

Quick Guideline for ITIL Compliant INCIDENT & PROBLEM MANAGEMENT Implementation

ITIL (the IT Infrastructure Library) is the most widely accepted approach to IT service management in the world, ITIL provides a comprehensive and consistent set of best practices for IT service management, promoting a quality approach to achieving business effectiveness and efficiency in the use of information systems.

ITIL is based on the collective experience of commercial and governmental practitioners worldwide. This has been distilled into one reliable, coherent approach, which is fast becoming a defacto standard used by some of the world's leading businesses.

This guideline provides a brief overview of the purpose, benefits, problems, tools, processes and procedures related to the implementation ITIL compliant processes for managing reported incidents and problems in live production environments.

Copyright © 2007-2009 Advalue Management Services Ltd - All rights reserved

Information in this document is subject to change without notice. Advalue Management Services Limited assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. Although the intellectual property of IIL best practices lies with OGC, the quick guide in this particular format remains intellectual property of the author and may be used for personal and organisational development provided a reference is made to Advalue Management Services.

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

About the Author



Ad Blankestein (PMP) has over 15 years international programme and project management experience in a variety of industries and countries.

Since 2003 Ad is providing project management services through his company "Advalue Management Services" based in New Zealand.

Advalue has a track record of successful completion of programmes and projects concerning software development & implementation, ITC infrastructure, Business Process Redesign & Organisational Changes, PMO & ITIL implementation, and last but not least recovery of troubled projects.

Ad's Contact Details:

Address: PO Box 641
Orewa, Hibiscus Coast, 0946
New Zealand

Phone: +64 9 424 5004
Mobile: +64 21 400 182
Email: Info@advalueservices.com
Web: www.advalueservices.com

Table of Content

1. INTRODUCTION	4
PURPOSE	4
INTENDED AUDIENCE.....	4
BACKGROUND	4
2. RELATIONSHIP WITH OTHER PROCESSES.....	5
RELATIONSHIP	5
3. BENEFITS & POSSIBLE PROBLEMS – PROBLEM MANAGEMENT	6
BENEFITS.....	6
POSSIBLE PROBLEMS FOR NOT HAVING PROBLEM MANAGEMENT.....	7
4. BENEFITS & POSSIBLE PROBLEMS – INCIDENT MANAGEMENT	7
BENEFITS.....	7
POSSIBLE PROBLEMS FOR NOT HAVING INCIDENT MANAGEMENT	7
5. INCIDENT MANAGEMENT SCOPE.....	8
PROCEDURES	8
SCOPE.....	8
6. PROBLEM MANAGEMENT SCOPE.....	11
PROCEDURES REACTIVE PROBLEM MANAGEMENT.....	11
SCOPE REACTIVE PROBLEM MANAGEMENT.....	11
PROACTIVE PROBLEM SCOPE	16
7. MANAGEMENT REPORTING.....	17
INCIDENT METRICS.....	17
PROBLEM METRICS.....	17
AUDITS	18
8. INCIDENT & PROBLEM MANAGEMENT TOOL	18
CONSIDERATIONS	18
9. FURTHER INFORMATION.....	19
ITIL INFORMATION.....	19

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

1. Introduction

<p>Purpose</p>	<p>The purpose of this guide is to provide a brief overview on how to establish ITIL compliant Issue & Problem Management processes and includes the procedures, tools and dependencies that need to be included in the planning for implementing and using these processes. The guide also describes the anticipated problems with implementing the processes and the benefits that can be achieved when following the processes.</p>
<p>Intended Audience</p>	<p>The intended audience of this guide is:</p> <ul style="list-style-type: none"> • ICT Managers; • Release Managers; • Helpdesk & support teams; • Application development & implementation teams; • Application test teams.
<p>Background</p>	<p>Incident Management</p> <p>The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and to minimise the adverse impact 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.</p> <p>In ITIL terminology, an Incident is defined as:</p> <p><i>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 that service.</i></p> <p>Problem Management</p> <p>The goal of Problem Management is to minimise the adverse impact of Incidents and Problems on the business that are caused by errors within the ICT Infrastructure, and to prevent recurrence of Incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.</p> <p>The Problem Management process has both reactive and proactive aspects. The reactive aspect is concerned with solving Problems in response to one or more Incidents. Proactive Problem Management is concerned with identifying and solving Problems and Known Errors before Incidents occur in the first place.</p>


Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<p>In ITIL terminology Problems are defined as: <i>An unknown underlying cause of one or more Incidents and a 'Known Error' is a Problem that is successfully diagnosed and for which a Work-around has been identified.</i></p>
--	--

2. Relationship with Other Processes

<p>Relationship</p>	<p>The incident and problem management processes have a strong relationship with each other. They also have relationships with change management, release management and configuration management.</p> <p>Problem Management differs from Incident Management in that its main goal of Problem Management is the detection of the underlying causes of an Incident and their subsequent resolution and prevention. In many situations this goal can be in direct conflict with the goals of Incident Management where the aim is to restore the service to the Customer as quickly as possible, often through a Work-around, rather than through the determination of a permanent resolution. In this respect, for Problem Management therefore, the speed with which a resolution is found is only of secondary (albeit still of significant) importance. Investigation of the underlying Problem can require some time and can thus delay the restoration of service, causing downtime but preventing recurrence.</p> <p>The cause of Incidents may be apparent and that cause can be addressed without the need for further investigation, resulting in a repair, a Work-around or an RFC to remove the error. In some cases the Incident itself, i.e. the effect or potential effect upon the Customer, can be dealt with quickly (e.g. by rebooting a PC), without directly addressing the underlying cause of the Incident.</p> <p>Where the underlying cause of the Incident is not identifiable, then it may be appropriate to raise a Problem record. A Problem is thus, in effect, indicative of an unknown error within the infrastructure. Normally a Problem record is raised only if investigation is warranted.</p> <p>This impact will often be assessed (both actual and potential), upon the business services, and the number of similar Incidents apparently sharing a common underlying cause that have been reported. This may be appropriate even where the actual result of the Incident has been addressed.</p>
----------------------------	--

Quick Guide:
 ITIL Compliant Incident & Problem Management Implementation

	<p>It can be seen therefore that a Problem record is independent of associated Incident records, and both the Problem record and the investigation into its cause can persist even after the initial Incident has been successfully closed.</p> <p>Successful processing of a Problem record will result in the identification of the underlying error, and the record can then be converted into a Known Error once a Work-around has been developed, and/or an RFC. This logical flow, from an initial report to the resolution of an underlying Problem, is as follows:</p> <div style="text-align: center;">  <pre> graph LR A[Error in Infrastructure] --> B[Incidents] B --> C[Problem] C --> D[Known Error] D --> E[RFC] E --> F[Structural Resolution] </pre> </div>
--	---

3. Benefits & Possible Problems – Problem Management

Benefits	<p>The benefits of taking a formal approach to Problem Management include the following:</p> <ul style="list-style-type: none"> • Improved IT service quality - Problem Management helps generate a cycle of rapidly increasing IT service quality. High-quality reliable service is good for the business users of ICT, and good for the productivity and morale of the ICT service providers; • Incident volume reduction - Problem Management is instrumental in reducing the number of Incidents that interrupt the conduct of business; • Permanent solutions - There will be a gradual reduction in the number and impact of Problems and Known Errors as those that <i>are</i> resolved <i>stay</i> resolved; • Improved organisational learning - The Problem Management process is based on the concept of learning from past experience. The process provides the historical data to identify trends, and the means of preventing failures and of reducing the impact of failures, resulting in improved User productivity; • Better first-time fix rate at the Service Desk - Problem Management enables a better first time fix rate of Incidents at the Service Desk, achieved via the capture, retention and availability of Incident resolution and Work-around data within a knowledge database available to the Service Desk at call logging.
-----------------	---

