Ministry
of Defence

JSP 945
MOD Policy for Configuration Management

Part 2: Guidance

Foreword

This Part 2 Joint Service Publication (JSP) provides guidance in accordance with the policy set out in Part 1 of this JSP; the guidance is sponsored by the Defence Functional Authority for Technical, Quality and Standardization. It provides policy-compliant business practices which should be considered best practice in the absence of any contradicting instruction. However, nothing in this document should discourage the application of sheer common sense.

Preface

How to use this JSP

1. This JSP Part 2 is a guidance document and all MOD Organisations responsible for the procurement and through life support and operation of Defence capability will provide adequate resources to follow this configuration guidance.

2. This JSP contains guidance on Configuration Management (CM) across the MOD and is the authoritative document supported by further detailed guidance within the Knowledge in Defence (KiD) and Defence Logistics Framework (DLF). The guidance is not intended to undermine statutory instruments nor existing contractual standards. If the guidance conflicts with either of those, the statutory instrument or contractual standards will take precedence.

3. This JSP is published in accordance with the direction on all JSPs following adoption of the MOD's New Operating Model, set out in 'How Defence Works'.

Coherence with other Defence Functional Authority Policy and Guidance

4. Where applicable, this document contains links to other relevant JSPs, Standardization Agreements (STANAGs), Defence Standards (DEFSTANs) or Allied CM Publications (ACMPs), some of which may be published by different Defence Functional Authorities or Functions. Where particular dependencies exist, these other Defence Authorities have been consulted in the formulation of the policy and guidance detailed in this publication.

The list below also contains publications which whilst not all under MOD control or influence, provide further information on CM and its application.

Related Publication	Title
ACMP 2000	NATO Policy on CM
ACMP 2009	Guidance on CM
ACMP 2100	NATO CM Contractual Requirements for Materiel
AQAP 2110	NATO Quality Assurance Requirements for Design, Development and Production
AQAP 2210	NATO Supplementary Software Quality Assurance Requirements to AQAP 2110 or 2310
AQAP 2310	NATO Quality Management Systems for Aviation, Space and Defence Suppliers
DEFSTAN 05 - 057	CM of Defence Materiel
DEFSTAN 05 - 061	Quality Assurance Procedural Requirements
EIA649B	Standard for CM
ISO 9001	Quality Management Systems - Requirements

ISO 10007	Quality Management Systems – Guidance for CM
ISO 12207	Systems and Software Engineering – Software Life Cycle Processes
ISO 15288	Systems and Software Engineering – System Life Cycle Processes
ISO 90003	Software Engineering – Guidelines for the Application of ISO 9001 to Computer Software
ITIL V3	Information Technology Infrastructure Library
JSP 935	Software Acquisition Management for Defence Equipment
JSP 940	MOD Policy for Quality
JSP 945 Part 1	MOD Policy for CM
MAA RAs	Military Aviation Authority – Regulatory Articles
STANAG 4427	CM in System Life Cycle Management

Functional Management and Training

5. CM, together with Government Quality Assurance and Quality Management combine to build confidence that the capability supplied to the end user is fit for purpose.

The Defence Functional Authority for Technical, Quality and Standardization is also the Deputy Head of Profession for CM. Responsibilities include championing the Configuration profession across all civilian and military staff in the Defence workforce.

The Deputy Head of Profession sponsors the MOD civilian functional competencies for CM and supports the development of individuals to ensure capable, suitably qualified and experienced personnel in CM across the department. The Deputy Head of Profession also maintains a strategic overview of Configuration specific competences and training available across all MOD Top Level Budget areas, including the training courses for CM.

The two CM training courses are:

- Principles of Configuration Management.
- Configuration Management for Practitioners.

Further Advice and Feedback – Contacts

6. The owner of this JSP is the Defence Functional Authority for Technical, Quality and Standardization. For further information on guidance, or to provide feedback on the content, contact:

Job Title/E-mail	Project focus	Phone
DES-QCM-Policy-Helpline@mod.gov.uk	MOD Configuration Policy	Civ: +44(0)30679 32681 Mil: 9679 32681

Version History

Date	Version	Summary of Change
January 2016	1.0	Initial issue
June 2022	2.0	JSP updated to: • Correct minor errors • The previous version referred to the generic term of CM Plan. The new version differentiates between The Project CM Plan (the MOD intentions) and the Deliverable CM Plan (written under contract in accordance with Def Stan 05-057) • The previous version focused on CM of the product. The new version includes the requirement to include supporting documentation within CM.

Contents

1 Introduction

1.1 Precedence

This JSP contains guidance on CM across the MOD and is the authoritative document supported by further guidance within the KiD and DLF. It is not intended to undermine statutory instruments nor existing contractual standards. If the guidance conflicts with either of those, the statutory instrument or contractual standards will take precedence.

1.2 Configuration Management

CM is an enterprise-wide management activity that applies technical and administrative direction, focusing upon the capability's physical and functional characteristics to ensure conformance with requirements and to control the change of formally approved Configuration Baselines.

The MOD Organisation Team Leader is ultimately responsible for the implementation of CM policy and ensuring the 5 Key CM Principles are applied appropriately. These are CM and Planning, Configuration Identification, Configuration Change Management, Configuration Status Accounting and Configuration Audit.

A quick reference guide and CM processes map of the through life CM processes and how they fit together can be found in Chapter 7. It is advisable that these are read in conjunction with this guidance for ease of understanding and clarity.

A Baseline is a specific version of a Configuration Item (CI) or group of CIs that has been officially selected and formally approved at a particular point in the item's lifecycle. It could be requirements, specifications, or a set of drawings or a product. It is used as a reference point for further development and may also be used as a fall-back point should an update result in a negative outcome.

