Quick Guideline for ITIL Compliant

CONFIGURATION 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 an ITIL compliant process for managing configuration items 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.

PO Box 641
Orewa, Hibiscus Coast 0946
New Zealand

Ph/Fax: +64 9 424 5004
Email: Info@advalueservices.com
Web: www.advalueservices.com

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

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

Table of Content

1. INTRODUCTION 4

PURPOSE 4
INTENDED AUDIENCE 4
BACKGROUND 4

2. RELATIONSHIP WITH OTHER PROCESSES 5

RELATIONSHIP 5
ASSET MNGT & CONFIGURATION MNGT 6
APPLICATION AREAS 6

3. BENEFITS & POSSIBLE PROBLEMS 7

BENEFITS 7
POSSIBLE PROBLEMS 8

4. CONFIGURATION MANAGEMENT SCOPE 9

PROCEDURES 9
SCOPE 9
CONFIGURATION ACTIVITIES 14

5. MANAGEMENT REPORTING 15

KEY PERFORMANCE INDICATORS 15
METRICS 16

6. CONFIGURATION MANAGEMENT TOOL 16

CONSIDERATIONS 16

6. FURTHER INFORMATION 17

ITIL INFORMATION 17

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

1. Introduction

Purpose	The purpose of this guide is to provide a brief overview on how to establish ITIL compliant Configuration 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.

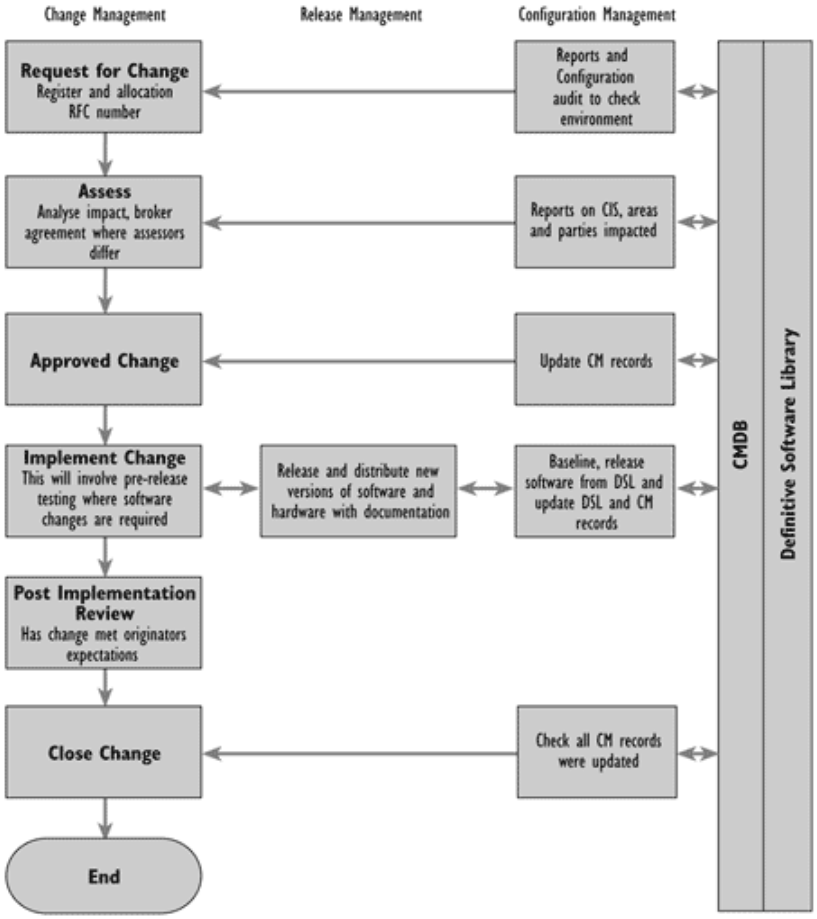
Intended Audience	The intended audience of this guide is: • ICT Managers; • Release Managers; • Helpdesk & support teams; • Application development & implementation teams; • Application test teams.

Background	All organisations require quality ICT services to be provided in the most efficient way. To be efficient and effective, all organisations need to monitor and control their ICT infrastructure & components and services. Configuration Management provides a logical model of the infrastructure and its components or a service by identifying, controlling, maintaining and verifying the versions of these components (in ITIL terms - Configuration Items (CIs)) in existence. The goals of Configuration Management are to: • Account for all the ICT assets and configurations within the organisation and its services; • Provide accurate information on configurations and their documentation to support all the other Service Management processes; • Provide a sound basis for Incident Management, Problem Management, Change Management and Release Management; • Verify the configuration records against the infrastructure and correct any exceptions.