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

<p>Possible Problems for not having Problem Management</p>	<p>In contrast, the consequence of not implementing a Problem Management process may include:</p> <ul style="list-style-type: none"> • Purely reactive support organisation, facing up to Problems only when the service to Customers has already been disrupted; • User organisation, confronted with recurring Incidents, losing faith in the quality of the ICT support organisation; • Ineffective support organisation, with high costs and low employee motivation, since similar Incidents have to be resolved repeatedly and structural solutions are not provided.
---	--

4. Benefits & Possible Problems – Incident Management

<p>Benefits</p>	<p>The benefits of taking a formal approach to Problem Management include the following:</p> <ul style="list-style-type: none"> • For the business as a whole: <ul style="list-style-type: none"> ○ Reduced business impact of Incidents by timely resolution, thereby increasing effectiveness; ○ Proactive identification of beneficial system enhancements and amendments; ○ Availability of business-focused management information related to the SLA. • For the IT organisation in particular: <ul style="list-style-type: none"> ○ Improved monitoring, allowing performance against SLAs to be accurately measured; ○ Improved management information on aspects of service quality; ○ Better staff utilisation, leading to greater efficiency ○ Elimination of lost or incorrect Incidents and service requests; ○ More accurate CMDB information (giving an ongoing audit while registering Incidents); ○ Improved User and Customer satisfaction.
------------------------	---

<p>Possible Problems for not having Incident Management</p>	<p>In contrast, the consequence of not implementing a Problem Management process may include:</p> <ul style="list-style-type: none"> • No one to manage and escalate Incidents - hence Incidents may become more severe than necessary and adversely affect IT service quality; • Specialist support staff being subject to constant interruptions, making them less effective;
--	---

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<ul style="list-style-type: none"> • Business staff being disrupted as people ask their colleagues for advice; • Frequent reassessment of Incidents from first principle rather than reference to existing solutions; • Lack of coordinated management information; • Lost, or incorrectly or badly managed Incidents.
--	--

5. Incident Management Scope

Procedures	<p>The ITIL guideline indicates that within the Incident Management process and procedures are needed for setting up and maintaining the following:</p> <ul style="list-style-type: none"> • Incident detection and recording; • Classification and initial support • Investigation and diagnosis; • Resolution and recovery; • Incident closure; • Ownership, monitoring, tracking and communication.
-------------------	--

Scope	<p>In more detail Incident Management processes and procedures should include the following:</p> <ul style="list-style-type: none"> • Incident detection & recording - Incident details from Service Desk or event management systems are the inputs for Incident Management. Resultant actions are to: <ul style="list-style-type: none"> ○ Record basic details of the Incident; ○ Alert specialist support group(s) as necessary; ○ Start procedures for handling the service request; ○ Outputs are: <ul style="list-style-type: none"> ▪ Updated details of Incidents; ▪ Recognition of any errors on the CMDB; ▪ Notice to Customers when an Incident has been resolved. • Classification & initial support <ul style="list-style-type: none"> ○ Inputs are: <ul style="list-style-type: none"> ▪ Recorded Incident details; ▪ Configuration details from the CMDB; ▪ Response from Incident matching against Problems and Known Errors;
--------------	---