CM enables the documented status of the capability or system to be known at any time. Effective CM ensures that the internal and external interfaces and the various parts of a complete product or system remain compatible, including software, spares, test equipment, tools, ancillaries and support documentation[1].

CM must be considered at the beginning of the Concept Phase in the capability lifecycle as it provides traceability of the evolution of the user requirements through to the manufacture of equipment, software development, firmware development, Complex Electronic Elements (CEEs) development, in-service modification or the provision of a service. The objective of CM is to define the system's physical and functional characteristics by specifications, datasheets, drawings and related documentation. This will identify configuration to the lowest appropriate level, required to assure repeatable performance, safety, quality, reliability, availability, maintainability, traceability, interchangeability, supportability and interoperability.

[1] DEFSTAN 05-057 - CM of Defence Materiel.

1.3 Through Life

CM is the through life management of changes to the requirements, the product as-designed, as-built and as-maintained / operated standard. It enables traceability and a comparison of changes to a different product baseline. This ensures the as-built configurations conform to their documented requirements and are built to the correct version of those documents. The quick reference guide at page 17 illustrates the through life nature of CM, its activities and outputs for each stage of the Concept, Assessment, Demonstration, Manufacturing, In-Service and Disposal (CADMID) cycle.

1.4 Disposal

When a product (which may include hardware, software and associated documentation) has reached the end of its service life, it must be disposed of in accordance with any applicable security and environmental regulations or directives. The product for disposal must be accompanied by suitable configuration documentation to allow its disposal by stripping, destruction or sale in the most responsible and cost-effective manner.

1.5 Responsibility and Level of Effort

The MOD Organisation[2] will identify and describe those responsible with their respective levels of authority for the implementation of the CM process. The levels shall be dependent on:

a. the type and complexity of the capability and its associated documentation.

b. the product life cycle stage.

c. the interoperability and interaction of the configuration items or product.

d. the level of involvement of internal and/or external stakeholders.

e. who has responsibility / delegated responsibility for CM.

f. who is authorised to carry out configuration auditing.

The MOD Organisation Team Leader is responsible for ensuring that the appropriate level of CM effort is applied to the capability they are responsible for.

[2] MOD Organisation – within the MOD Organisational management structure this may be sited at TLB, Command, Section, Project or Delivery Team level, whichever is appropriate.

2 Configuration Planning

2.1 MOD CM Planning

CM planning shall be documented from project initiation through to project termination or disposal. At the beginning of the project's life, it will be a high- level strategy which will develop into a more detailed plan as the project evolves. The Project CMP (PCMP) will describe the purpose and scope of CM activities and explain how CM requirements for the project are to be managed, recorded and implemented. The complexity, its level of interoperability and the frequency of changes to the project will dictate the CM resources allocated to it. The PCMP will be produced by the MOD Organisation Team Leader. Depending on complexity and risk the MOD Organisation may choose to contract for a more detailed Deliverable CMP (DCMP). If this is the case, Def Stan 05-057 shall be invoked. All plans should clearly articulate the CM responsibilities of both the contractor as well as those of the MOD Organisation. The MOD Organisation Team Leader is responsible for ensuring the appropriate level of CM effort is applied to the projects they are responsible for.

2.2 The CM Plans (CMPs)

The MOD PCMP (mandated) and the DCMP (if required), will need tailoring to suit the project as stated above.

The list below shows points which may feature in both the DCMP and the PCMP. Generally, the DCMP will contain more detail whereas the PCMP may contain higher level principles.

a. The CM systems, tools (including software packages), procedures and resources used for Configuration Control Board (CCB), Configuration Control Committee (CCC), Local Technical Committee (LTC), etc. (the function of the Change Boards and their hierarchy are explained in more detail in para 4.3 and Annex A).

b. Provide a list of Stakeholders, Organisations and Committees as well as their individual and collective responsibilities / authority.

c. Detail the CM contractual requirements and policies. (Collaborative NATO projects are supported by ACMP 2100 which identifies NATO CM Contractual Requirements for Materiel).

d. Explain the scope and purpose of the work programme for modification / update implementation.

e. How Configuration Items (CIs) will be selected, identified and documented (Drawings, schematics, datasheets, etc.).

f. How the CIs will interface with each other and the wider system.

g. The configuration change management (CCM) procedures, meetings and communications.

h. Detail the version and change control record for the CMP and details of signatories.

i. The policy for managing subcontracted items if applicable.

j. The relationship of the CMP with other plans (Quality, Risk, Communication, other CMPs etc.).

k. The policy for maintenance, certification and re-certification of Government Furnished Assets, Equipment or Information (collectively known as GFA).

l. The policy for GFA modified by the contractor as part of the product's development process.

m. The policy for dealing with Commercial Off-The Shelf (COTS) and Non-Developmental Items (NDI). COTS or NDI shall be considered as CIs as a minimum and subjected to configuration control. If they are excluded from configuration control, the reasons why and the risks in doing so must be clearly stated in the CMP.

n. The arrangements for carrying out Configuration Status Accounting (CSA). This will include a list of approved configuration documentation, the status of proposed changes to the configuration, the implementation status of approved changes and a record of rejected change proposals.

o. The generation and maintenance of individual Configuration Status Records (CSR). The CSR should describe the status of the CI at any stage in its life cycle.

p. The frequency of CM reviews.

q. The process for handover from Under Contractor Control (UCC) to Under Ministry Control (UMC).

r. The requirement for and frequency of configuration audit.

s. The system for managing software licensing.

A PCMP template can be found in GEAR and a PCMP guidance document can be found in the CM section of the KiD.

3 Identification and Documentation

3.1 Functional Breakdown Structure (FBS)

A FBS is a modular decomposition of every activity which must be done to perform a particular mission or activity. It details the expected outputs which should be performed by the product not the physical attributes of the product or its component parts. It is a holistic activity providing a system overview which aids in system integration. It also provides a framework which will help in preventing the “under specification” of system requirements as all the functions are identified and the product or its components are aligned to these functions.