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

2. Relationship with Other Processes

Relationship	Configuration Management interfaces directly with application development projects or ICT implementation projects, Change Management and Release Management in order to incorporate new and updated CIs in the live production environment. Handover of new or updated CIs by a project or supplier to the service organisation (e.g. 3rd party support organisation or internal Help Desk) should include accurate configuration records. It is recommended that Configuration, Change and Release Management processes will be developed in conjunction with each other and implemented at the same time.



Copyright © 2007-2009 - Advalue Management Services, all rights reserved

Asset Mngt & Configuration Mngt	Configuration Management covers the identification, recording, and reporting of ICT components, including their versions, constituent components and relationships. Items that should be under the control of Configuration Management include hardware, software and associated documentation. Given the definition above, it should be clear that Configuration Management is not synonymous with Asset Management, although the two disciplines are related. Asset Management is a recognised accountancy process that includes depreciation accounting. Asset Management systems maintain details on assets above a certain value, their business unit and their location. Configuration Management also maintains relationships between assets, which Asset Management usually does not.

Application Areas	Configuration Management is responsible for the following: • Planning Planning and defining the purpose, scope, objectives, policies and procedures, and the organisational and technical context, for Configuration Management. • Identification Selecting and identifying the configuration structures for all the infrastructure's CIs, including their 'owner', their interrelationships and configuration documentation. It includes allocating identifiers and version numbers for CIs, labeling each item, and entering it on the Configuration Management Database (CMDB). • Control Ensuring that only authorised and identifiable CIs are accepted and recorded, from receipt to disposal. It ensures that no CI is added, modified, replaced or removed without appropriate controlling documentation, e.g. an approved Change request, and an updated specification. • Status accounting The reporting of all current and historical data concerned with each CI throughout its life cycle. This enables Changes to CIs and their records to be traceable, e.g. tracking the status of a CI as it changes from one state to another for instance 'under development', 'being tested', 'live', or 'withdrawn'. • Verification and audit A series of reviews and audits that verify the physical existence of CIs and check that they are correctly recorded in the Configuration Management system.

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

3. Benefits & Possible Problems

Benefits	The real value of ICT assets is generally much greater than their capital value because of the part these assets play in supporting the provision of quality ICT services. The consequential losses to the organisation if these services are not provided can be very substantial. Configuration Management contributes to the efficient and effective delivery of ICT services by: • Providing accurate information on CIs and their documentation. This information supports all other Service Management processes; • Controlling valuable IC's - Configuration Management helps ICT management to know what its assets are supposed to be, who is responsible for their safekeeping, and whether the actual inventory matches the official one; • Facilitates adherence to legal obligations - Configuration Management maintains an inventory of all items of software within an IT infrastructure. CIs that come to light that are not on this list are not authorised and may well have not been paid for; • Financial and expenditure planning - Configuration Management provides a complete list of CIs. It is easy to produce from this list expected maintenance costs and license fees; maintenance contracts; license renewal dates, etc. By providing this information Configuration Management contributes to ICT financial planning. • Making software Changes visible - Such Changes can be used to trigger investigations by IT management into possible Changes that may be needed for data protection, license management and regulatory compliance; • Contributing to contingency planning - The CMDB and secure libraries facilitate the restoration of IT service in the event of a disaster, by identifying the required CIs and their location (provided, of course, that they are themselves properly backed-up); • Supporting and improving Release Management - Configuration Management information supports the roll-out across distributed locations by providing information on the versions of CIs and Changes incorporated into a Release; • Improving security - by controlling the versions of CIs in use. This makes it more difficult for these CIs to be changed accidentally, maliciously, or for erroneous versions to be added;

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

	• Providing Problem Management with data on trends - Such data will relate to trends in Problems affecting particular CI types, e.g. from particular suppliers or development groups, for use in improving the IT services. This information on Problem trends supports the proactive prevention of Problems.

