

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**



**Ministry
of Defence**

**JSP 886
DEFENCE LOGISTIC SUPPORT CHAIN MANUAL**

**VOLUME 7
INTEGRATED LOGISTIC SUPPORT**

**PART 8.12
CONFIGURATION MANAGEMENT**

Version Number	Version Date	Version Description
1.0	23/06/09	Supersedes JSP 586 Volume 4.
1.1	15/07/11	Updated contact details.
1.2	14/02/13	Minor Changes to Format and POC.
1.3	24/06/13	Policy Statement and updated guidance to support the application of Configuration Management (CM) principles for contractual product development and In-Service configuration change. Addition of CM Support Maturity Levels and Domain CM Standards / Processes.
1.4	07/03/14	Part 5: Identification of CM activities for program review and ILS support.
1.5	16/02/15	Chapter 1, minor conceptual change (page 4 paragraph 1) and change to POC.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Contents

Contents	2
CHAPTER 1: CONFIGURATION MANAGEMENT	4
Context	4
Precedence and Authority	4
Mandated Requirement	5
Policy	5
CM Policy Statement	5
Key Principles	5
Ownership and Points of Contact	6
General	6
Definitions	7
CHAPTER 2: CONFIGURATION MANAGEMENT PROCESS.....	8
Configuration Management Responsibility	8
Configuration Management Planning	8
CM planning – Concept phase (Support to Initial Gate).....	8
CM planning – Assessment, Demonstration, Manufacture Phase (Support to Main Gate)	9
CM planning - In-Service and Disposal (Support to Modification programmes)	10
Configuration Identification and Documentation.....	12
Serial / Lot Numbering.....	13
Commercial off-the shelf (COTS) and Non-Developmental items	13
Product Configuration Information.....	13
Configuration Baselines.....	14
Configuration Change Management	18
Change Control - General	18
Change Control - Responsibilities through life	18
Change Control - Initiation, Identification and Documentation	19
Change Control - Evaluation	20
Change Control – Disposition (Approval / Rejection).....	21
Change Control - Implementation and verification of change	22
Change Control - Categories of Change	22
Change Control - Concessions.....	23
Configuration Status Accounting	23
Concept phase CSA	24
Assessment Phase CSA	24
Demonstration Phase CSA.....	24
Manufacture Phase CSA	25
Delivery to the Authority	25
In-Service Phase	26
Disposal Phase.....	26
Configuration Status Accounting - Records and Reports.....	27
Configuration Audit	28
Delivery Team interaction with Supplier Configuration Audit	29
Functional Configuration Audit	29
Physical Configuration Audit.....	30
Software configuration Audit.....	31
Final Conference	32
Configuration Audits of (Non-contracted) In-Service Change	33
Physical Configuration Audit (PCA) - Checklist.....	34
CHAPTER 3: CONFIGURATION MANAGEMENT GUIDANCE	35
Part 1: Configuration Management Plan – Recommended Contents	35
Part 2: Selection Criteria - Configuration Items	39
Part 3: Configuration Change Management Responsibilities (Example)	42
Objectives	42
Configuration Change Authority	42
Responsibilities.....	42
Composition.....	43
Configuration Manager	44
Part 4: Configuration Management (Support Maturity Levels)	45
Success Criteria	45

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Part 5: Configuration Management Activities for Program Review and ILS Support	48
Support Maturity Level 1 – User Requirements Definition, Concept Phase and Concept Technology Review	48
Objectives	48
Supporting Activities	48
CM Activities	48
Objective	49
Supporting Activities	49
CM Activities	49
Support Maturity Level 3 - Preliminary Design Review & Support to Main Gate	50
Objective	50
Supporting Activities	50
CM Activities & Contract Considerations	50
System Design Review (Non-Support Maturity Level)	51
Objective	51
Supporting Activities	51
CM Activities	51
Support Maturity Level 4 - Critical Design Review	52
Objective	52
Supporting Activities	52
CM Activities	52
Integrated Logistic Support	53
Manage Logistic Configuration	53
Acceptance of Support Recommendation	53
Support Maturity Level 5 and 6 Support Solution Validation, Logistic Support Date and Test Readiness Review (TRR)	54
Objective	54
Supporting Activities	54
CM Activities	54
Support Maturity Level 7 - In-Service Date & Deliverable Product Acceptance	54
Objective	54
Supporting Activities	55
CM Activities	55
Integrated Logistic Support and Acceptance	55
Support Maturity Level 8 - In-Service Support Review - Responsibility for revised capability and design integrity (Modification of Configuration Baselines)	55
Objectives	55
Supporting Activities	55
CM Activities	56
Configuration Status Accounting (CSA)	57
Functional & Physical Configuration Auditing	57
In-Service Contract Considerations	57
Support Maturity Level 9 - Product / System Disposal	57
Objectives	57
CM Tasks	58
Part 6: Definitions	59

Figures:

Figure 1: Configuration Management Process	9
Figure 2: Example of Product Structure	12
Figure 3: Configuration Information.	14
Figure 4: Baselines and the CADMID Cycle.	15

Tables:

Table 1 Contractual CM Standards and Domain In-Service Processes for CM (Example)	10
Table 2: Typical Status Accounting Information throughout the CADMID Cycle.	27
Table 3: Functional Configuration Audit Checklist.....	33
Table 4: Physical Configuration Audit Checklist.....	34

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

CHAPTER 1: CONFIGURATION MANAGEMENT

CONTEXT

1. The MOD acquires products which may be subject to alterations and updates throughout a project life-cycle. Therefore, it is essential that the product or system performance, physical and functional attributes can be compared with the design and operational requirements at any time.
2. Configuration Management (CM) is a management activity that enables the documented status of the product or system to be known at any time. The application of through life CM can ensure a disciplined approach for product development and maintain design integrity through life.
3. The identification of Configuration Items (CIs) within a product breakdown structure and associated product configuration information can provide the framework for structured arguments that underpin the product / system safety case.
4. Configuration Management supports the Requirements Management role for control, monitoring and administration of capability requirements; by tracking the implementation of the requirements. The evaluation of CI Configuration Baseline information against requirements documentation and use of Functional and Physical Configuration Audits can help to assure that capability requirements are met.
5. Configuration Management supports the Management of Design through life in JSP 886, Volume 7 Part 10 and the configuration of Integrated Logistic Support products as expressed in JSP 886 Volume 7 Part 2, Chapter 2.
6. CM strategies and planning by the Delivery Team and Supplier can be used to provide the basis for the assurances required by the Support Solutions Envelope (SSE), Governing Policy 2.5: Configuration Management; see JSP 886 Volume 1 Part 3.
7. The lack of Baseline configuration information can lead to the need for costly corrective action to establish the required information for the continued use, or further development, of a particular product or system. The investment for CM is returned by reductions associated with the costs for intervention, corrective action, risk and possible liability.