3.2 Product Breakdown Structure (PBS)

A PBS (also sometimes known as Bill of Materials) is sometimes used to illustrate how materials, components, sub-assemblies and assemblies come together to form the product or service. CIs are usually individual replaceable units or assemblies/sub-assemblies of the larger product. Software and CEEs are classified as a CI as they control the functionality of the product. The identification of CIs using a PBS illustrates the hierarchical inter-relationships and dependencies of the CI whilst allowing them to be managed separately. This is essential in allowing the product to develop and evolve whilst maintaining design integrity.

3.3 Configuration Items (CIs)

A CI (including software CI) must be clearly defined and identified in an appropriate manner. To fully identify an asset a NATO Stock Number (NSN) where applicable, a manufacture’s part number, and a serial number is required. The product’s documentation will include the CIs current build standard (baseline), a change log detailing a record of changes or change requests, the status of these requests and the differences between the different baselines. This information forms the Configuration Status Record (CSR).

3.4 CI Selection

The selection of an item as a CI is by agreement with the Design Organisation or by mutual agreement between the Delivery Team, the User and the Original Equipment Manufacturer (OEM). A CI must conform to strict criteria as detailed in the CM documentation.

Criteria for CI selection may include but not be limited to the following:

a. **Safety**. Where item failure would pose a risk to the user or other personnel or where failure would affect the safety of the product.

b. **Criticality**. Where item failure would result in product failure, product unavailability, or a loss of interoperability.

c. **Complexity**. Where the item is a complex or integral part of the product or has a long lead-time for manufacture.

d. **Costs and Purchasing**. Items which have significant financial impact or are difficult to procure / manufacture or items which are used in large quantities (typically, at least 10 per cent of the configured items electronic parts count).

e. **Functionality**. Where item failure would, affect the product or wider system resulting in it becoming unavailable / unable to achieve mission objectives or cause extensive and/or expensive maintenance and repair.

f. **Performance**. Where the failure of the item would prevent the acquisition of data to: evaluate system safety, availability, mission success, or the need for maintenance / repair.

g. **Duplication**. CI used more than once within a product.

h. **Interchangeability**. CI used in more than one product or project.

i. **Status as a Replaceable Item**. CI at different build standards which are interchangeable however control is required / items at different build standards which are similar however not interchangeable.

j. **Integrated Logistic Support (ILS)**. CI that has a limited shelf or operating life due to vibration, environment or thermal constraints. These CI may be replaced at predetermined intervals based on, reliability data, regulatory requirements or for economic reasons.

k. **Handling Storage and Transport**. CI requiring special handling, transportation, storage and / or test procedures.

3.5 Establishment of an Initial Product Baseline

CIs can be established at any time. However, this is usually done at the end of the Assessment stage with the establishment of an initial product baseline. These may be from Supplier recommendations as a result of system engineering analysis of the initial Systems Requirements Document. Further CIs are likely to be identified during product development up to the time that the product design configuration baseline is established at design freeze prior to manufacture.

4 Change Management

4.1 Configuration Change Management (CCM)

CCM is the process where configuration baselines are established, and all changes managed. These changes can be driven by a change in the requirement which would require a revision of the requirements documentation.

Changes can include documentation change for software as well as hardware. Changes may be driven by the need to mitigate risk, conform to legal or regulatory change, to improve quality, safety, address obsolescence, to improve availability, maintainability, reliability or interoperability, improve performance or reduce operating / support costs.

CCM ensures:

a. control of configuration baselines.

b. coherence between product and its documentation.

c. changes/updates if required to documentation are implemented.

d. dissemination of change.

e. stakeholders fully understand the impact of proposed change(s), the reasons for them and the benefits derived from change(s) to product.

f. stakeholders’ commitments and interests are considered.

g. updates to training or training equipment are managed.

h. updates to facilities (if required).

i. backward compatibility (if required).

j. all variants of product are managed when operating multiple versions.

k. interfaces/interoperability with other products, are not compromised by change(s).

l. recording and management of concessions, repairs, deviations or any other non-conformance.

m. product is still supported after change(s).

n. the management of information is in accordance with approved security procedures.

o. release management is controlled (including withdrawal of obsolescent / obsolete products).

4.2 Change Control Responsibilities

The Supplying Organisation, Design Organisation or OEM as appropriate is responsible under contract for configuration change management of the product up until delivery. The authority for Configuration Change Control usually but not always transfers to the MOD Organisation Delivery Team Leader post-delivery and the product is taken ‘Under Ministry Control. The authority to make product change now ultimately resides with the MOD Organisation Delivery Team Leader. If the product is a COTS item, DEFCON 502 should be used to inform the MOD post transfer of any obsolescence issues or changes to the CIs which may affect product supportability, changeability or interoperability.

If CM post-delivery is contracted out, it should be with the Supplying Organisation or a suitably competent Design Organisation. However, the authority for change and the risks still reside with the MOD Organisation.

4.3 Dispositioning Authority / Change Authority

A person or a group responsible for and authorised to make decisions on changes to the functional and physical characteristics of a product or configuration item are referred to as the Configuration Change (Dispositioning) Authority or more commonly the Configuration Control Board (CCB). The CCB usually sits at the Programme or Senior Responsible Owner level.

The Configuration Control Committee (CCC) is subordinate to the CCB and usually sits at the Delivery Team level with the Local Technical Committee (LTC) subordinate to the CCC. The LTC is made up of several Subject Matter Experts (SMEs) within the Delivery Team and makes decisions on minor changes. The CCB or its subsidiary committee, the CCC are not responsible for the day to day management of the individual CIs. These will be the responsibility of the MOD Organisation Delivery Team or its appointed support Organisation. The CCB and CCC authorises and manages major changes. The hierarchy of and levels of autonomy for these boards / committees should be detailed within the PCMP.