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<ul style="list-style-type: none"> ○ Actions are: <ul style="list-style-type: none"> ▪ Classifying Incidents; ▪ Matching against Known Errors and Problems; ▪ Informing Problem Management of the existence of new Problems and of unmatched or multiple Incidents; ▪ Assigning impact and urgency, and thereby defining priority; ▪ Assessing related configuration details; ▪ Providing initial support (assess Incident details, find quick resolution); ▪ Closing the Incident or routing to a specialist support group, and informing the User(s). ○ Outputs are: <ul style="list-style-type: none"> ▪ RFC for Incident resolution; ▪ Updated Incident details, and ▪ Work-around for Incidents, or Incident routed to second- or third-line support. ● Investigation & diagnosis <ul style="list-style-type: none"> ○ Inputs are: <ul style="list-style-type: none"> ▪ Updated Incident details; ▪ Configuration details from the CMDB. ○ Actions are: <ul style="list-style-type: none"> ▪ Assessment of the Incident details; ▪ Collection and analysis of all related information, and resolution; ▪ (Including any Work-around) or a route to n-line support. ○ Outputs are: <ul style="list-style-type: none"> ▪ Incident details yet further updated, and a specification of the selection or required Work-around. ● Resolution & Recovery <ul style="list-style-type: none"> ○ Inputs are: <ul style="list-style-type: none"> ▪ Updated Incident details; ▪ Any response on an RFC to effect resolution for the Incident(s); ▪ Any derived Work-around or solution. ○ Actions are: <ul style="list-style-type: none"> ▪ Resolve the Incident using the solution/Work-around or, alternatively, to raise an RFC (including a check for resolution); ▪ Take recovery actions.
--	--

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<ul style="list-style-type: none">○ Outputs are:<ul style="list-style-type: none">▪ RFC for future Incident resolution;▪ Resolved Incident, including recovery details,▪ Updated Incident details.● Incident Closure<ul style="list-style-type: none">○ Inputs are:<ul style="list-style-type: none">▪ Updated Incident details;▪ Resolved Incident.○ Actions are:<ul style="list-style-type: none">▪ The confirmation of the resolution with the Customer or originator;▪ Close category;▪ Close Incident.○ Outputs are:<ul style="list-style-type: none">▪ Updated Incident detail;▪ Closed Incident record.○ When an incident has been closed it should be ensured that:<ul style="list-style-type: none">▪ Details of the action taken to resolve the Incident are concise and readable;▪ Classification is complete and accurate according to root cause;▪ Resolution/action is agreed with the Customer - verbally or, preferably, by email or in writing;▪ All details applicable to this phase of the Incident control are recorded, such that:<ul style="list-style-type: none">● The Customer is satisfied;● Cost-centre project codes are allocated;● The time spent on the Incident is recorded;● The person, date and time of closure are recorded.● Ownership, Monitoring, Tracking and Communications<ul style="list-style-type: none">○ Inputs are:<ul style="list-style-type: none">▪ Incident records.○ Actions are:<ul style="list-style-type: none">▪ Monitor Incidents;▪ Escalate Incidents;▪ Inform User.
--	---