PRECEDENCE AND AUTHORITY

8. When ever there is a conflict between this document and the contractual standards identified in Paragraphs 13 and 14, the requirements of the contractual standards take precedence.
9. One of the roles of the MOD Quality Assurance Authority (QAA) is to define CM Policy requirements, for MOD organisations or individuals in the Acquisition of defence equipment through life.
10. Quality and Configuration Management (Policy) as the executive arm of the MOD QAA sets a framework of CM policy, contractual standards and guidance for the Acquisition community. CM Policy is detailed within this JSP 886 Volume and within the Acquisition Operating Framework.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

11. The Delivery Team Leader is ultimately responsible for the implementation of Configuration Management Policy for the duration of the project lifecycle and must appoint competent personnel to ensure effective application of through life CM policy.

MANDATED REQUIREMENT

12. To meet the MOD duty of care obligations, product configuration information shall be provided or made available with all products, systems and equipment Configuration Items.

POLICY

13. UK National programs requiring contractual product design and development should invoke Defence Standard 05-57: Configuration Management of Defence Materiel within Invitations to Tender (ITT) and subsequent contracts.

14. To fulfil the agreements in [STANAG 4159](#) and [STANAG 4427](#), Joint International programmes requiring contractual product design development should invoke the [Allied Configuration Management Publications \(ACMP - 1 to 6\)](#) in ITT and contracts.

15. Although Configuration Management may be contracted with a Supplier - Design Organisation, the Authority's role as the Decider with an Industry role as the Supplier must be maintained through out the life of the contract, including availability type contracts where airworthiness and duty holder responsibilities must be fulfilled.

16. The aims of the following CM Policy Statement must be considered through life:

CM POLICY STATEMENT

17. All requirements generated by the Authority for output based specification are to be developed under a change management system for contractual baseline.

18. All platform systems and components that are to be owned and operated by the Authority and designated as Configuration Items (CI)s; shall be designed, developed and produced under a formal configuration change management system and delivered against a formally recorded and approved configuration baseline.

19. Product CI configuration information is to be made available for the Authority's In-Service requirements.

20. Change to the delivered product Configuration Baseline is to be established under a formal configuration change management system to ensure the integrity of design In-Service.

KEY PRINCIPLES

21. Configuration Management is a management activity that applies technical and administrative direction, focusing upon the product physical and functional characteristics to ensure conformance with requirements and to control the change of formally approved Configuration Baselines. Operational information is contained in Configuration Documentation and realised in the product or system design and supporting information. The use of the inter-related CM principles is detailed in Chapter 2.

22. The Acquisition process usually requires an Industry Design Organisation to be responsible for product or system development; therefore CM is often managed by

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Industry under contract, on behalf of the Authority. Within this arrangement the Delivery Team must ensure that the delivered product / system will have a formally recorded and approved Configuration Baseline.

OWNERSHIP AND POINTS OF CONTACT

23. The owner of this Policy is Director Joint Support Chain (D JSC). Head of Supply Chain Management (Hd SCM) is responsible for the management of JSC policy on behalf of D JSC. The policy sponsor for this document is. DES TECH-QSEP QCM-Pol-SkC4.

24. Enquiries concerning the content of this instruction should be addressed as follows:

25. For enquiries on the Technical content to the policy sponsor:

DES TECH-QSEP QCM-Pol-Int6
Tel: 07760 990522

26. For enquiries on accessibility and presentation:

ACDS LOGOPS-Def Log Pol-JSP886 (MULTIUSER);
Tel: Mil 9679 Ext 80953. Civ: 030679 80953
Associated Standards, Guidance and References

GENERAL

27. The following Associated Standards, Guidance and References apply:

- a. Defence Standard 05-57: Configuration Management of Defence Materiel – Issue 5, dated June 2005.
- b. STANAG 4159, Edition 2 Amendment 1: NATO Configuration Management Policy and Procedures for Multinational Joint Projects.
- c. STANAG 4427, Edition 2: Introduction of Allied Configuration Management Publications.
- d. BS ISO 10007:2003: Quality Management System: Guidelines for Configuration Management.
- e. DEFCON 117: Supply of Documentation for NATO Codification.
- f. Defence Standard 05-10: Product Definition Information.
- g. Defence Standard 05-61 Part 1: Concessions.
- h. JSP 886, Volume 7 Part 2: Chapter 2: ILS Management.
- i. JSP 886, Volume 7, Part 10; Chapter 2: Manage Design Through Life.
- j. JSP 886, Volume 7 Part 8.14: Management of Items Requiring Special Identification.

Air Environment:

- k. MAA Regulatory Articles: 5000 Series.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- I. Maintenance Airworthiness Process (MAP) – 01, Issue 4 dated Sep 12.

Maritime Environment:

- m. BR 1313: Maintenance Management in Surface Ships: Chapter 4: Configuration Management and Ship Fit Definition.

- n. BRd 8593(17): Addition and Alteration (A&A) Procedures and Modifications in Surface Ships.

Land Environment:

- o. JSP 886 Volume 5, Part 2A: Configuration Management, Land Modifications.

DEFINITIONS

- 28. See Definitions and Abbreviations in Chapter 3 Part 6.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

CHAPTER 2: CONFIGURATION MANAGEMENT PROCESS

CONFIGURATION MANAGEMENT RESPONSIBILITY

1. A Configuration Change (Dispositioning) Authority¹ must be identified at all times throughout the product lifecycle to make decisions on product configuration as defined in the requirements for design, realisation, verification, operation and support.
2. The Configuration Change Authority can also be known as the Configuration Control Board (CCB) and should include interested stakeholders.

CONFIGURATION MANAGEMENT PLANNING

3. Configuration Management (CM) planning should identify the processes, procedures, responsibilities and authorities for the effective application of the CM principles within the context of the contractual and project lifecycle requirements.
4. The programme complexity and nature must be considered by CM planning to enable the effective and efficient application of the following CM principles:
 - a. Configuration Identification and Documentation.
 - b. Configuration Change Management.
 - c. Configuration Status Accounting.
 - d. Configuration Audit.
5. CM planning should be controlled and approved.
6. The requirement for typical CM Plan in Chapter 3, Part 1 should be followed while considering the planning guidance below. The interaction of the CM principles indicated by the CM Process, Figure 1, should also be considered.