4.4 Meetings

The complexity, its level of interoperability, frequency and impact of changes to the capability will dictate the CM resources allocated to it. The attendees at meetings will change however attendees should be suitably empowered and able to make decisions on the CM proposals placed before them. Meetings will normally be composed of, but not be limited to the following individuals:

a. Chairman – MOD Organisation Team Leader for CCB, Delivery Team Leader for CCC or the CM focal point or someone with delegated authority for LTC.

b. MOD Organisation Team members.

c. MOD Organisation Commercial Officer.

d. MOD Organisation Finance Officer.

e. The Contractor.

f. The Design Organisation (if not the contractor).

g. Safety manager (If applicable).

h. Other stakeholders as required due to the nature of the Requests For Change (RFC).

i. Stakeholders from interfacing equipment (when required).

j. User.

k. Maintainer

4.5 Rationale for Change under Consideration by CCB / CCC/ LTC

There are various reasons for configuration change and the following is a sample list:

a. To comply with Legislative and regulatory change.

b. To reduce Risk and improve product safety.

c. To improve product’s performance.

d. To provide enhanced capability.

e. To address product’s obsolescence.

f. To increase spares availability.

g. Technology insertion.

h. To correct premature product failure (including preventative measures).

i. To increase product supportability.

j. To improve survivability.

4.6 Change Proposals

Engineering Change Proposals[3] (sometimes referred to as Configuration Change Proposals or Modification Proposals) should be uniquely identified and recorded prior to submission for evaluation to the Configuration Change (Dispositioning) Authority.

Change Proposals should typically include but not be limited to the following information:

a. Details of the CIs and related documentation which will be subject to change (including details of their title and current revision status).

b. Timescales for fitting / embodiment.

c. A description of the proposed change.

d. A list of other CIs and related documentation affected by the change.

e. Cost of the change.

f. Details of the Proposer and the date it was prepared.

g. Rationale for the change including the risk of doing / not doing change.

h. The category of the change.

i. To support the evaluation of change, additional details can include:

(1) Design, development and testing involved.

(2) Operational and maintenance documentation updates.

(3) The Training requirements.

(4) Products affected, e.g. in build, storage or retrofitting to existing products.

(5) The effects on spares and replacements.

(6) Safety assessment / recommendation.

(7) The Interfaces with other equipment.

4.7 Evaluation of Change

Evaluations of proposed changes must be documented and consider the risk / potential impact. The extent of an evaluation will depend upon the product complexity and change category. The Design Organisation will normally detail; the benefits of incorporating the

[3] DEFSTAN 05-057 - CM of Defence Materiel.

change, carry out the impact assessment detailing the risks of incorporating / not incorporating the change, the timescales for implementation and provide a fielding plan.

The Design Organisation and the Dispositioning Authority must determine the applicability of the Change Request and identify the product CIs requiring change. Other considerations should include the interchangeability of configuration items and the need for re-identification, the interfaces between configuration items, test and inspection methods, inventory, delivery activities and support requirements[4].

The Design Organisation should provide a detailed estimate of the costs and timescales for incorporating the change. They should also consider any knock-on costs if the change has an effect on the wider system or system of systems. Priority should be given to changes where safety is affected.

4.8 Disposition (Approval/Rejection) of Change Proposals

In-Service configuration change approval / rejection is provided by a meeting of the CCB or CCC, attended by the Design Organisation and relevant sub-suppliers. These SMEs can include but not be limited to:

a. Safety.

b. Integrated Logistics Support (ILS).

c. Quality Management.

d. Front Line Command (customer/user).

If the change is authorised the meeting will then consider:

a. Proposed start date and time for implementation.

b. Initiation of changes, including ‘changes to the configuration information being released to relevant interested parties’[5].

c. A list of further activities, which may need to occur because of the change such as training, location of the product, down time and shipping equipment.

d. Who will be responsible for carrying out or fitting / embodying the change, the Supplier, Design Organisation, another suitably qualified Design Organisation or the User.

[4] ISO 10007 - Guidance for CM.

[5] ISO 10007 - Guidance for CM.

4.9 Implementation and Verification of Change

When implementing and verifying authorised changes which are often referred to as Release Management, you must consider:

a. The release of product configuration information such as Modification instructions, withdrawal of existing product documentation and the issue of updated product documentation to stakeholders.

b. The mechanism for verification (audit) change to ensure it is complete (audits are to be carried out in accordance with ISO 10007 – Guidelines for CM).

c. The communication method by which the organisation responsible for change shall update the Dispositioning Authority / CCB / CCC to confirm that the change is complete (this is recorded in the Configuration Status Account for traceability – see para 5.1)

4.10 Categories of Change

In their simplest form, changes are classed as major or minor (standard or normal[6] for IT). The impact threshold, approval and classification of changes will be by agreement of the CCB. The classification will be dependent on the risk involved in the change or the impact of the proposed change. Major changes can be authorised at local level for expediency, however these changes would need to be ratified at a later date by the CCB / CCC. Minor changes are all other changes which are not major.

4.11 Concessions

A Concession is permission to use, embody, deliver or release a product that does not conform in full to contract requirements. A Concession can also apply prior to production / realisation (this process was formerly known as a Production Permit/Deviation)[7]. Concessions are to be restricted to a specific use, limited by time and quantity. They must specify that non-conforming characteristics may not violate specified limits[8]. Concessions are classified as either major or minor. Concessions should only be approved if there is a clear demonstrable benefit to the Authority.

Major concessions are authorised in accordance with the guidance contained in Def Stan 05-061 Part 1. These are non-conformances which may have an adverse effect on safety, supportability, reliability, interchangeability, life, strength, functioning of the product and specification compliance.

