Ministry
of Defence

# Configuration Management
## Aide Memoire

September 2017

# Policy and Precedence

MOD policy on Configuration Management (CM) is contained in JSP 945 Part 1. This is the MOD's authoritative policy document for CM and sets out the mandated CM processes which must be followed by MOD Organisations when procuring and supporting in-service products. This JSP derives its authority from the PUS Letter of Delegation to the Defence Authority for Technical & Quality Assurance and the associated Defence Authority Directive. CM is considered with Quality Assurance and Quality Management as one of the 3 sub-categories which collectively achieve the Management of Quality. It is a key engineering function and a critical enabler for equipment safety and supportability throughout the products lifecycle.

JSP 945 Part 2 provides the authoritative guidance on CM. It is supported by further guidance on the web-based Acquisition System Guidance (ASG) Governing Policy 2.5 and the Defence Logistics Framework (DLF). Both of these 2 web tools are accessed through the Defence Gateway (login required).

This aide Memoire is a quick reference guide aimed at providing limited information and should not be considered as an authoritative document. Please refer to JSP 945 if you require more detailed information on CM policy and guidance.

## Functional management and Training

CM along with Quality Assurance and Quality Management are the 3 elements which added together ensure the Management of Quality. The Defence Authority for Technical & Quality Assurance is also the Deputy Head of Profession for CM, and responsibilities include championing the configuration management discipline across all civilian and military staff in Defence. The Deputy Head of Profession also supports the development of individuals to ensure capable, Suitably Qualified and Experienced Personnel (SQEP) in CM are available across the MOD. The Deputy Head of Profession sponsors the MOD civilian functional competences for CM, and maintains a strategic overview of competences and training available across all MOD Top Level Budget areas, this includes the training courses for CM delivered by the Defence Academy. Currently there are courses for awareness and practitioner which are delivered throughout the year.

## Further Advice and Feedback – Contacts

DS&EQT provide help with CM Policy & Guidance on behalf of the Defence Authority for Technical & Quality Assurance. The information contained within this Aide Memoire is taken from JSP945 Parts 1 and 2 which are the authoritative documents for CM within the MOD.

Quality, Safety, & Environmental Protection (QSEP)
Director Safety & Environment, Quality and Technology
Elm 1a, #4127
MoD Abbey Wood
BRISTOL
BS34 8JH

Helpline: Mil: 9679 32681
Civ: 030 679 32681

**Email**: Destech-qsepqcm-pol-helpline@mod.uk

# 1. Configuration Management (CM)

CM is the process of managing change, the equipment or products that we support will almost certainly be subject to modification or change.  This is due in part to the extended periods that those products remain in-service necessitating change due to reasons such as obsolescence, technology insertion or to comply with legislative or regulatory changes.  However the changes may also be driven by emerging threats, the need to mitigate or nullify the effects of product deterioration due to ageing, corrosion or repair on repair. The changes may also take the form of in-service modification to: improve safety, reduce risk, to mitigate obsolescence, to improve performance the need to improve supportability, availability, reliability & maintainability or to resolve product defects.

## 1.1 What is the purpose of CM?

The purpose of CM is to understand and manage the impact of changes to the design baseline.  CM ensures that changes to the products physical or functional baseline design or its supporting documentation occur in a managed, controlled and auditable manner.  This makes sure that the design remains safe, relevant and complies with the requirements documentation.   Those responsible for implementing CM will change many times though out the products extended lifecycle.  It is important that product changes are documented to ensure the history of changes are recorded.  This ensures those currently responsible for CM can see the evolution of design, previous changes, there impact and prevents the repetition of past mistakes.

CM manages the through-life changes to the products as-designed, as-built and as-maintained standard. It enables changes and different build standards to be traced back to the system design and operational requirements at any given time throughout the products lifecycle.  CM also allows for the functional or physical attributes to be compared with the latest authorised product documentation set.  Thereby, providing assurance of the products operation and ensuring integrity of the products design.

Configuration Management (CM) defines 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, standardization, safety, quality, reliability, availability, maintainability, traceability, interchangeability, supportability and interoperability.