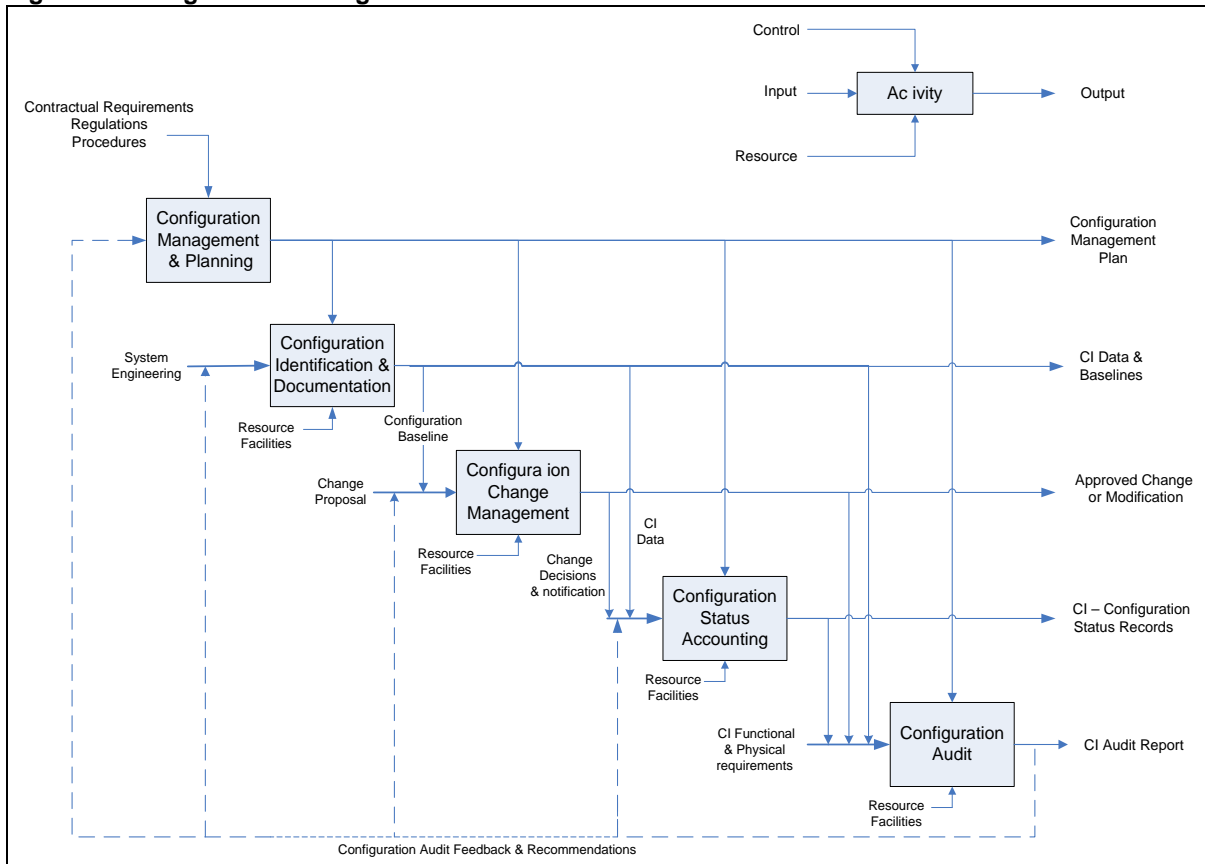
CM PLANNING – CONCEPT PHASE (SUPPORT TO INITIAL GATE)

7. Concept Phase planning should identify the CM processes required from project initiation to the beginning of Assessment Phase. At this stage of the project lifecycle, this planning should include a CM strategy of management intent for the subsequent Assessment Phase through to product delivery.
8. The CM strategy should include the relevant CM contract standards for Invitation to Tender (ITT) together with supplier assessment criteria that may include the need for high level CM planning from the ITT respondents.
9. CM planning should identify the process / procedure(s) to approve and authorise the release of the User Requirements Document (URD) for development of the System Requirements Document (SRD).

¹ Dispositioning Authority - A person or group of persons, assigned responsibility and authority to make decisions on product configuration as defined in the requirements for product design, realisation, verification, operation and support (ISO 10007).

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Figure 1: Configuration Management Process.



CM PLANNING – ASSESSMENT, DEMONSTRATION, MANUFACTURE PHASE (SUPPORT TO MAIN GATE)

10. During the Assessment Phase, the product / system design will be developed and baselined for manufacture and delivery. Therefore the CM planning should identify the procedures, responsibilities and authority for CM up to delivery of the product In-Service.

11. Delivery Team CM planning for Main Gate should include:

- a. CM contractual standards and In-Service processes specific to each domain (see Table 1 below).
- b. The process for seeking Front Line Command (customer) engagement when the requirements of the URD are affected by Supplier non-conformances against the SRD.
- c. The interaction of the Delivery Team with the Supplier to monitor the development product baselines, see Configuration Baselines.
- d. The initial identification of product configuration information required for the In-Service product baseline and operational information and the Contract Data Requirements.
- e. A consideration that drawings required from the Supplier should be supplied in accordance with Defence Standard 05-10: Product Definition Information.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- f. The requirements for disposal and the need to uniquely identify product CIs (eg Part number + Serial number) during manufacture to enable through life tracking and disposal management.
- g. The need to identify and record the Configuration Items (CIs) for System of Systems integration, where capability is to be achieved by the Systems of Systems approach.
- h. A requirement for a deliverable CM plan from the Supplier, dependent upon the complexity and nature of the programme.

CM PLANNING - IN-SERVICE AND DISPOSAL (SUPPORT TO MODIFICATION PROGRAMMES)

12. During the In-Service phase when the Authority has accepted the product / system from the initial development contract the Delivery Team Leader has responsibility for configuration change management. Examples of In-Service Change Management procedures specific to each domain are identified in Table 1 below.

13. CM Planning should include:

- a. The contractual CM policy and advice contained in this JSP.
- b. The relationship between the In-Service Configuration Change Authority and the subsidiary change management committee(s), see Chapter 3, Part 3 for guidance.

14. Where a Supplier is contracted for In-Service changes to the product, the Delivery Team should ensure that Supplier's CM planning identifies the interaction between the Supplier and the Authority's In-Service Configuration Change Authority and configuration change management processes.

Table 1 Contractual CM Standards and Domain In-Service Processes for CM (Example)

Generic Contract Standards for CM	
UK National Contractual Requirements.	Defence Standard 05-57 – Configuration Management of Defence Materiel Issue 5 dated
	Standard 05-10 – Product Definition Information
Joint International Contractual Requirements (NATO Nations)	Allied Configuration Management Publications 1 to 6
Air Domain Standards for CM	
Air Sector Contractual and Regulatory Articles	RA 5221 - Traceability of Aircraft Identifiable Parts.
	RA 5301 – Control of Designs.
	RA 5302 – Design Records.
	RA 5303 – Local Technical Committee.
	RA 5304 – Configuration Control Board.
	RA 5305 – Modification Classification.
	RA 5306 – Draft Modification Leaflets.
	RA 5307 – Identification and Recording of Design and Modification States of Materiel.
	RA 5308 – Service Modifications.
	RA 5308 Annex A – Overview of Service Modification Process.
	RA 5311 - Configuration Management - Project Team (CM planning).
	RA 5312 – In Service Design Changes.
	RA 5313 – Design Modifications.
RA 5602 – Control of Engine Critical Parts.	