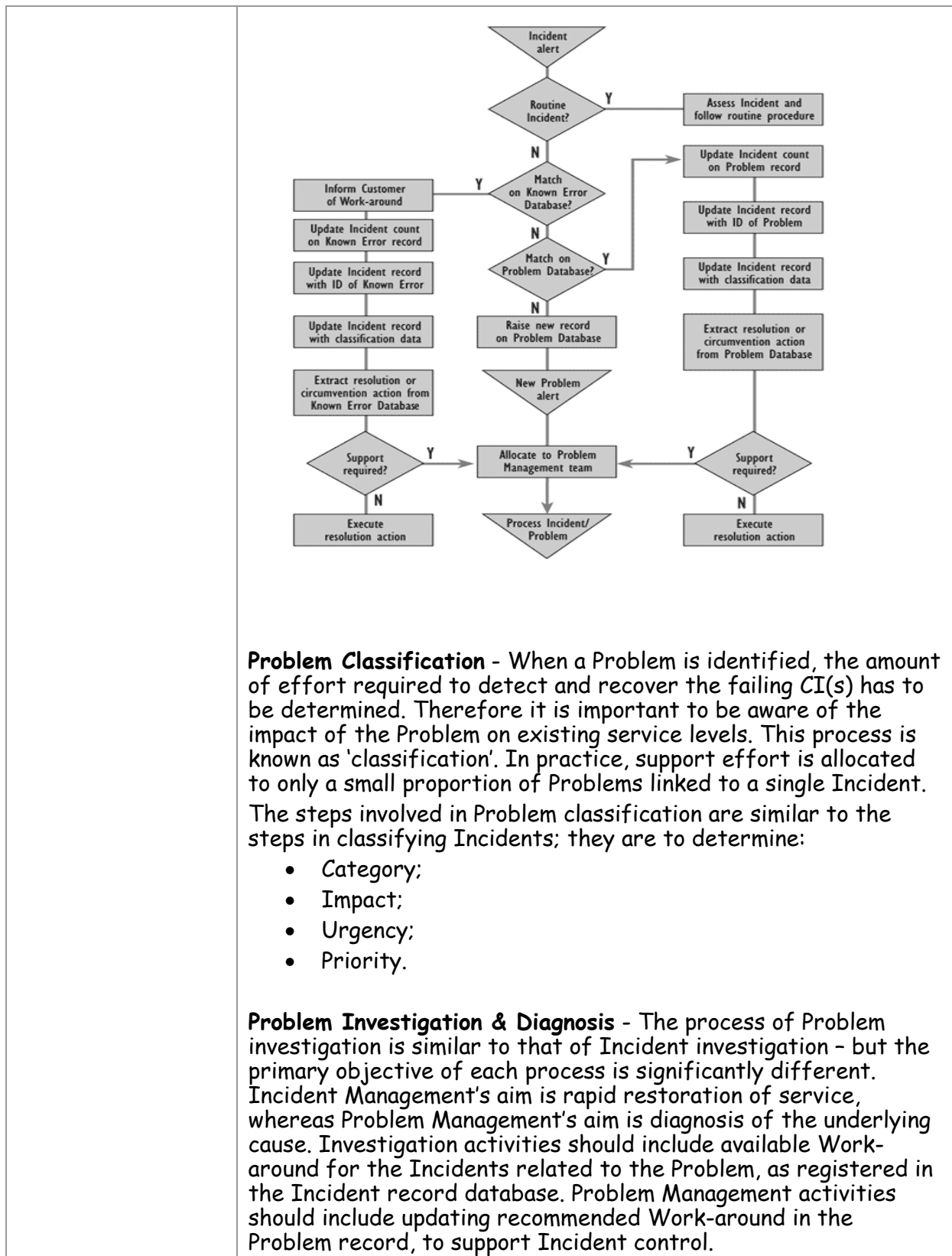
Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<ul style="list-style-type: none"> ○ Outputs are: <ul style="list-style-type: none"> ▪ Management reports about Incident progress ▪ Escalated Incident details; and ▪ Customer reports and communication.
--	--

6. Problem Management Scope

<p>Procedures Reactive Problem Management</p>	<p>The ITIL guideline indicates that Reactive Problem Management is concerned with identifying the real underlying causes of reported Incidents in order to prevent future recurrences. The three phases involved in the (reactive) Problem control process are:</p> <ul style="list-style-type: none"> • Problem identification and recording; • Problem classification - in terms of the impact on the business; • Problem investigation and diagnosis; • Error Control. <p>If the problem diagnosis shows the need for a change (e.g. changing code), the results will feed into to Error Control process which directly interfaces with the Change Management process.</p>
<p>Scope Reactive Problem Management</p>	<p>In more detail Reactive Problem Management processes and procedures should include the following:</p> <p>Problem identification & recording - Reported incidents that need further investigation need to be recorded in a database (ideally the CMDB) and are very similar to Incident records. They usually exclude some of the standard Incident data (e.g. User data) that is inappropriate. However, Problem records should be linked to all associated Incident records. The solution and Work-around of Incidents should be recorded in the relevant Problem records for others to access should other related Incidents occur. The high level process looks as follows:</p>

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation



Problem Classification - When a Problem is identified, the amount of effort required to detect and recover the failing CI(s) has to be determined. Therefore it is important to be aware of the impact of the Problem on existing service levels. This process is known as 'classification'. In practice, support effort is allocated to only a small proportion of Problems linked to a single Incident. The steps involved in Problem classification are similar to the steps in classifying Incidents; they are to determine:

- Category;
- Impact;
- Urgency;
- Priority.