Possible Problems	Design and implementation of ITIL compliant Configuration Management may experience the following problems: • CIs are defined at the wrong level with too much detail (so that staff become involved in unnecessary work) or too little detail (so that there is inadequate control); • Implementation is attempted without adequate analysis and design. The end result is, consequently, not what is required; • Tactical schedules are overambitious. Configuration Management may be perceived as a bottleneck if adequate time is not built into schedules to allow staff to carry out their duties. When Changes and Releases are being scheduled, past experience of the time taken to complete Configuration Management activities should be taken in to account; • Commitment is lacking. Without a firm commitment to the processes from managers, it is difficult to introduce the controls that some staff would prefer to avoid; • The process is perceived to be too bureaucratic or rigorous. Consequently, individuals and groups use this as an excuse for not following the process; • The process is routinely circumvented. Some people will try to circumvent Configuration Management in the interests of speed or with malicious intent. Attempts should be made to overcome this problem by making such people aware of the benefits of Configuration Management; • Processes are inefficient and error-prone. This is often the case where manual processes are in use. In almost all cases it is advisable to choose an electronic configuration management tool from the outset; • Expectations of what the tool can do are unrealistic. Staff and managers may expect a Configuration Management tool to deliver a total solution and end up blaming the tool for processes or people that appear insufficient for the task; • The chosen tool may lack flexibility. Problems can occur when the Configuration Management tool does not allow for new requirements or does not support all CI categories;

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

	• Configuration Management has been implemented in isolation. If Configuration Management is implemented without Change Management or Release Management, it is much less effective and the intended benefits may not be realised; • Expectations of what the Configuration Management process can do are unrealistic. Asset and Configuration Management cannot and should not be expected to make up for poor project management or poor acceptance testing; • Proper configuration control is not in place. For example, Configuration Management may be difficult where Users have the ability to purchase, download and install software from the Internet.

4. Configuration Management Scope

Procedures	The ITIL guideline indicates that within the Configuration Management process and procedures are needed for setting up and maintaining the following: • Configuration Management planning • Configuration identification & CI's • Controlling CI's • Configuration status accounting • Configuration verification and auditing • Configuration base lining • Configuration Management Database (CMDB) • Software and document libraries • License management

Scope	Configuration Management processes and procedures should include the following: • Configuration Management planning - The planning of Configuration Management should reference existing procedures and plans wherever possible, in order to keep things simple and to avoid duplication. A Configuration Management plan should define: ○ the purpose, scope and objectives of Configuration Management (and how it fits in with the organisation's overall Change Management and Configuration Management plan);

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

	○ related policies, standards and processes that are specific to the support group; ○ Configuration Management roles and responsibilities; ○ CI naming conventions; ○ the schedule and procedures for performing Configuration Management activities; ○ Configuration Management systems design, including scope and key interfaces. • Configuration identification - The IT infrastructure configuration should be broken down and uniquely identified to enable effective control, recording and reporting of CIs to the level that the business requires. Examples of the components that should be identified are: ○ Hardware (including network components where relevant); ○ System software, including operating systems; ○ Business systems – custom-built applications; ○ Packages – commercial off-the-shelf packages, standard products, and database products; ○ Physical databases; ○ Feeds between databases, applications and EDI links; ○ Software releases; ○ Configuration documentation, e.g. system and interface specifications, licenses, maintenance agreements, SLAs, decommissioning statement; ○ Change documentation, deviations and waivers; ○ Other documentation e.g. ICT business processes, workflow, procedures; ○ Network components; ○ Service Management components and records such as capacity plans, IT service continuity plans, Incidents, Problems, Known Errors, RFCs, etc. • Configuration structures - should describe the relationship and position of CIs in each structure. In addition to the infrastructure configuration structure, there should be service configuration structures that identify all the components in a particular service (e.g. the retail service).

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

- CI types and lifecycles:
  - Components should be classified into CI types because this helps to identify and document what is in use, the status of the items and where they are located. Typical CI types are: software products, business systems, system software, servers, mainframes, workstations, laptops, routers and hubs;
  - The life-cycle states for each CI type should also be defined; e.g. an application Release may be registered, accepted, installed, or withdrawn.
- CI relationships - the relationships between CIs should be stored so as to provide dependency information. For example:
  - CI is a part of another CI (e.g. a software module is part of a program, a server is part of a cluster) – this is a 'parent/child' relationship;
  - CI is connected to another CI (e.g. a desktop computer is connected to a LAN);
  - CI uses another CI (e.g. a program uses a module from another program, a business service uses an infrastructure server).
- Identification of software & document libraries - Physical and electronic software libraries should be uniquely identified with the following information:
  - Contents, location and medium of each library;
  - Conditions for entering an item, including the minimum status compatible with the contents of the library;
  - How to protect the libraries from malicious and accidental harm and deterioration, together with effective recovery procedures;
  - Conditions and access controls for groups or types of person registering, reading, updating, copying, removing and deleting CIs.
- Identification of configuration baselines - configuration baselines should be established by formal agreement at specific points in time and used as departure points for the formal control of a configuration. Configuration baselines plus approved Changes to those baselines together constitute the currently approved configuration.
- Naming conventions - Naming conventions should be established and applied to the identification of CIs, configuration documents and Changes, as well as to baselines, Releases and assemblies. The naming conventions should be unique and take into account the existing corporate or supplier naming/numbering

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

structures.