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

	RA 5603 – Design Change Approval and Validation of Modifications.
	RA 5721 – Systems Integrity Management.
	RA 5722 – Propulsion Integrity Management.
	RA 4350 – Technical Information Management
	RA 4353 - Amendment to Technical Information
In-Service Processes	(MAP) 01, Chapter 10 - Maintenance Airworthiness Process Configuration Control.
Maritime Domain Standards for CM	
Contractual Standards	DEFSTAN 21-12 Master Record Index
	DEFSTAN 21-13 Combat System Interface and Link Documentation – Including use of SiCA database for sharing of interface information between products when used on a single platform.
	DEFSTAN 02-38 Requirements for the Preparation, Identification and Management of Datum Pack Drawings and Photographs for Swiftshure, Trafalgar and Vanguard Class Nuclear Submarines.
	DEFSTAN 02-41 (NES 41) - Requirements for Configuration Management of Surface Ships.
	DEFSTAN 21-88 - Policies and Procedures for Combat Integration of Surface Ships.
	DEFSTAN 02-28 - CM- Nuclear Submarines - In Service Support.
Maritime Domain Processes for CM	
Key Processes In-Service Submarine	Key Process 2.20 – Preserve Design Intent
	Key Process 2.30 – Manage Design Change
	Key Process 2.31 – End to End Design Change processes
	Key Process 2.32 – Implement a Design Change
	Key Process 2.34 – Unauthorised Design Changes (Amnesty process)
	Key Process 2.41 – Manage Requirements
	Key Process 2.50 – Manage Design Information
In-Service Submarine (ISM) Business Processes (BP) (Examples) Note: See ISM Controlled Document Index for full list	ISM – Authorisation Condition 22 – Modification or experiment on existing plant.
	BP 1.11 287 – Control of Organisational change and production of submissions
	BP 2.30.400 – Change Impact Assessment Procedure (CIAP)
	BP 230.817 – Completion of Safety Requirements - Proposed Change
	BP 232.505 – Obtain Clearance for use of Design Change Equipment
	BP 232.713 – Process an Submarine Alteration and addition to Approval
	BP 232.714 – Process a Class Modification to Approval
BP 2.5.401 - Requirements for the Exchange of Information with CRISP and Maritime Information Group.	
Key – Processes Surface Ship	BR 1313 – Maintenance Management in Surface Ships – Chapter 4 Configuration Management and Ship Fit Definition.
	BRd 8593(17) – Addition and Alteration (A&A) Procedures and Modifications in Surface Ships.
Land Domain - In-Service Process for CM	
	JSP 886 Volume 5 Part 2A: Configuration Management, Land Modifications.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

CONFIGURATION IDENTIFICATION AND DOCUMENTATION

15. The selection of the Configuration Items (CIs) is fundamental to the efficient and effective management of product development and system design integrity, it is the selection of these management units for configuration that determine the levels and visibility for product / system configuration change control and interface management.

16. CIs are usually established at the end of the Assessment stage, from Supplier recommendations as a result of system engineering analysis of the initial Systems Requirements Document. Further CIs may be identified during product development up to the time that the product design Configuration Baseline is established at Critical Design Review. Criteria for the selection of CIs are detailed in Chapter 3 Part 2.

17. CIs are usually the deliverable and separately installable units of the system. Computer software items are normally recognised as CIs because of the control of systems functionality.

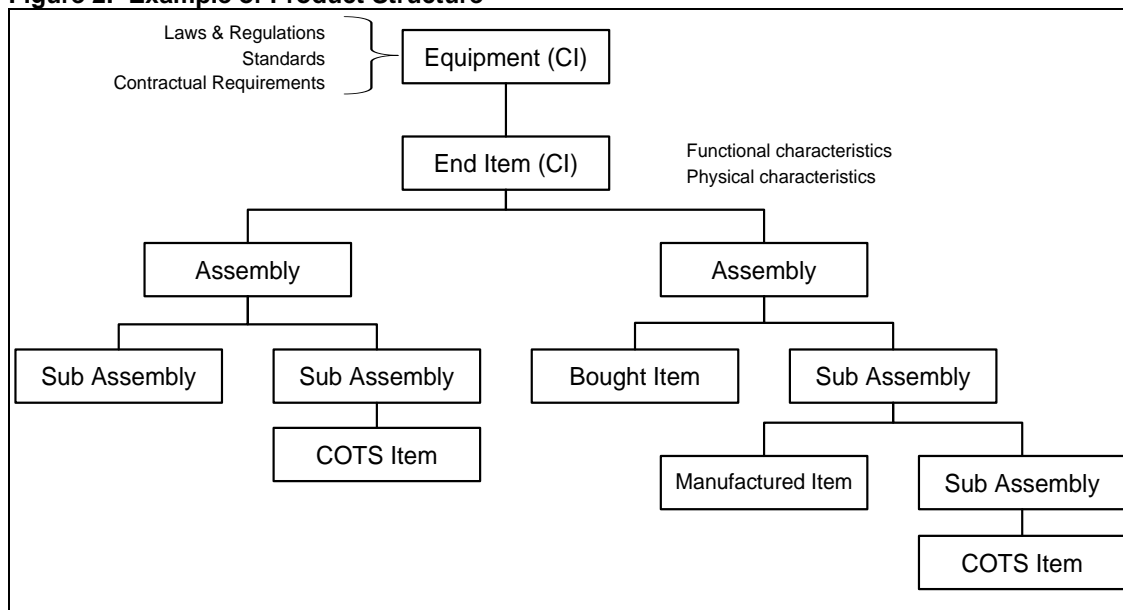
18. The selection of configuration items and their interrelationships should describe the product structure (ISO 10007), including a list of assemblies, sub-assemblies and items that require configuration management. The diagram in Figure 2 is an example of a top-down product structure, highlighting the relationships of the assemblies, sub assemblies and components that make up the system.

19. Within each level of the product structure reference should be made to product configuration information (eg – design data, operational information, maintenance procedures, storage requirements and training requirements).

20. CIs are defined within technical documentation that should also detail the interfaces between other product CIs. The release of approved configuration information establishes CI baselines.

21. The establishment of the initial CIs results in the Allocated - Design Baseline and supports the approved architecture.

Figure 2: Example of Product Structure



**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

22. CIs are usually identified by part numbers and naming convention. The Supplier – Designer will usually use its own numbering system and maintain traceability between the Supplier's identification numbering and the NATO Stock Number (NSN).

23. Where CIs are designated for the MOD Supply System, a NSN must be established for each item of supply. The contractual requirement for NSN support is invoked by DEFCON 117: Supply of Documentation for NATO Codification.