## 1.2 Under Ministry Control

The supplier will be responsible for managing changes to the product until it is formally handed over to the MoD.  It will then come "Under Ministry Control" (UMC) and the responsibility for changes transfers to MOD Senior Responsible Owner or Duty Holder.

## 1.3 Contracting for CM

CM in may be contracted out by invoking Defence Standard (DEFSTAN) 05-057 in UK Projects and Allied Configuration Management Publication (ACMP) 2009 in Multi National Projects) with the Supplier, OEM or some other responsible Design Organisation (see JP 945 Part 2, section 4.2).  In these instances, even though Configuration Management may be contracted out with the Supplier, OEM or Design Organisation, the MOD (Authority's) role as the final arbiter and authority for changes must be maintained for the duration of the contract.   The responsibility for CM when contracted out may reside with the contractor however, the risks and accountability will ultimately always reside with the MoD.

## 1.4 CM Responsibility

### 1.41 QCM policy

QCM policy is responsible for setting CM policy within the MOD on behalf of the Defence Authority for Technical & Quality Assurance.

### 1.42 MOD organisation

All MOD organisations who are responsible for the procurement and support of Military Capability should:

1. Develop and document a CM strategy detailing what CM activities they will carry out. This strategy will evolve into a more detailed CM Plan (CMP) as the product progresses through its lifecycle.

2. Confirm that the configuration status is defined and traceable back to the user requirements at acceptance prior to the product being taken “Under Ministry Control” (UMC). This usually takes place prior to manufacture and before the product or equipment enters service.

3. Assign suitably qualified and experienced personnel (SQEP) who will be responsible for the development, application and documentation of CM activities.

4. Manage the through-life configuration of the product invoking Defence Standard (DEFSTAN) 05-057 in the UK and Allied Configuration Management Publication (ACMP) 2009 in Multi National Projects where necessary in procurement and logistics support contracts (see JSP 945 Part 1, section 1.3.

It must be noted that CM is not a stand-alone process and changes to the products configuration can have a major impact on other processes such as safety management. The authority to make changes when the product is taken “UMC” ultimately resides with the MOD Organization Delivery Team Leader. However, changes are normally authorised by the responsible CM focal point utilising the appropriate committee unless there are Safety implications. In those cases, authorisation must be sought from the Duty Holder or Senior Responsible Owner.

For details of the different committees their autonomy and authority, please refer to JSP945 Part 2 Annex A.

### 1.43 The Supplier

The Supplier is responsible for fulfilling the contractual CM requirements including all sub-contractor CM activities and to ensure that their CM controls are effective in accordance with Defence Standard 05-057 (Configuration Management of Defence Materiel).

# 2. Principles of Configuration Management

There are 5 key principles to CM and they are:

1. CM Planning
2. Configuration Identification and Documentation
3. Configuration Change Management (Control)
4. Configuration Status Accounting
5. Configuration Audits

## 2.1 CM Planning

CM planning is a precondition to all future CM activities as without planning your approach will risk being unstructured and chaotic.  As every project undertaken is a unique enterprise with its own set of challenges, there is no CM planning template available that can be uniformly applied across all projects.  Therefore, you will need to tailor any template to suit your individual project.  A CM Plan (CMP) template can be downloaded from the CM section of the Acquisition System Guidance (ASG) website.

CM must be considered at the earliest stages in the capability lifecycle as it provides traceability of the evolution of the user requirements through to the eventual manufacture of the product, or provision of service. Changes to the CM strategy / CMP will be documented and recorded by the MOD Organisation throughout the lifecycle of the product from concept to retirement / termination.  When planning for CM, include only relevant CM activities which will add value to the process thereby reducing nugatory effort.

## 2.2 Identification and Documentation

Configuration identification is the activity which seeks to identify both hardware and software items.  Though the methods for identification of hardware and software items differ slightly, both use technical documentation

Configuration or Configured Item's (CI's) are sometimes referred to as assets, artefacts, entities or data sets. Whatever descriptor is used, configuration identification is a prerequisite for later configuration management activities as you need to know what assets you have if you are to manage them adequately.

A CI may be selected for a number of reasons such as safety, criticality, supportability or cost.