Minor concessions are all other concessions which are not major and ‘are to be recorded and controlled in accordance with the Contractor’s quality management system’.

[6] ITIL V3 - Information Technology Infrastructure Library.

[7] DEFSTAN 05-061 Part 1 - Quality Assurance Procedural Requirements.

[8] ISO 9000 2015 Edition - Quality Management Systems.

5 Status Accounting

5.1 Configuration Status Accounting (CSA)

CSA is ‘the CM activity concerning capture and storage of, and access to, configuration information needed to manage products and product information effectively’[9]. It is a data repository and may be a commercial software package however, it could be as simple as a spreadsheet. The quantity and detail of the information captured in the CSA will be dependent on the product’s complexity, its operating environment and the number of changes to the product. The Configuration Item Records (CIR) are stored in the CSA along with the results of configuration audits.

5.2 Configuration Item Record (CIR)

A CIR documents the lifecycle of a CI and should contain but not be limited to the following information:

a. Identifying reference or NATO Stock Number when applicable.

b. Product type (including if it is COTS / MOTS).

c. Product Name.

d. Version / revision number including date when revised and list of changes / impending changes.

e. Product description (drawing, specification or datasheet).

f. Who owns the CIR (Dispositioning Authority – UCC or UMC).

g. Supplier / manufacturer or OEM.

h. Interfacing equipment or system(s).

i. Location (if fitted as part of a system or system of systems).

j. A list of items used to support the product such as documentation, special tools, models, test equipment, handling equipment and packaging (some of which may also be CIs).

[9] MIL-HDBK-61A - CM Guidance.

6 Auditing

6.1 Configuration Audit

An audit is an independent assessment of products and processes, conducted by an authorised person to assess compliance with requirements. A configuration audit is likely to be required before the formal acceptance of a CI or before the product is formally handed over from the supplier to the MOD. It is not intended to replace other forms of verification, review, test or inspection, but will be affected by the results of these activities.

Two types of configuration audit are generally recognised as Configuration Management tools: Functional and Physical Audit, but in addition to these two types of audits, benefit maybe derived from Software Configuration Audit detailed in section 6.4.

6.2 Functional Configuration Audit (FCA)

FCA confirms the CI meets all the functional requirements (including performance). The FCA embodies a review of the CIs performance, to ensure it not only meets the specification but that there are no undesirable emergent properties / unintended functional characteristics. FCAs conducted early in the prototype stage, ensure the design will meet the requirements. FCA may be conducted before the Physical Configuration Audit (PCA) in an effort to reduce cost, if there is a possibility there will be product amendment / Modification because of the FCA.

An FCA should be conducted for each CI, or system, for which a separate development / requirement specification has been baselined.

Initial FCA should be undertaken, and the results recorded at the end of the assessment phase and during the demonstration phase. However, subsequent FCA can be carried out at any time in the product lifecycle.

Products evolve during development and this in turn leads to different builds prior to the final agreed build standard at design freeze / manufacturing baseline. Each build should be tested against the product requirements or function during the audit activity.

If prototype or pre-production models are not to be produced, then the test data can be collected from the testing of the first production item.

In the case of complex systems, FCA may be carried out in increments prior to a full system audit to ensure all of the requirements have been satisfied.

In cases where functional verification can only be completed after system integration and testing, the final FCA can be conducted alongside the PCA.

An FCA report should be produced to verify the CI meets the required functional specification.

6.3 Physical Configuration Audit

PCA involves the comparison of the manufactured item against the design documentation to ensure the physical characteristics and interfaces conform to the agreed product specification.

Initial PCA demonstrates:

a. completion of product development (design freeze / manufacturing baseline).

b. provides evidence for verification and validation that product has been built using:

   i. the correct materials.
   ii. to the required specification.

Further PCA will demonstrate agreed changes to product specification are complete or in-service modifications have been embodied.

A PCA should be established against the proposed production CI, (First Article Inspection) to assure the requirements are met, prior to the Product Baseline. The PCA should not be started unless the FCA of the CI has already been successfully completed or is being carried out concurrently with the PCA.

During the PCA any differences between the physical configurations of the selected production CI and the development CIs used for the FCA should be evaluated to assure no degradation of the functional characteristics of the selected CI.

The configuration change management control mechanism should be considered for audit to ensure it correctly controls all internal and external changes.

The PCA should:

a. determine the acceptance testing requirements prescribed by the documentation is adequate for the acceptance of CI production units.

b. include detailed audit of product design and production documentation, specifications, technical data, and tests utilised in the production of the CI, and consider operation and support documentation.

c. include an audit of the released product configuration documentation and quality control records to make sure the hardware – as built, or software – as coded (source or object) configuration are consistent with the documentation.

d. for Computer Software Configuration Items (CSCIs) or CEEs the product specification, Interface Design Document and Version Description Document should be considered by the PCA.

PCA considerations should assure:

a. product design is consistent with the CIR in the CSA.
b. release records identify all relevant product design information.
c. outstanding changes to the product are recorded within the CIR.

6.4 Software Configuration Audit (SCA)

In addition to PCA and FCA, benefit maybe derived from an additional software configuration audit.

The CM principles apply equally to software or hardware including all CEEs.

The following considerations should also be considered by SCA:

a. Compare detailed design descriptions with the software listing for accuracy and completeness.

b. Examine CSCI delivery media to ensure conformance with the software requirements specifications.

c. Review the source code for compliance with specified coding standards.

d. Ensure that the version (of software development tools or software produced as part of the product) used is the latest approved version under configuration control (including cloud stored software).

e. Review all required operation and support documents for completeness, correctness, incorporation of comments made at Critical Design Review (CDR), and adequacy to operate and support the CSCI(s).