Note: When a change to a CI affects the fit, form or function, it will affect the Configuration Baseline. The revised CI must be identified with a new NSN to differentiate this new CI from the earlier CI version.

SERIAL / LOT NUMBERING

24. Serial / Lot Numbers must be unique, consecutive, and non-duplicating for all items with a specific nomenclature. The original Serial Number of a unit / item / CI must not be changed even when a change affecting interchangeability may require rework and re-identification. Once assigned, Serial Numbers must not be reused for the same item / CI. (ACMP 2). Further information regarding the use of serial numbers is contained in [JSP 886, Volume 7 Part 8.14: Management of Items Requiring Special Identification](#).

COMMERCIAL OFF-THE SHELF (COTS) AND NON-DEVELOPMENTAL ITEMS

25. Commercial off-the-shelf items are **not** to be considered as CIs unless these COTS items are to be the subject of re-development under contract.

26. Suppliers must not develop COTS items supplied as Government Furnished Equipment / Assets (GFE / GFA), unless the Supplier seeks the approval of the Authority's Representative who is to ensure that the revised COTS item is identified as a CI with unique identification to differentiate from the original COTS item.

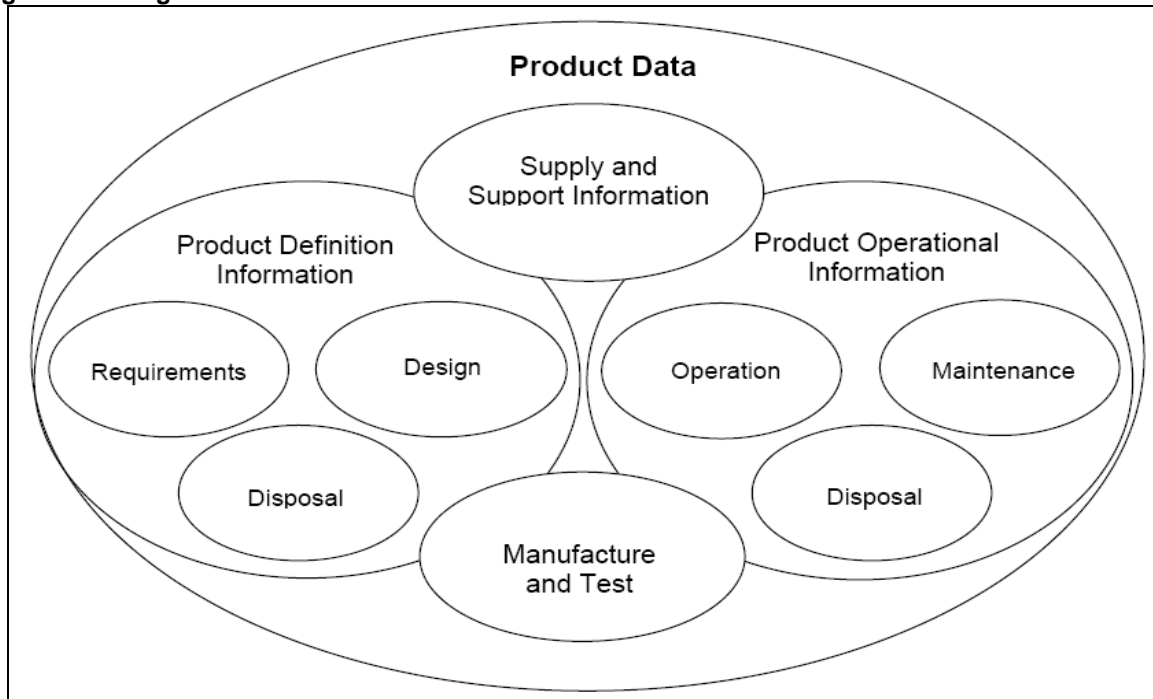
PRODUCT CONFIGURATION INFORMATION

27. The illustration at Figure 3 shows the generic categories of product CI information and how they relate. The two major sets of information for each CI are the product definition (physical and functional requirements) and the operational information that must be traceable. All physical and functional information necessary to define a CI must be documented. (ISO 10007).

28. Defence Standard 05 -10 – Product Definition Information should be considered when Drawings are contractually required from the Supplier.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Figure 3: Configuration Information.



CONFIGURATION BASELINES

29. Configuration Baselines should be established as a reference for further activities / future change. A Configuration Baseline consists of the approved configuration information to satisfy the requirements for design, verification, operation and support. (Reference ISO 10007)

30. Configuration Baselines provide stakeholders a mechanism for common understanding and an assurance that the product or system meets the contractual requirements. The level of detail for Configuration Baseline depends upon the degree of control required.

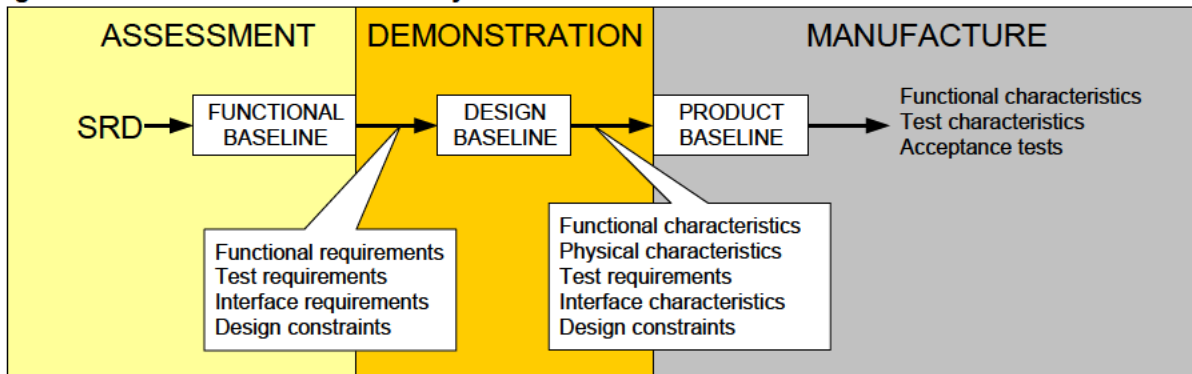
31. The recognition of a contractual deliverable Configuration Baseline provides the basis for In-Service configuration change by the Authority and contractual arrangements for Modification.

32. Before any product configuration documentation or data set is considered for baseline, it must be reviewed to ensure that the document is complete and valid for use.

33. Traditional CM practices can recognise the following product documentation baselines shown in Figure 4:

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Figure 4: Baselines and the CADMID Cycle.