- Labeling CI's - All CIs should be labeled with the configuration identifier so that they can be easily identified. Plans should be made to label CIs and to maintain the accuracy of their labels.
- Control CI's - The objective is to ensure that only authorised and identifiable CIs are recorded in the CMDB upon receipt. The procedures should protect the integrity of the enterprise's data, systems and processes. When a Change is processed, the components being changed move through a number of planned/agreed states. Examples of states are: 'registered', 'fit for use', 'installed', 'in use', 'withdrawn', 'for disposal', 'disposed' and 'under Change'. Procedural and technical controls should be introduced to ensure that unauthorised Change is virtually impossible.
- Registration of new CI's and versions - The registration begins with items being ordered or with development being commissioned. Some organisations use their procurement process to ensure that CIs are added when they are ordered. Suppliers may also participate by labeling CIs prior to dispatch. In this way the ordering and delivery of CIs is under Configuration Management control.

- Registration of new software:
  - In-house developed software - For software developed in house, the point of 'receipt' is normally the point at which software is ready for operational acceptance. The use of a DSL is recommended, where all software CIs and their documentation are held in their definitive, quality-controlled state. Registration procedures should ensure that details of all authorised software and supporting documentation CIs are entered in the CMDB before the CIs are transferred from the development library into the DSL. The status of the CIs should be altered when they enter the DSL (e.g. from 'planned' to 'present');
  - Off the shelf software - ensure that all authorised new CIs are correctly registered in the CMDB before they are delivered and that the status of these CIs is changed as they are delivered, installed, tested and accepted. A check should be made that delivered CIs are authorised. Installation procedures should not commence until this check has been satisfactorily carried out;

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

- New CI's & versions from building and releasing - Good build and Release controls ensure that updated versions of software and hardware are built correctly and distributed to target environments that are compatible with the Release. Configuration Management with Release Management should record and report the versions of software, hardware and documentation that were the result of the build and Release processes.

- Updating CI's - The status of CIs changes as they progress from delivery to live use. Ideally, the CMDB should be updated automatically as the status of CIs and Releases changes. Associated documentation, such as test certificates and licenses, should be placed in a controlled document library.
- License Control - verify that secure master copies of software, documentation, data, licenses and agreements for supply, warranty and maintenance are lodged within the Configuration Management system or DSL.
- Updating record for decommissioned IC's - Scheduling and controlling the removal and disposal of CIs is often important for financial and security reasons. There should be procedures in place for decommissioning equipment or software so as to ensure correct disposal of the organisation's assets, and that the relevant records are updated and the status of the CIs promoted to the final state, e.g. 'withdrawn' or 'archived'.
- Protecting the integrity of configurations - To protect the integrity of the configuration and to provide the basis for the control of Change, it is essential that CIs, their constituent parts and their documentation be held in an environment that:
  - Is commensurate with the environmental conditions required (e.g. for computer hardware, software, data, documents, drawings etc.);
  - Protects them from unauthorised change or corruption;
  - Provides a means for disaster recovery;
  - In the case of software, data and documentation, permits the controlled retrieval of a copy of the controlled master;
  - Supports consistency between the as-built state of a configuration and the as-planned state;
  - Is secure and protected by up-to-date anti-virus software.

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

	• Configuration status accounting - Status reports should be produced on a regular basis, listing, for all CIs under control, their current version and Change history. Status accounting reports can be used to establish system baselines and enable Changes between baselines and Releases to be traceable. • Configuration verification and audit - Before a major Release or Change, an audit of a specific configuration may be required to ensure that the Customer's environment matches the CMDB. Before acceptance into the live environment, new Releases, builds, equipment and standards should be verified against the contracted or specified requirements. There should be a test certificate that proves that the functional requirements of a new or updated CI have been verified, or some other relevant document (i.e. RFC). Plans should be made for regular configuration audits to check that the CMDB is consistent with the physical state of all CIs, and vice versa. The configuration audits should check in addition that Change and Release records have been properly authorised by Change Management and that implemented Changes are as authorised. • CMDB back-ups, archives and housekeeping - Backup copies of the CMDB should be taken regularly and securely stored. It is advisable for one copy to be stored at a remote location for use in the event of a disaster. The frequency of copying and the retention policy will be dependent on the size and volatility of the IT infrastructure and the CMDB. Typically, the CMDB should contain records only for items that are physically available or could be easily created using procedures known to, and under the control of Configuration Management. When Configuration Management has been operating for a period of time, regular housekeeping should be carried out to ensure that redundant CI records are systematically deleted.
Configuration Activities	The planning of Configuration Management should reference existing procedures and plans wherever possible, in order to keep things simple and to avoid duplication. A Configuration Management plan should define: • The purpose, scope and objectives of Configuration Management (and how it fits in with the organisation's overall Change Management and Configuration Management plan);