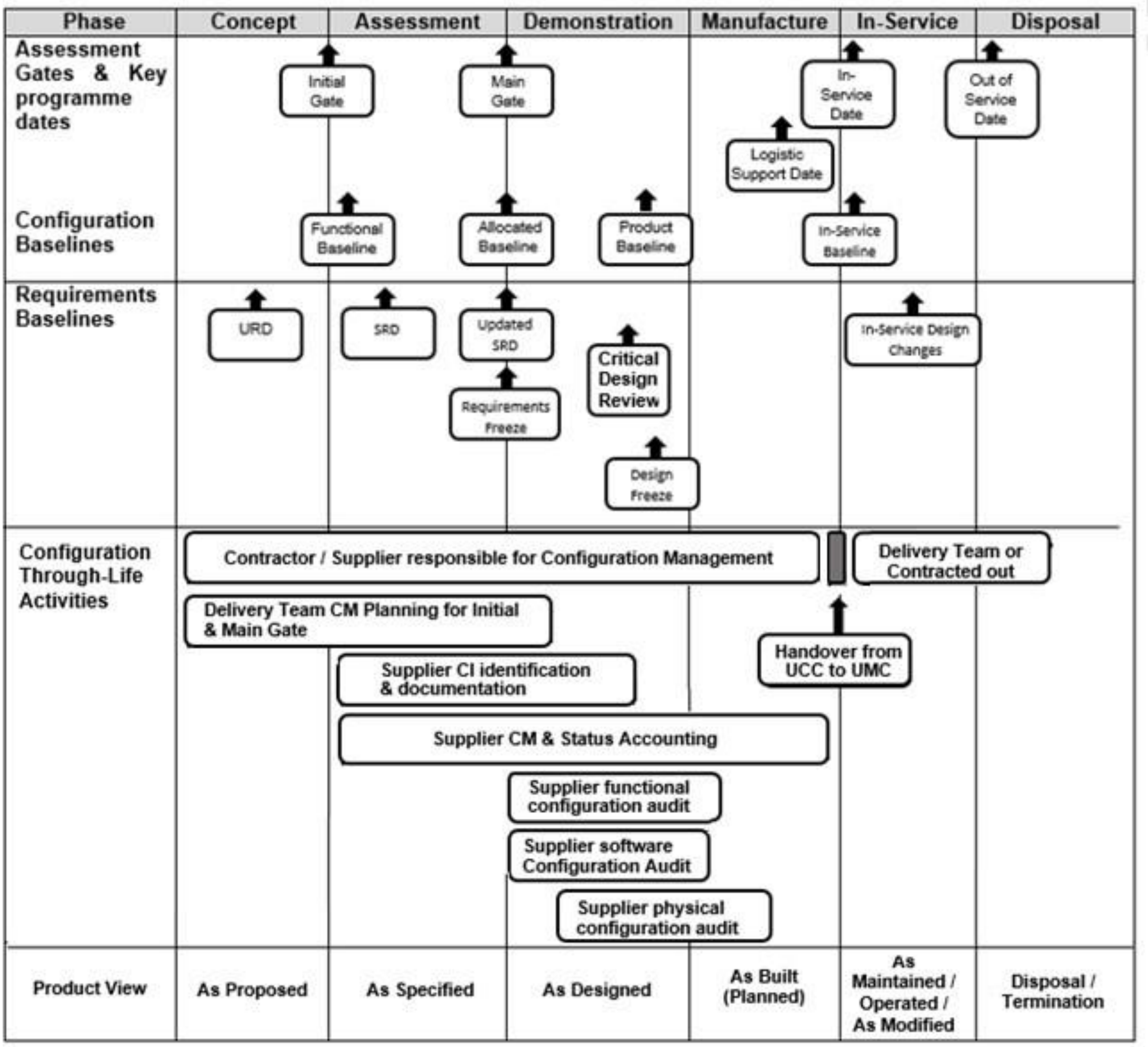
f. Ensure configuration documentation details the relationship of the CSCI to the parts, components or assemblies and properly describes the executable data. For Firmware, ensure the information describes the requirements for installation of the CSCI into the programmable parts or assemblies. Ensure the provision of sufficiently detailed documentation to allow for the procurement of follow-on firmware if necessary.

g. Using deliverable or MOD owned support software, assure by demonstration each CSCI can be generated. Carry out a comparison of the regenerated CSCI to the actual CSCI delivery media to ensure they are identical.