- a. **Functional Baseline.** The configuration documentation formally designated during the Assessment Phase.
 - b. **Design (Development or Allocated) Baseline.** The configuration documentation formally designated at the end of the Assessment phase and before Demonstration. When Configuration Items are formally allocated to the design.
 - c. **Product Baseline.** The configuration documentation formally designated at the beginning of the Production / Manufacture. The Product Baseline + agreed Concessions = Delivered Product / In-Service Baseline.
34. The product configuration information established for Configuration Baselines can also be used to support the following [design review objectives](#) highlighted in Figure 5 below.
- a. **Concept and Technology Review (CTR).** To baseline the user requirements (URD) and the technology maturation strategy. The CTR usually takes place in the Concept phase just before the Initial Gate review.
 - b. **System Requirements Review (SRR).** To baseline the SRD and assesses the maturity and understanding of the System requirements and constraints, performance, technology maturity and Systems management activities. Ensure that the preliminary system requirements are traceable to the user requirements. An SRR would normally take place during the Assessment Phase.
 - c. **Preliminary Design Review (PDR).** To agree product CI or system design and updated SRD against which contracts can be placed or evaluated. The Whole System PDR is a multi-disciplined product and process assessment to ensure that the proposed system solution under review can proceed into detailed design, meet the stated performance requirements in the SRD. The PDR takes place during the Assessment Phase, immediately before the Main Gate review.
 - d. **System Design Review (SDR).** To approve and baseline architectural design and System performance measures. Assess if the proposed system solution can be reasonably expected to meet the SRD and fulfil the CONEMP (Concept of Employment) after the recommendations from the Main Gate review and the views of industry, related suppliers and supporting systems stakeholders have been consulted. An SDR is usually performed during the Demonstration Phase immediately after the Main Gate review.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- e. **Critical Design Review (CDR).** To baseline System design for production / manufacture. The CDR assesses the technical solution to ensure it has an expectation of meeting the URD and the SRD. A CDR normally occurs during the Demonstration phase prior to the transition to the Manufacture phase.
 - f. **Test / Trials Readiness Review (TRR).** Agreement to commence System testing. At the TRR the whole system is assessed for readiness to undergo trial or test in the appropriate environment. A TRR can take place at any time but usually only once the whole system can be brought together.
35. Product configuration information established for the design reviews described above can also be used to evaluate the Support Maturity Levels (SML), see Figure 5 and the configuration management measures of effectiveness for each SML in to Chapter 3 Part 4.
36. The measures of effectiveness for each SML should be agreed with the supplier and included in the development or support contract.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Figure 5; Configuration Management Relationship and Baseline Support to Product Requirements, Acceptance and Design Review

Phase	Concept	Assessment	Demonstration	Manufacture	In-Service	Disposal			
Assessment Gates & Key programme dates	◇ <i>Initial Gate</i>	◇ <i>Main Gate</i>		◇ <i>Logistic Support Date</i>	◇ <i>In-Service Date</i>	◇ <i>Out of Service Date</i>			
Configuration Baselines	◇ Functional Baseline	◇ Allocated Baseline		◇ Product Baseline (PBL)	◇ In-Service Baseline (PBL + Concessions)				
System Engineering Baselines		◇ System Design	◇ Approved Architecture	◇ Product Baseline		◇ In-Service Baselines			
Requirements Baselines	◇ URD	◇ SRD	◇ Updated SRD			◇ In-Service Design Changes			
		◇ Requirement Freeze	◇ System Design Freeze						
Project Review	CTR	SRR	PDR	SDR	CDR	TRR	In Service Change Processes		
Support Maturity Level	SML 1	SML 2	SML 3	SML 4	SML 5	SML 6	SML 7	SML 8	SML 9
Configuration through life Activities	Delivery Team CM Planning for Initial & Main Gate Supplier CI Identification and Documentation Supplier Configuration Management & Status Accounting Supplier Functional Configuration Audit Supplier Physical Configuration Audit					Delivery Team or Contracted Configuration Management			
Product View	As Proposed	As Specified	As Designed	As Planned / As Built	As Maintained / As Modified	Disposal			

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

CONFIGURATION CHANGE MANAGEMENT

Change Control - General

37. Configuration change management is applied through the process of establishing baseline reference points from which to control change. A Baseline reference point consists of a documented product definition baseline, which can include but not limited to; design information, software version documentation and associated validation and operational information.

38. A change to a Baseline can be initiated by the need to implement regulatory, safety, quality, or performance improvements including supportability arrangements or a need to meet new requirements for improved capability.

39. The purposes of configuration change management are to ensure:

- a. Control of Configuration Baselines.
- b. Consistency between product and product configuration information.
- c. Communication of change information.
- d. Change decisions understand the impact of change.
- e. Changes are necessary or offer significant benefit.
- f. Stakeholder interests are considered.
- g. Product interfaces are controlled.
- h. Concessions - are recorded and managed.
- i. Products are supportable after change.

40. Classified data, essential to the evaluation and disposition of change, should be submitted separately in accordance with the approved security procedures.

CHANGE CONTROL - RESPONSIBILITIES THROUGH LIFE

41. A Supplier – Design Organisation will be required, under the terms of the development contract, to ensure that configuration change management is applied to product / system development up to the delivery of the product baseline for In-Service use.

42. Once the product design drawings are completed under contract and sealed (design freeze) the supplier relinquishes Configuration Change Authority control, and therefore can no longer make changes unilaterally. At this point, the responsibility for configuration change decisions is transferred to the Authority's Delivery Team Leader responsible for In-Service design integrity.