CI are identified, classified and grouped using an agreed method to ensure they are traceable and manageable.  Whichever system is used to select, identify and classify CI's, the CI must have a unique numbering or referencing system with enough supporting information for each item to distinguish them from similar items.

CI's will have their own Configuration record which comprises of the current built state, previous build states, a history of changes, details of rejected change proposals and any pending authorised changes.

What constitutes a CI or the level of deconstruction is set by the MOD Organisation Delivery Team who introduces the product and the Supplying or Design Organisation who ultimately provides the enduring support for the product.

For a more detailed list of reasons for selection of CI, please refer to JSP 945 Part 2 section 3.4.

## 2.3 Configuration Change Management (Control)

Configuration Change Management (sometimes referred to as Configuration Change Control / Configuration Control) is; the activities to manage and control changes to the products design after formal agreement of that design.  These take the form of changes or modifications to drawings, parts or software that have already been released and agreed during the products lifecycle.  A person or group responsible for and authorised to make decisions on changes to the functional, physical or software characteristics of the product or its CI are referred to as the Configuration Change or Dispositioning Authority.  They may also be referred to as the Configuration Control Board (CCB).  The CCC / CCB consider the impact of the proposed change on the CI and wider system ensuring any interfaces are maintained.

For a more detailed description of the CCB and its subordinate committees, please refer to JSP945 Part 2 section 4.3.

In software change control is referred to as Version control as you are modifying computer code which exists as a collection of 1's and 0's in a file.  You are not changing a physical or tangible product merely creating multiple versions of numerous files.  This means that the version control process must be very robust as software changes can occur simultaneously in multiple locations which are great distances apart (referred to as parallel development). Part of the change management approvals process is a snapshot of the product at a given time and is called a baseline.

### 2.3.1 Baseline

A baseline is the “as designed”, “as built”, or “as supported” product or system that has been reviewed and formally agreed upon. Baselines provide a reference point in the products design lifecycle from which further development progresses forward. They are useful should an update or change result in a negative outcome and a reversion to an earlier version is required. There are various reasons for changes such as to improve safety, reliability, maintainability, to comply with legislative change or technology insertion. Baselines are also described in software as different variants or versions. A record of the current and all previous baselines are recorded in the Configuration Status Account.

For a more information, please refer to JSP 945 Part 2 section 1.2.

### 2.3.2 Documentation

The requirement to formally record and document changes to the product is referred to as configuration documentation. Changes to the product will result in a need for revision to the products documentation set, to ensure it is reflective of the new product build state. The requirement and rationale for the changes will need to be recorded by means of a unique identifier and recorded in the CI record.

For a more detailed description of Configuration Item Records please refer to JSP945 Part 2 section 4.

## 2.4. Configuration Status Accounting

Configuration Status Accounting (CSA) is the capture and storage of configuration information (data). It must be stored in a method that it is retrievable and contain information suitably detailed to enable effective configuration management. The CSA contains a record of the status of pending, approved and embodied changes to the product or CI (known as the Configuration Item Record or CIR) and can therefore provide a picture of the CI at any given time.

For a more detailed description of a CIR please refer to JSP945 Part 2 section 5.2.

In the case of software ITIL (Information Technology and Infrastructure Library) state, software CI will evolve and as part of this evolution exist in various states. These states need to be defined as to what function they can and cannot perform. There are clear definitions for each state and release such as, registered, accepted, installed or withdrawn. ITIL regard CSA as a task of CM which records the status of a CI’s past, present or future (a CI pending a change).

There are many software tools to manage CM the following are just a few:

1. VSS – Visual source safe
2. CVS- Concurrent version system
3. Rational Clear Case
4. SVN- Subversion
5. Perforce
6. TortoiseSVN
7. IBM Configuration management version management
8. Razor

9. Quma version control system
10. SourceAnywhere

The 2 most used hardware or equipment CM tools used in the MOD are:

1. Windchill
2. CMPRO

CSA is a repository for information to answer queries relating to change, design problems, the past, present and any pending changes. CSA is more than just a CM activity, information retained within the CSA can be used to reduce risk within the product and wider project. This is because CM can provide the structure to identify and manage risks as the products design evolves

The CSA size will depend on how complex the product is or the number of changes to the product. The CSA can be as simple as an EXCEL spreadsheet for a simple product or in the case of the Dreadnought Class Nuclear Submarine a bespoke software application. In this case CM information is provided by the Design Organisation where both manufacturer and the MoD have access to the CSA with varying levels of authority to amend the information.