Problem Investigation & Diagnosis - The process of Problem investigation is similar to that of Incident investigation - but the primary objective of each process is significantly different. Incident Management's aim is rapid restoration of service, whereas Problem Management's aim is diagnosis of the underlying cause. Investigation activities should include available Work-around for the Incidents related to the Problem, as registered in the Incident record database. Problem Management activities should include updating recommended Work-around in the Problem record, to support Incident control.

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

Diagnosis frequently reveals that the cause of a Problem is not an error in a registered CI (hardware, software item, documentation or procedure) but is procedural. Incorrect release of a version of a program is one example. These situations result in Problem closure with an appropriate categorisation code.

Problems of this type do not automatically achieve the formal status of Known Error. To ensure that these Problems are followed up and that action is taken to address them, consider creating a dummy CI record for the offending procedure and re-classifying the Problem as a Known Error, or raise an RFC.

Diagnosis showing the cause to be a fault in a registered CI should automatically change the status of the Problem into a Known Error. At this point the error control system and procedures take over

Methods on Problem Analysis - Literature provides many methods for structural Problem analysis and diagnosis. Some available methods are:

- Kepner and Tregoe;
- Ishikawa diagrams;
- Brainstorming sessions;
- Flowchart methods.

Problem Management should select methods that best fit the organisation's purposes.

Tips on Problem Control - The following are points worth remembering in relation to Problem control:

- The categorisation of Incidents can produce a first step towards Problem definition. Problem Management therefore should closely relate with Incident Management with regard to establishing common Incident and Problem categories. Appropriate categories should be created both for recording reported Incidents, which should be in 'Customer terms', and for recording the finally detected causes, more likely to be expressed in 'IT terms'.
- If possible, establish a multidisciplinary team with, for instance, Problem Management, as coordinator, in order to involve as many different perspectives as possible in the investigation.
- Ensure that support specialists involved have adequate tools and diagnostic aids in order to be able to carry out their tasks effectively.

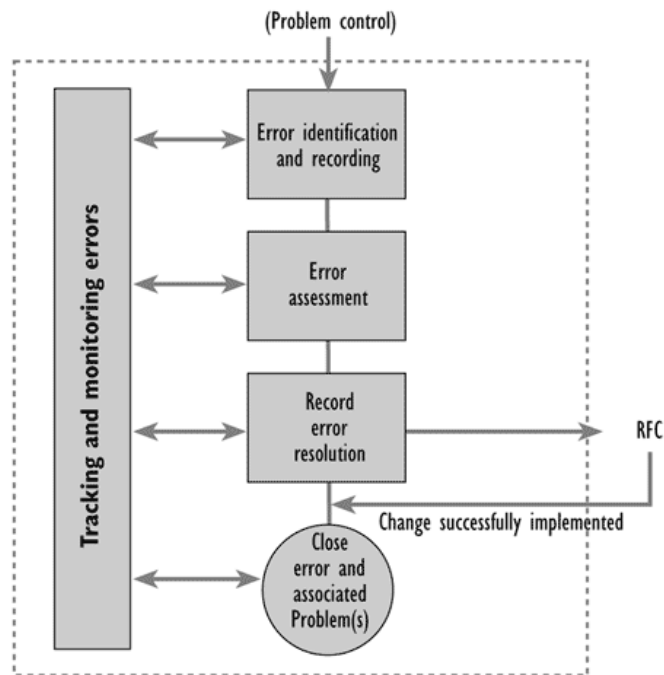
Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

