tier 2 support ■ Tier 3 support ■ External suppliers
The percentage of incidents assigned more than twice.
The number or percentage of major incidents.
The size of the backlog of unresolved incidents.
Breakdown of incidents by time of day, to help pinpoint peaks and ensure matching of resources.
Breakdown of incidents at each stage of the process (e.g. logged, work in progress, closed etc.).
Number and percentage of incidents incorrectly assigned.
Number and percentage of Incidents incorrectly categorised.
Number of incidents handled by each incident model.
Number and percentage of incidents resolved remotely, without the need for a visit.
Number and type of reoccurring incidents.

Tip: beware of using percentages in too many cases; it may even be better to use absolute values when the potential number of maximum failures is less than 100.

Reports should be produced under the authority of the Incident Manager/Incident Process Owner, who should draw up a schedule and distribution list, in collaboration with the service desk and support groups handling incidents. Distribution lists should at least include IT service management and specialist support groups. Consider also making the data available to users and customers, for example via Service Level Agreement reports.

Reports for management

Management reports help identify trends and allow review of the *health* of the process. Setting a level on certain reports may be appropriate as may be categorising the report as strategic, operational or tactical.

The acid test of the relevance of a report is to have a sound answer to the question, *"What decisions is this report helping management to make?"*

Management reports for incident management should include those in the following table.

Report	Timeframe/notes/who
Major incidents logged and resolved. As well as the numbers, a very concise view of major incidents may also be included.	Priority 1 incidents should be fully described.
Summary of incidents that are still to be resolved. Management will be interested to see the number of higher priority incidents still awaiting resolution. Importantly, each outstanding incident should show how long it has been in this status. Incidents that have been waiting for resolution for long periods of time may be downgraded or even closed.	
The number of incidents attributable to different business/organisation areas. This will help management to understand which areas are in a state of continual disruption. Incidents can indicate poor management, fluctuating internal pressures, and/or increasing pressures from external forces.	
The situation regarding the process staffing levels and any suggestions regarding redistribution, recruitment and training required.	
Audit reports should verify that any selected Incident contains all relevant and expected information.	
Relevant financial information (to be provided in conjunction with financial management for IT services) This information will include a cost per incident summary.	