For a more detailed description of the CSA please refer to JSP945 Part 2 section 5.1.

## 2.5. Configuration Audit

A CM Audit is an independent inspection and verification of a systems design, operation or performance. Configuration Audits are carried out to assess consistency between the physical or functional configuration of the product and its document set. Initial audits are carried out to confirm compliance with the stated system requirements prior to handover of the product from the Supplier or Contractor (Under Contractor Control UCC to Under Ministry Control UMC). Further audits can / are carried out when the product is in-service. Configuration audits are also carried out after an upgrade to confirm the updated build state or periodically to assure conformance with the publications set. During In-service, responsibility for CM may switch from MOD to contractor for the duration of a modification or mid-life upgrade. However MOD would still retain the final say on configuration changes.

There are 3 types of CM audit. Functional, Physical and Software which are detailed below.

### 2.5.1 Functional Configuration Audit (FCA)

FCA, is an independent assessment of the complete product to measure its compliance with its stated requirements performance, characteristics and specification. In the case of complex equipment’s, incremental FCA may be carried out to ensure all the individual requirements have been satisfied.

For a more detailed description of FCA please refer to JSP945, Part 2 section 6.2.

### 2.5.2 Physical Configuration Audit (PCA)

PCA, are done to verify the “as built” configuration is the same as the “as planned” configuration and that this is commensurate with the products documentation set. An initial PCA is carried out upon completion of the products development phase (sometimes referred to as Design Freeze / Manufacturing Baseline).

A further PCA will be carried out prior to handover from UCC to UMC. A PCA can be carried out in-service to confirm the embodiment of a modification or to confirm the in-service product is compliant with the current authorised build standard as detailed in the products support documentation set.

For a more detailed description of PCA please refer to JSP945 Part 2 section 6.3.

### 2.5.3 Software configuration Audit (SCA)

The principles of CM apply equally to Software as to Hardware including all Complex Electrical Equipment's (CEE). SCA confirms the loaded software complies with: the detailed description in the software listing for accuracy and completeness, the software requirements specifications and the specified coding standards.

For a more detailed description of SCA, please refer to JSP945 Part 2 section 6.4.

## 3. Assurance

Quality is about consistently meeting the agreed standard for performance, cost and time in the delivery of Defence Capability. CM is one of the 3 activities (the others being Quality Management (QM) and Quality Assurance (QA) which collectively ensure the management of quality. Further information on QA and QM can be viewed in JSP940. Top Management across MOD are responsible for setting the acceptable standard for Quality, ensuring controls are effective and managing any associated risks. Assurance is all the activities through which justified confidence is provided that the standard is met (JSP 940 Part 1). Assurance for all users of CM can be provided by carrying out a Project Review & Assurance (PR&A) assessment. PR&A is an activity designed to deliver progressive assurance throughout the life of a project and prior to key investment decisions. QCM Policy aids in the delivery of PR&A by attending key stage review meetings, supporting ILS activities and reviewing the Support Solution Development Tool (SSDT) for CM Content.

## 4. Lifecycle Phases

The product whether it is hardware or software will be developed using some sort of lifecycle model. In this publication the model from ISO 15288 is used and comprises of 7 stages. These are Exploratory (Pre-Concept), Concept, Development, Manufacture, Production, Utilisation and Retirement. There will be overlap in these phases with activities being repeated to incorporate enhancements or modification as the product evolves. Approved Configuration or Baselines can be found in all phases (in some cases at the same time) dependent on the development model used such as evolutionary or incremental. CM allows the development of these different configurations to be used, managed and controlled. The application of CM will vary dependent on the products lifecycle phase and its complexity. Figure 1 is a simple table demonstrating some of the activities per phase which CM will impact upon. Requirements for example will evolve and this evolution needs to be traced and under version control (CM). Modification or technology insertion will need to be controlled should these changes result in a negative outcome and a reversion to an earlier build standard. CM using agreed baselines will control the introduction of these changes.