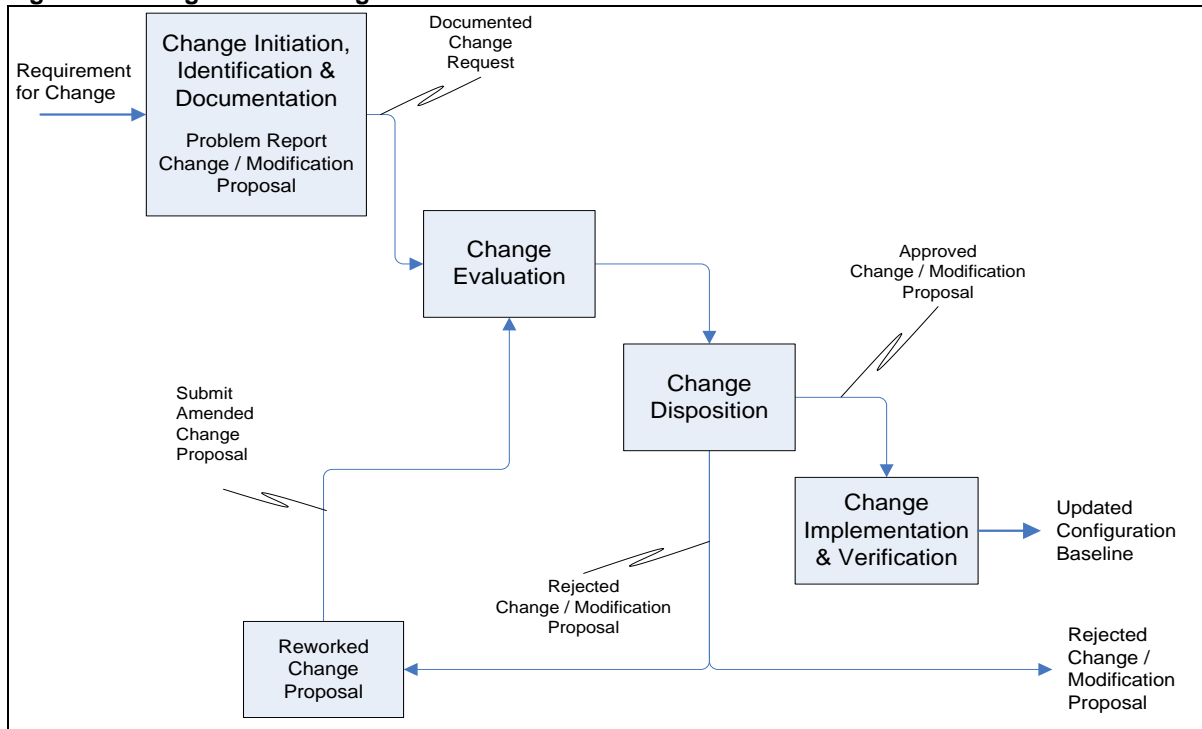
43. The Delivery Team Leader is supported by a Configuration Control Board (CCB), subsidiary committee (s) and personnel with configuration management responsibilities.

Note: Examples of Configuration Change Management responsibilities for the CCB, subsidiary committee (s) and configuration manager are contained in Chapter 3 Part 3.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

44. In-Service contractual arrangement for configuration change should be with the original or other competent Design Organisation.
45. A generic process for Configuration Change is detailed in Figure 6 and the Change Control paragraphs below.

Figure 6: Configuration Change Process



CHANGE CONTROL - INITIATION, IDENTIFICATION AND DOCUMENTATION

46. Change Control is fundamental for conveying systems engineering requirements into product attributes to meet contract and capability requirements and is initially the responsibility of the Supplier up to the delivery of the product baseline for In-Service use; when the responsibility for configuration change decisions is transferred to the Delivery Team Leader.

47. In-Service configuration change control should be managed under the contractual standards and the change management process for each Domain identified in Figure 1.

48. The following is a sample of reasons for change:

- a. Improvements to safety / risk elimination.
- b. Changes to legislation.
- c. Improvements to product performance.
- d. Provide new capability requirements.
- e. Obsolescence of products or equipment.
- f. Availability of spares.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- g. Insertion of new technology.
 - h. Correct defects (both preventive and corrective).
 - i. Improve product support.
49. Prior to submission for valuation to the Configuration Change Authority all Change Proposals should be identified and documented.
50. ISO 10007 advises that Change Proposals should typically include the following information:
- a. Configuration item(s) and related information to be changed, including details of their title(s) and current revision status.
 - b. A description of the proposed change.
 - c. Details of other configuration items or information that may be affected by the change.
 - d. The interested party preparing the proposal, and the date it was prepared.
 - e. The reason for the change.
 - f. The category of the change.
51. To support the evaluation of Change; additional details can include:
- a. Design, development and testing involved.
 - b. Operational and maintenance documentation updates.
 - c. Training requirements.
 - d. Products affected, ie products in build and / or retrofit to existing product.
 - e. Effects on spares and replacements.
 - f. Interfaces with other equipment.
52. Further change management considerations during the In-Service phase are identified in [Defence Standard 05-57, Annex D: Example Modification Proposal Form](#). The MOD Delivery Team and the Supplier may utilise or develop this Example Modification Proposal Form. Completion details are contained in Defence Standard 05-57.
53. In-Service configuration change across the MOD Domains is usually managed using the Modification and Alterations & Additions processes detailed within the Contractual Standards and processes identified in Figure 1.

CHANGE CONTROL - EVALUATION

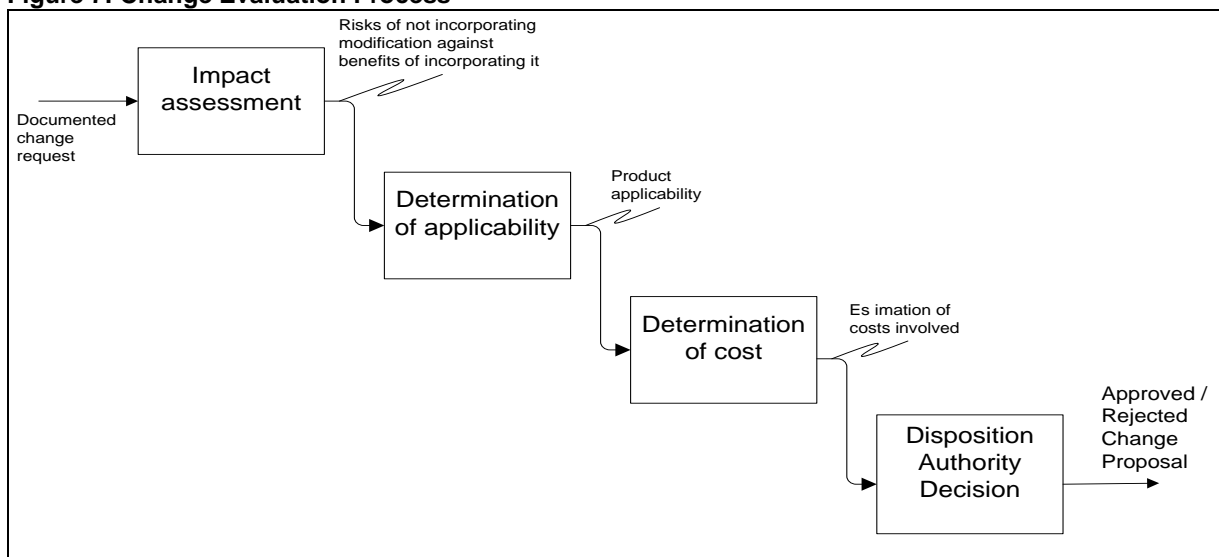
54. Evaluations of proposed changes must be documented and consider the risk / potential impact. The extent of an evaluation will depend upon the product complexity and change category, see paragraphs 61 to 66.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

55. The following stakeholders will normally be involved in the evaluation of change process shown in Figure 7.

- a. The Design Organisation will normally detail the benefits of incorporating the change and carry out the impact assessment, while detailing the risks for the change.
- b. The Design Organisation and the Authority's Representative(s) must determine the applicability of the Change Request and identify the product CIs requiring change.
- c. 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 (Reference ISO 10007).
- d. The Design Organisation should detail the costs for incorporating the change.