- If a Problem does not involve an error in a system component but is caused by say, a general lack of User training, execute any resolution action and close the Problem record. Alternatively, a new CI record can be created - in this example for 'training Problems' - and the Problem can then be converted into a Known Error in the usual way. Ensure that the detected cause reflects the situation, e.g. lack of user knowledge, training.
- Investigation procedures during the Incident or Problem control process require that documentation on all products in the IT infrastructure is available to the process and to support staff for reference purposes. This includes documentation on the following:
 - Application systems;
 - Systems software;
 - In-house utility routines;
 - Networking hardware and software;
 - Overall configuration/network diagrams.
- In addition to product information, it is also necessary to have effective procedures to collect diagnostic data for Problem resolution. It is particularly important that support staff is familiar with these procedures, as any inappropriate use during an Incident can delay the resumption of normal IT services.
- You also need procedures that support and enforce your process requirements - and those procedures might include adequate training, qualifications etc.
- Often, support specialists are involved in both the Incident Management process and the Problem Management process. Keeping in mind the different goals of these processes (quick resolution versus structural resolutions), it can prove useful to assign specialists to both processes for a fixed percentage of their time, perhaps 80% to Incident Management and 20% to Problem Management. This prevents support specialists becoming fully absorbed by reactive Incident Management.
- During Incident and Problem investigations, Problem Management staff also require accurate records of recent Changes, because these may provide pointers to the cause

Error Control - Error control covers the processes involved in successful correction of Known Errors. The objective is to change IT components to remove Known Errors affecting the IT infrastructure and thus to prevent any recurrence of Incidents. Many IT departments are concerned with error control, and it spans both the live and development environments.

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

It directly interfaces with, and operates alongside, Change Management processes. The diagram shows the three phases of the error control process. The monitoring and tracking phase covers the entire Problem/error life-cycle.



Tips on Error Control - The following are points worth remembering in relation to Error control:

- Not all Known Errors need to be resolved. An organisation can decide to allow Known Errors to remain - for instance because the resolution is too expensive, technically impossible, or requires too much time to resolve. In practice, error control is concerned with selecting justifiable investments to resolve a Problem.
- Preparing an RFC is one of the responsibilities of error control. Resolutions are often found in technical adjustments. Don't forget that these RFCs may also need to include amendments to procedures, working methods and/or organisational structures.
- Consider creating standard error records, by specific device (CI) or by device category, for routine hardware failures. Use these to maintain a quick guide to the failure rate - although most information, such as mean time between failures (MTBF) and downtime, is produced from Incident data.

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<ul style="list-style-type: none"> • The rectification of many hardware faults is carried out under Incident control, and not via error control and Change Management. Any Changes to the specification of hardware should, however, be subject to the normal Change Management procedures. • Ideally, common tools should be used for Incident, Problem and error control in live and development environments. If this is not possible, because of the use of specific CASE tools in the development environment, it will be necessary to design and produce a viable transfer mechanism. • In practice, the level of detail usually required for development Configuration Management often precludes a viable shared system. The key thing is to share the data, especially in terms of passing to the live environment information on Problems, Known Errors and ongoing Changes that are being handed over with any new or changed software.
<p>Proactive Problem Scope</p>	<p>The activities described so far in Problem and error control are mainly reactive.</p> <p>Proactive Problem Management activities are concerned with identifying and resolving Problems and Known Errors before Incidents occur, thus minimising the adverse impact on the service and business-related costs.</p> <p>Problem prevention ranges from prevention of individual Problems, such as repeated difficulties with a particular feature of a system, through to strategic decisions. The latter may require major expenditure to implement, such as investment in a better network. Problem prevention also includes information being given to Customers that obviates the need to ask for assistance in the future. Analysis focuses on providing recommendations on improvements for the Problem solvers, e.g. provision of online technical tools may reduce the time taken to resolve Problems, thereby reducing the length of time that calls are outstanding.</p> <p>The main activities within proactive Problem Management processes are trend analysis and the targeting of preventive action.</p>