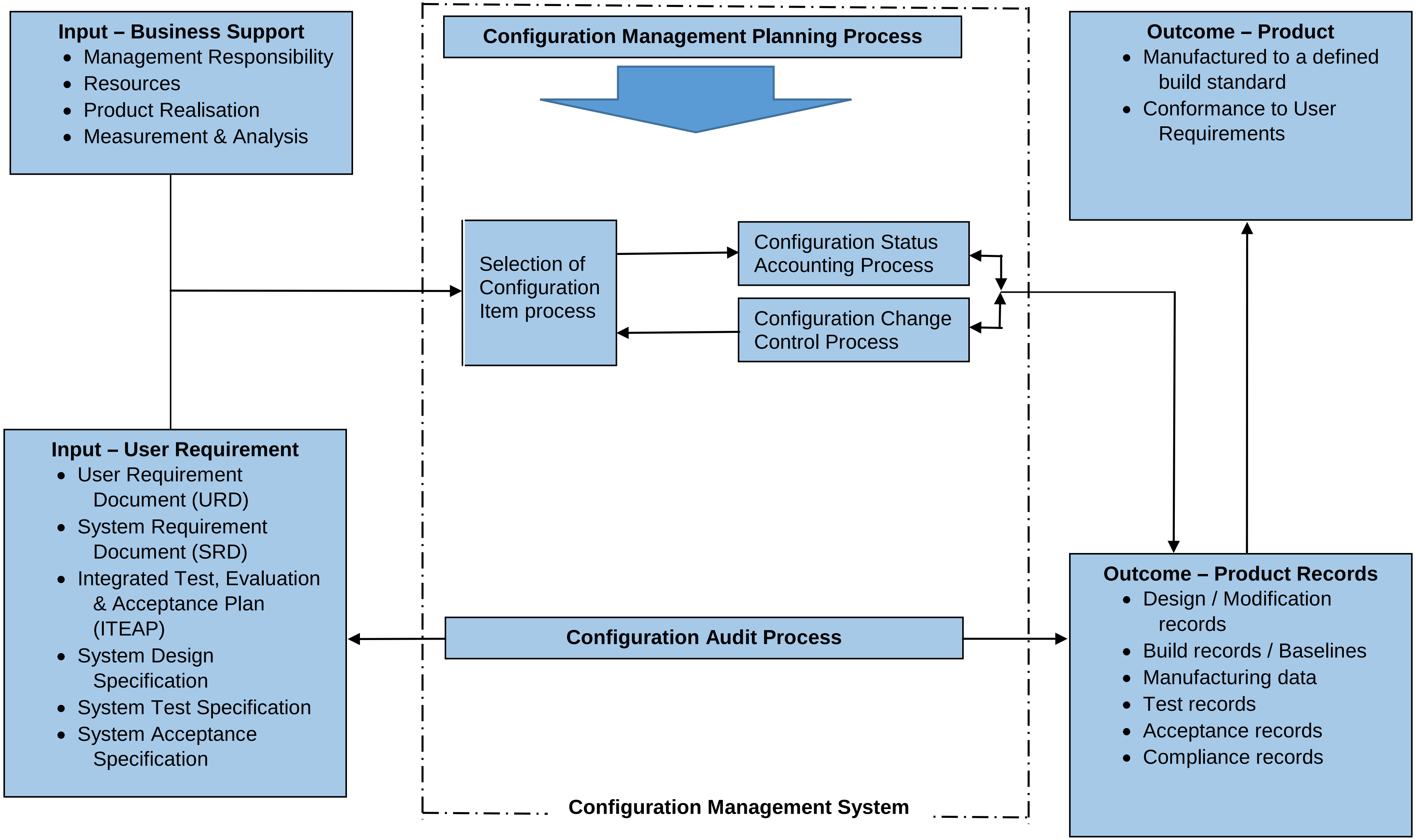
The table is not meant to be a definitive guide as the activities will vary dependent on the development model used and the complexity of the product.