7 CM Guide and Process

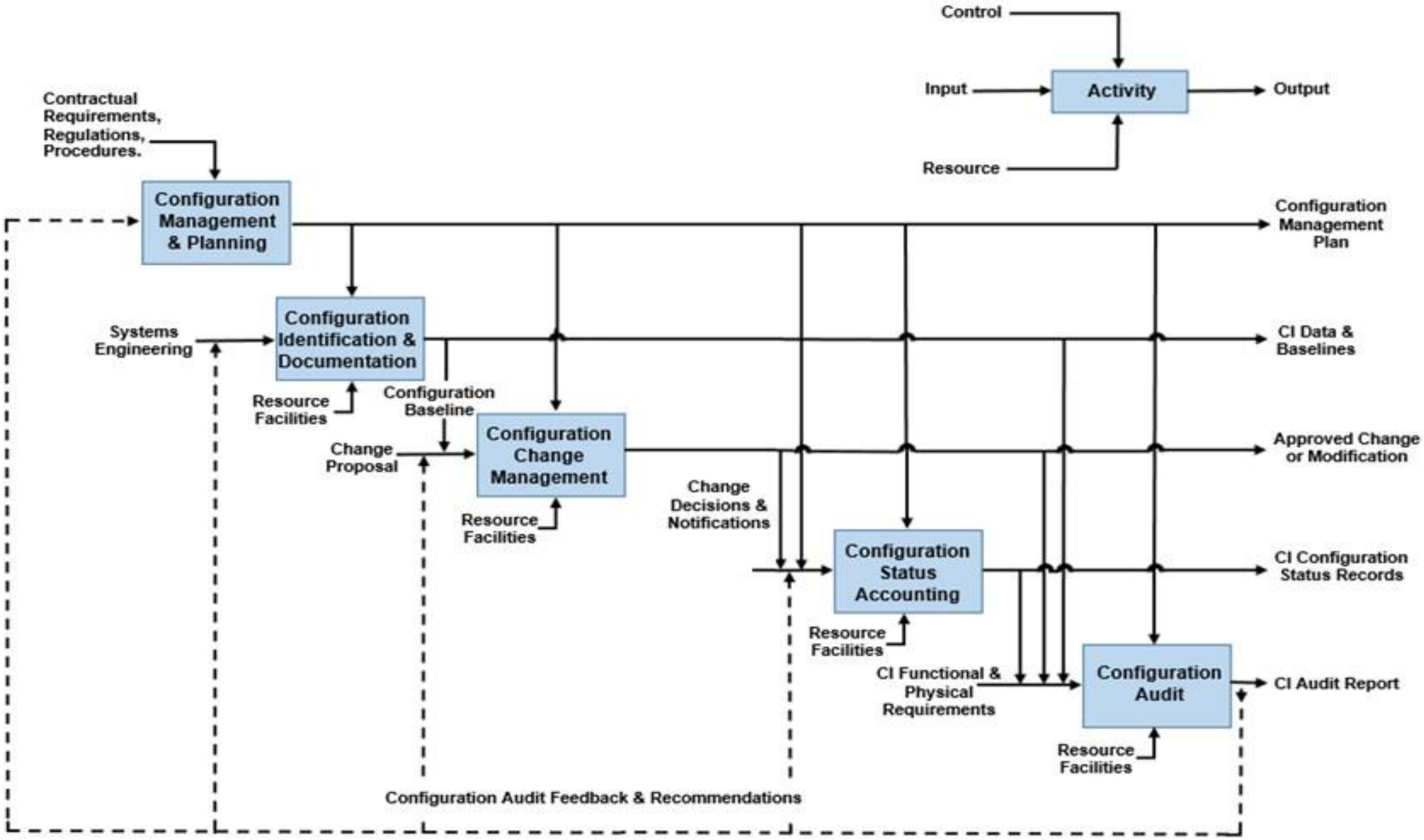
Quick Reference Guide

The Reference Guide shown relates more to Waterfall methodologies. Readers should be aware that other PM methodologies are also available. These include for example Agile methodology.



Phase
Concept
Assessment
Demonstration
Manufacture
In-Service
Disposal
Assessment Gates & Key programme dates
Initial Gate
Main Gate
In-Service Date
Out of Service Date
Logistic Support Date
Configuration Baselines
Functional Baseline
Allocated Baseline
Product Baseline
In-Service Baseline
Requirements Baselines
URD
SRD
Updated SRD
Requirements Freeze
Critical Design Review
Design Freeze
In-Service Design Changes
Configuration Through-Life Activities
Contractor / Supplier responsible for Configuration Management
Delivery Team or Contracted out
Delivery Team CM Planning for Initial & Main Gate
Handover from UCC to UMC
Supplier CI identification & documentation
Supplier CM & Status Accounting
Supplier functional configuration audit
Supplier software Configuration Audit
Supplier physical configuration audit
Product View
As Proposed
As Specified
As Designed
As Built (Planned)
As Maintained / Operated / As Modified
Disposal / Termination

CM Process



Control
Input
Activity
Output
Resource
Contractual Requirements, Regulations, Procedures.
Configuration Management & Planning
Configuration Management Plan
Systems Engineering
Configuration Identification & Documentation
CI Data & Baselines
Resource Facilities
Configuration Baseline
Change Proposal
Configuration Change Management
Approved Change or Modification
Resource Facilities
Change Decisions & Notifications
Configuration Status Accounting
CI Configuration Status Records
Resource Facilities
CI Functional & Physical Requirements
Configuration Audit
CI Audit Report
Resource Facilities
Configuration Audit Feedback & Recommendations

Glossary of Terms

Audit	An independent assessment of products and processes, conducted by an authorised person to assess compliance with requirements.
Baseline	A Baseline is a specific version of a Configuration Item that has been officially selected and formally approved at a particular point in the item's lifecycle. It may also refer to a product or a capability depending on where the system or system of systems CM boundary is set.
Critical Design Review (CDR)	A CDR normally occurs during the Demonstration phase prior to the transition to the Manufacture phase. The CDR assesses the technical solution to ensure it has an expectation of meeting the URD and the SRD.
Commercial-off-the-Shelf Item / Non Developmental Item	An item available in the commercial market place requiring no Modification to meet the requirements of the Authority
Computer Software Configuration items (CSCI)	Software that is selected for CM and is treated as a single article in the CM process.
Concession	A concession is permission to use, embody, deliver or release a product that does not conform in full to contract requirements. A concession can also apply prior to production / realisation (this process was formerly known as a Production Permit/Deviation
Configuration Management	An enterprise wide activity where the objective is to define the products physical and functional characteristics by specifications, datasheets, drawings and related documentation. This will identify configuration to the lowest appropriate level as well as establishing system / sub-system interfaces.
Configuration Management Plan	The document that formally describes the scope of CM, the CM Organisation, the CM procedures for the programme as mutually agreed by all stakeholders and those responsible for CM.
Configuration Status Accounting	Configuration Status Accounting (CSA) is the activity that results in records and reports that relate to product configuration information. (ISO10007).
Configuration Status Record (CSR)	The CSR should describe the status of the CI at any stage in its life cycle, including where appropriate, the current version of a CI.