7. Management Reporting

<p>Incident Metrics</p>	<p>Regular reports to Management on Incident Management should include the following:</p> <ul style="list-style-type: none"> • Total numbers of Incidents; • Mean elapsed time to achieve Incident resolution or circumvention, broken down by impact code; • Percentage of Incidents handled within agreed response time (Incident response-time targets may be specified in SLAs, for example, by impact code); • Average cost per Incident; • Percentage of Incidents closed by the Service Desk without reference to other levels of support; • Incidents processed per Service Desk workstation; • Number and percentage of Incidents resolved remotely, without the need for a visit.
<p>Problem Metrics</p>	<p>Regular reports to Management on Problem Management should include the following:</p> <ul style="list-style-type: none"> • Number of RFCs raised and the impact of those RFCs on the availability and reliability of the services covered; • Amount of time worked on investigations and diagnoses per organisational unit or supplier, split by Problem types; • Number and impact of Incidents occurring before the root Problem is closed or a Known Error is confirmed; • Ratio of immediate (reactive) support effort to planned support effort in Problem Management; • Plans for resolution of open Problems with regard to resources: <ul style="list-style-type: none"> ○ People; ○ Other used resources; ○ Costs (against budget). • Short description of actions to be undertaken; • Number of Problems and errors split by: <ul style="list-style-type: none"> ○ Status; ○ Service; ○ Impact; ○ Category; ○ User group. • Total elapsed time on closed Problems; • Elapsed time to date on outstanding Problems;

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<ul style="list-style-type: none"> • Mean and maximum elapsed time to close Problems or confirm a Known Error, from the time of raising the Problem record, by impact code and by support group (including vendors); • Any temporary resolution actions; • Expected resolution time for outstanding Problems; • Total elapsed time for closed Problems.
--	---

Audits	<p>Process control requires periodic audits of all operations and procedures. These audits are intended to confirm that the Problem Management and support teams are adhering to defined procedures. The audits should analyse major problem reviews, and check:</p> <ul style="list-style-type: none"> • That reports are produced and analysed according to the agreed schedule; • A representative sample of Incidents, to verify that related Problems have been correctly identified and recorded; • A representative sample of Problems, to verify that Problems are diagnosed correctly and diagnosed within the prescribed period; • A representative sample of Known Errors, to verify that Known Errors are cleared by authorised Changes to CIs and within the prescribed period; • That thresholds for escalation have been adhered to; • A representative sample of records, for correctness and completeness; • That documentation is being maintained correctly - updates being distributed by Problem Management staff and executed by recipients; • That management reports are produced regularly and are meaningful; • For evidence of trend analyses and the identification of preventive actions; • Staff training records.
---------------	--

8. Incident & Problem Management Tool

Considerations	Tool requirements specific to the Incident Management process are thus:
-----------------------	---

Quick Guide:
ITIL Compliant Incident & Problem Management Implementation

	<ul style="list-style-type: none"> • Automatic Incident logging and alerting in the event of fault detection on mainframes, networks, servers and so on (possibly through an interface to system management tools) all modifications to the Incident record being registered in order to keep control; • Automatic escalation facilities so as to facilitate the timely handling of Incidents and service requests; • Highly flexible routing of Incidents as a basic requirement, because control staff may be located at multiple sites or they may be co-located at an operations bridge, and such a physical distribution may vary depending on the time of day; • Automatic extraction of data records from the CMDB of a failed item and affected items; • Specialised software: speed and effectiveness are major objectives of handling Incidents, and because achievement depends upon a very accurate level of Incident classification and successful matching at the point of alert, it is the classification-matching process that is an ideal application area for the use of software; • ACD (telephone) systems integration for automatically registering names and phone numbers of Users; • Presence of diagnostic tools/modules (i.e. Case-Based Reasoning) can help the diagnostic process.
--	---

9. Further Information

ITIL Information	<p>For more comprehensive information on ITIL Incident & Problem Management:</p> <p>See the ITIL website: www.itil-officialsite.com See the best practices website: www.best-management-practice.com</p> <p>Or</p> <p>Contact Advalue Management Services: info@advalueservices.com www.advalueservices.com</p>
-------------------------	--