## Figure 1

| Phase of the Product Lifecycle | | | | | | |
|---|---|---|---|---|---|---|
| Pre-concept | Concept | Development | Production | Utilisation | Support | Retirement |
| Define the user requirements and constraints.<br>Requirements analysis and feasibility study including technology readiness assessment. | Explore alternate solutions to satisfy stakeholder needs.<br>Create models or in some cases prototypes. | Development of selected engineering solution.<br>In software, identify source coding and build software | Build final product (may in some cases result in product modification to reduce production costs). | Deploy solution.<br>(Incorporate system into wider system if applicable).<br>Install software solution onto hardware | Maintenance, support and repair. Modification and technology insertion to extend life of product or reduce support costs.<br>Software updates and releases to resolve bugs and security issues. | Remove from service, disposal by sale or destruction in accordance with regulatory policies.<br>Replace software with newer version |
| Configuration Management Activities / Outputs | | | | | | |
| **CM Strategy** | | ← | | **CM Plan** | → | |
| Version control of product documentation such as requirements, analysis, reports, models possible prototypes. | | Version control of documentation. Identification of CI's. Generate CIR (CSR) and CSA.<br>. | Functional (incorporating Software if necessary) and Physical CM Audit Prior to handover from UCC to UMC. | CM to enable interface management when product is used as part of a system or system of system. | CCM to introduce modification. Status accounting to enable identification of alternate or replacement spares to resolve spares unavailability. | CM audit to identify hazardous materials or remove any restricted items such a secret software or technology. |

## 5. Configuration Management System

The Inputs and Outputs generated by a typical Configuration Management System are shown below.



**Input – Business Support**

- Management Responsibility
- Resources
- Product Realisation
- Measurement & Analysis

**Input – User Requirement**

- User Requirement Document (URD)
- System Requirement Document (SRD)
- Integrated Test, Evaluation & Acceptance Plan (ITEAP)
- System Design Specification
- System Test Specification
- System Acceptance Specification