Defence Lines of Development (DLoDs)	The DLoDs provide a mechanism for co-ordinating the parallel development of different aspects of capability that need to be brought together to create a real Military Capability.
Defence Logistics Framework (DLF)	The DLF is the central point for Logistics policy information covering the life cycle of a system. It is a software package accessed through the Defence Gateway (Login required).
Design freeze	The product design drawings are completed under contract and sealed. (Design Freeze) The supplier surrenders Configuration Change Authority control, and can no longer make changes without first consulting 'The Authority' or the Senior Responsible Owner responsible for in service design changes
Design Organisation	Can also be known as the Design Authority. Design Authority, an Organisation appointed by contract to be responsible for a design or Modification of a design, and for signing the Certificate of Design. The authority for acceptance of a design and any subsequent change to that design remains with the Authority.
Engineering Change Proposals	Formal documentation that is prepared to provide engineering information and other data in sufficient detail to support the evaluation of an engineering change.
Firmware	An ordered set of instructions and associated data stored in a way that is functionally independent of main storage, usually in a ROM.
Functional Breakdown Structure (FBS)	A FBS is a modular decomposition of every activity which must be done to perform a particular mission or activity. It details the expected outputs which should be performed by the product not the physical attributes of the product or its component parts.
Functional Configuration Audit (FCA)	An FCA confirms that the CI meets all the functional requirements (including performance).
Joint Service Publication (JSP)	JSP are a set of publications covering a wide variety of subjects, both administrative and technical.
Knowledge in Defence (KiD)	KiD defines how the MOD conduct, govern and control their defence acquisition process and is the primary bearer of all policy and guidance governing defence's project delivery and commercial functions.
Modification	An In-Service design change to a CI after the formal establishment of the

	Configuration Baseline, after the production drawings have been sealed.
MOD Organisation	Within the MOD Organisational management structure, this may be sited at TLB, Command, Section, Project or Delivery Team level; whichever is appropriate.
NATO Stock Number	A 13-digit numeric data string, which on its own uniquely identifies an Item of Supply in the NATO Inventory.
Physical Configuration Audit (PCA)	A comparison of the manufactured item against the design documentation to ensure that the physical characteristics and interfaces conform to the agreed product specification.
Product Breakdown Structure (PBS)	A product Breakdown Structure (PBS) is a hierarchical deconstruction of the product down to its component parts. It identifies the interrelationships and dependencies of the CI whilst allowing them to be managed separately.
Regulatory Authority	The Regulatory Authority / Agency / Body is the government agency responsible for applying autonomous authority over an area of activity in a supervisory or regulatory capacity.
Release Management	Release management is the process of managing, planning, scheduling and controlling a software build through different stages and environments, including testing and deploying software releases.
Senior Responsible Owner	The single individual with overall responsibility for ensuring that a project or programme meets its objectives and delivers the projected benefits.
Suitably Qualified and Experienced Person (SQEP)	A person who by virtue of their qualifications and experience in the appropriate field is deemed to be a competent person. A competent person is someone who has sufficient training and experience or knowledge and other qualities that allow them to carry out a particular activity in a safe manner.
System Requirements Document (SRD)	A System Requirements Document (SRD) is the structured and definition of the optimal system requirements (including constraints), bounding contracting and verification activities. It is the solution-focus response to the capability focussed User Requirements Document (URD) and is managed through life.

Under Contractor Control (UCC)	The responsibility and control of CM (CM) is with the contractor, Supplier or Design Organisation.
Under Ministry Control (UMC)	The responsibility and control of Configuration Management (CM) is with the Authority i.e. MOD.
User Requirements Document (URD)	User requirements define the ‘gap’ between the existing capability and the required capability. They are the outcomes, effects and services that the user needs to achieve or deliver through deploying or exercising the capability within an operational environment or process.

Annex A - Terms of Reference (Exemplar) for a CCB / CCC

The Terms of Reference (TORs) for the Configuration Control Board / Committee meeting are:

a. to assess and decide if the proposed changes to the product's design will deliver improvement with regard to cost, time and performance.

b. to seek stakeholder agreement for and authority to, proceed with the proposed changes.

c. to agree changes to the product delivery timescales.

d. to agree the product configuration change policy.

e. to provide authority for the contractor to proceed with approved changes.

f. to resolve conflict or problems between MOD, the contractor and the Design Organisation (if not the Contractor), arising from proposed change(s).

g. to define the limits of delegated authority for any subsidiary meeting or Committee.

h. to disseminate the decisions of, recommendations by and minutes of the meeting.

Membership

Routine members of the CCB / CCC are:

a. MOD Organisation Team Leader (CCB) or Delivery Team leader / in-service support lead (CCC) – Chairman.

b. Senior Engineer – Secretary.

c. Engineers as required.

d. Commercial Manager.

e. Quality Manager.

f. Finance Manager.

g. User / Front Line Command (FLC) representative.

h. Design Organisation / Equipment Manufacturer / Supplier representative.

i. Specialists or temporary attendees as required.

Frequency of Meetings

The frequency of meetings will be dependent on the project phase and set by the CCB / CCC chair.

Outputs

The CCB / CCC shall be responsible for the following outputs:

a. The CM Plan – Both PCMP and DCMP.

b. The approval or rejection of referred change proposals requiring authorisation.

c. Formal recording of minutes of CCB / CCC meetings.

Agenda

The routine agenda for the CCB / CCC is shown in table below.

Ser.	Agenda Item	Lead
1	Introduction	Chairperson
2	Review of previous minutes and actions	Secretary
3	Review of CM Process and CMPs	Chairperson
4.	Review of escalated items from CCC	Snr Engineer
5.	Review of proposed changes	Secretary
6.	Any other business	Secretary
7.	Date of next meeting	Secretary

Review Date

These TORs will be reviewed as necessary (minimum of 3 yearly).