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

	• Related policies, standards and processes that are specific to the support group;
	• Configuration Management roles and responsibilities;
	• CI naming conventions;
	• The schedule and procedures for performing Configuration Management activities:
	  ○ Configuration identification, control, status accounting, configuration audit and verification;
	• Interface control with third parties, e.g. Change Management, suppliers;
	• Configuration Management systems design, including scope and key interfaces, covering:
	  ○ CMDB;
	  ○ Locations of Configuration Management data and libraries;
	  ○ Controlled environments within which CIs are manipulated;
	  ○ Links and interfaces to other Service Management systems;
	  ○ Support tools (e.g. build and installation tools);
	• Housekeeping, including license management, archiving and the retention period for CIs;
	• Planned configuration baselines, major Releases, milestones, workload and resource plan for each subsequent period.

5. Management Reporting

Key Performance Indicators	The following Key Performance Indicators may be used for monitoring and reporting on the effectiveness of Configuration Management: • Occasions when the 'configuration' is not as authorised; • Incidents and Problems that can be traced back to wrongly made Changes; • RFCs that were not completed successfully because of poor impact assessment, incorrect data in the CMDB, or poor version control; • The cycle time to approve and implement Changes; • Licenses that have been wasted or not put into use at a particular location; • Exceptions reported during configuration audits; Unauthorised IT components detected in use.

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

Metrics	Regular management reports should be generated and these should include the following metrics: • Results of configuration audits; • Information on any non-registered or inaccurately registered CIs that have been detected and the corrective action; • Information on the number of registered CIs and CI versions, broken down by CI category, type and status (and possibly also by location or other CI attributes); • Growth and capacity information; • Information on the rate of change of CIs/CMDB and the DSL; • Details of any backlogs of Configuration Management work or any delays caused by Configuration Management activities, and proposed remedies; • Configuration Management staffing position; • The amount of authorised work done out of hours by other ICT services staff; • The results of efficiency/effectiveness reviews, growth reviews and audits of the Configuration Management system and proposals for tackling actual or potential Problems; • Data and analyses on the number of CIs by type (e.g. services, servers, routers, hubs, software licenses, desktop PCs, etc); • The value of CIs (or assets) • The location of CIs by business unit, support group or service. Consideration needs to be given, in consultation with the stakeholders, to the manner in which the management information is presented. In many cases, percentages, and graphical or pictorial representations, are more meaningful than bare numerical data.

6. Configuration Management Tool

Considerations	Many organisations have some form of Configuration Management in operation, but it is often paper-based. For large and complex infrastructures, Configuration Management will operate more effectively when supported by a software tool that is capable of maintaining a CMDB. The CMDB contains details about the attributes and the history of each CI and details of the important relationships between CIs.

Copyright © 2007-2009 - Advalue Management Services, all rights reserved

	Ideally, the CMDB should be linked to the DSL and other software libraries. Often, several tools need to be integrated to provide the fully automated solution across platforms. The Configuration Management system should prevent Changes from being made to an ICT infrastructure without valid authorisation via Change Management. The authorisation record should automatically 'drive' the Change. As far as possible, all Changes should be recorded on the CMDB at least by the time that the Change is implemented. The status (e.g. 'live', 'archive', etc.) of each CI affected by a Change should be updated automatically if possible. Example ways in which this automatic recording of Changes could be implemented include automatic updating of the CMDB when software is moved between libraries (e.g. from 'acceptance test' to 'live', or from 'live' to an 'archive' library), when the service catalogue is changed, and when a Release is distributed. Support tools should allow control to be maintained, for applications software, from the outset of systems analysis and design right through to live running. Ideally, organisations should use the same tool to control all stages of the life-cycle, although this may not be possible if all the platforms cannot be supported by one software tool. If this is not possible, then the IT infrastructure Configuration Management tool should at least allow Configuration Management information to be transferred from a software development Configuration Management system into the CMDB without the need for rekeying.

6. Further Information

ITIL Information	For more comprehensive information on ITIL Configuration Management: See the ITIL website: www.itil-officialsite.com See the best practices website: www.best-management-practice.com Or Contact Advalue Management Services: info@advalueservices.com www.advalueservices.com

Copyright © 2007-2009 - Advalue Management Services, all rights reserved