**Configuration Management Planning Process**

Selection of Configuration Item process

Configuration Status Accounting Process

Configuration Change Control Process

**Configuration Audit Process**

**Configuration Management System**

**Outcome – Product**

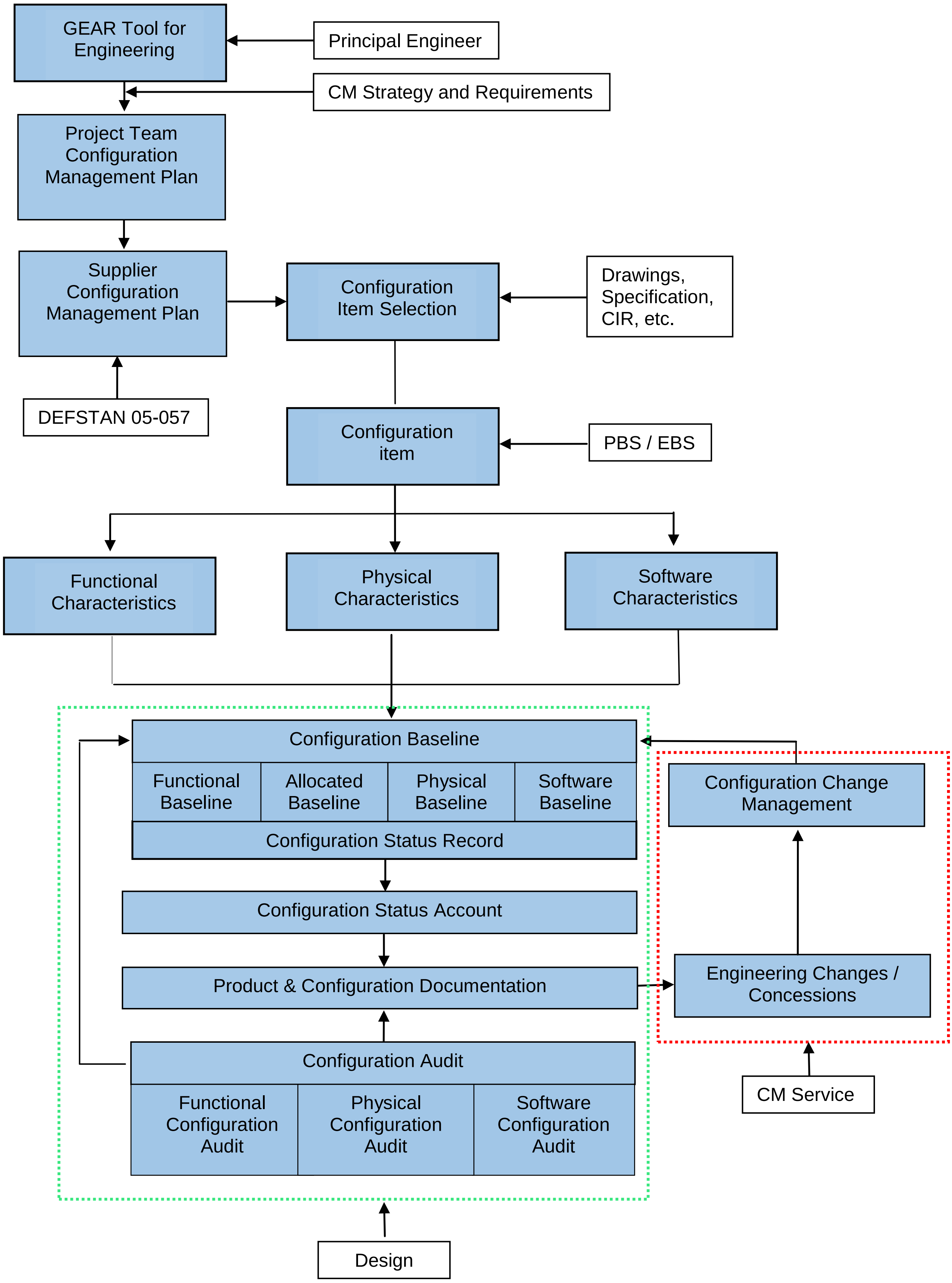
- Manufactured to a defined build standard
- Conformance to User Requirements

**Outcome – Product Records**

- Design / Modification records
- Build records / Baselines
- Manufacturing data
- Test records
- Acceptance records
- Compliance records

## 6. CM Activity in a MOD product lifecycle

A typical CM activity flow diagram is shown below.


GEAR Tool for Engineering
Principal Engineer
CM Strategy and Requirements
Project Team Configuration Management Plan
Supplier Configuration Management Plan
Configuration Item Selection
Drawings, Specification, CIR, etc.
DEFSTAN 05-057
Configuration item
PBS / EBS
Functional Characteristics
Physical Characteristics
Software Characteristics
Configuration Baseline
Functional Baseline
Allocated Baseline
Physical Baseline
Software Baseline
Configuration Status Record
Configuration Change Management
Configuration Status Account
Product & Configuration Documentation
Engineering Changes / Concessions
Configuration Audit
Functional Configuration Audit
Physical Configuration Audit
Software Configuration Audit
CM Service
Design

## 7. Informative Reference Table

The table below contains a list of standards and publication where further guidance on CM can be found.

| Related Publications | Title |
|---|---|
| JSP940 | MOD policy for Quality |
| DEFSTAN 05 - 061 | Quality Assurance Procedural Requirements |
| DEFSTAN 05 - 057 | Configuration Management of Defence Materiel |
| STANAG 4427 | Configuration Management in System Life Cycle Management |
| ACMP2000 | NATO Policy on Configuration management |
| ACMP2100 | NATO Configuration Management Contractual Requirements for Material |
| ACMP2009 | Guidance on Configuration Management |
| 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 |
| EIA649B | Standard for Configuration Management |
| MIL-HDBK-61A | Configuration Management Guidance |
| MAA RA’s | Military Aviation Authority - Regulatory Articles |
| ISO 10007 | Quality Management Systems – Guidance for Configuration Management |
| ISO 12207 | Systems and Software Engineering – Software Life cycle processes |
| ISO15288 | Systems and Software engineering – System Life Cycle Processes |
| ITIL V3 | Information Technology Infrastructure library |