Figure 7: Change Evaluation Process



CHANGE CONTROL – DISPOSITION (APPROVAL / REJECTION)

56. The Prime Supplier is responsible under contract, for configuration change during initial product development and for the integrity of the deliverable Product Baseline. Following delivery of the product baseline for In-Service use, the responsibility for configuration change control is transferred to the Authority.

57. In-Service configuration change approval / rejection is provided by a meeting of the Configuration Change Authority - CCB or subsidiary committee attended by the Industry Design Organisation and relevant sub-suppliers. The Authority's representatives can include Safety; ILS, Quality Management and the Front Line Command (customer).

58. Where configuration change is agreed then the change control process should consider:

- a. When the change can be incorporated – (Effectivity Date).
- b. How the change will be incorporated.

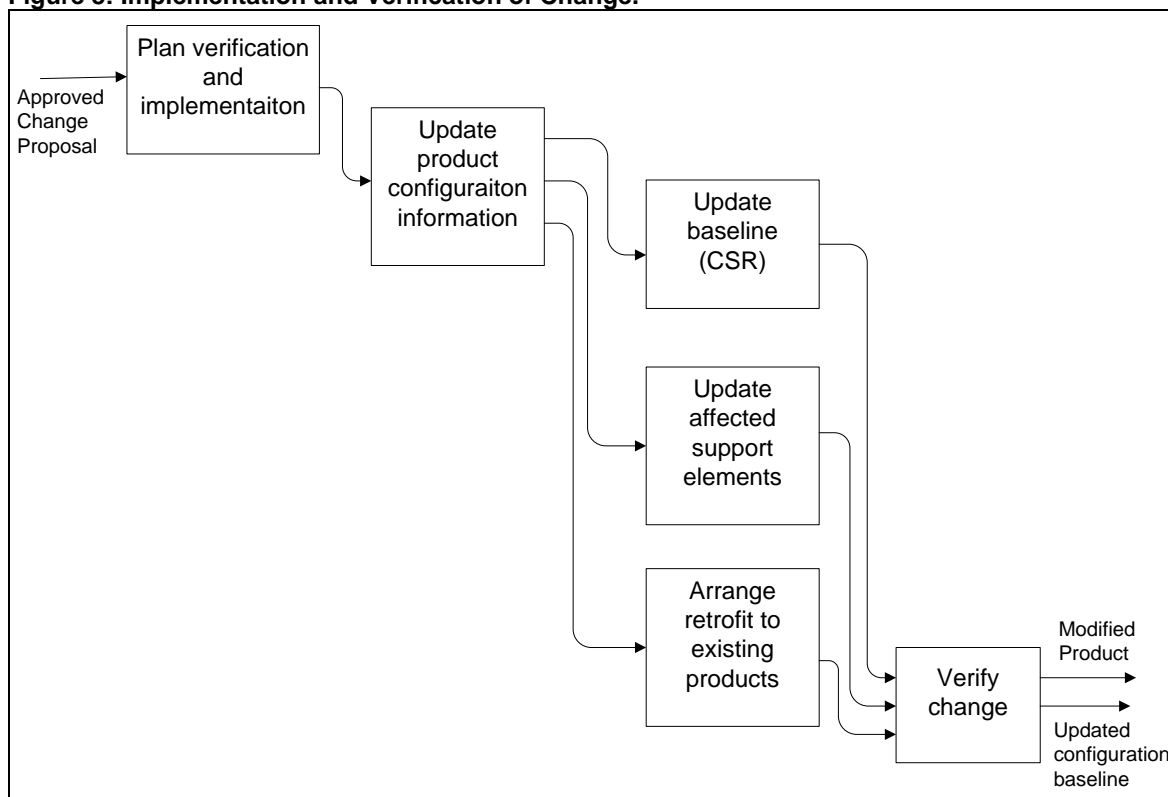
**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- c. Who will incorporate the change? (Reference ISO 10007).

CHANGE CONTROL - IMPLEMENTATION AND VERIFICATION OF CHANGE

- 59. Considerations when implementing and verifying authorised change are:
 - a. The release of product configuration information to relevant stakeholders.
 - b. To ensure that action is taken by relevant stakeholders affected by the required change.
 - c. Establish records of compliance with the authorised change. (Reference ISO 10007).

Figure 8: Implementation and Verification of Change.



- 60. Stakeholders responsible for the change implementation must verify with the In-Service Configuration Control Authority or subsidiary committee that required change is implemented. This verification must be recorded to allow traceability.

CHANGE CONTROL - CATEGORIES OF CHANGE

- 61. The categorisation of Alterations & Additions and Modifications for Surface Ships is detailed within BRd 8593 (17) – Addition and Alteration (A&A) Procedures and Modifications in Surface Ships.

- 62. The Air Domain modification classifications are detailed within the Military Air Authority (MAA) Regulatory Article 5305 and MAP 01, Chapter 10 - Maintenance Airworthiness Process, Configuration Control.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

63. The Land Domain In-Service modification categories are detailed in JSP 886, Volume 5 Part 2A.

64. Supplier's proposing engineering changes, may wish to classify an Engineering Change Proposal (ECP) as either a Class I or Class II. An ECP shall be a Class I if the product Configuration Baselines, once established, are affected to the extent that the contract requirements are not met, or change to the Product Baseline, once established, impacts one or more of the following:

- a. Government Furnished Equipment (GFE).
- b. Safety (to include safety critical software).
- c. Security.
- d. Deliverable computer software.
- e. Compatibility or interoperability with interfacing items.
- f. Delivered operational and maintenance manuals.
- g. Interchangeability or replace-ability. or
- h. Skills, manning, training, biomedical factors or human engineering design.

65. Class I changes must be agreed by the Authority's representative and communicated to the Configuration Change Authority- CCB.

66. Class II ECP addresses all changes not classified as Class I. The Delivery Team Leader should have the ability to review Class II changes for concurrence of Class 1. (Reference ACMP 3)

CHANGE CONTROL - CONCESSIONS

67. Concessions are contractual non-conformities and do not affect the product or system configuration baseline. A concession is generally limited to the delivery of the product that has nonconforming characteristics within specified limits for an agreed time or quantity of that product. (Reference ISO 10007).

68. Concessions form part of the Status Accounting records for a particular baseline, the management of Concessions should be contractually invoked in accordance with the Defence Standard 05-61, Part 1 – Concessions.

CONFIGURATION STATUS ACCOUNTING

69. Configuration Status Accounting (CSA) is the activity that results in records and reports that relate to product configuration information. (ISO 10007) Effective configuration management relies upon the availability of the up-to date product configuration information and the communication of change(s) to relevant stakeholders in a timely manner. Examples of through life CSA information is shown in Figure 9 below.

70. The depth and range of the information captured in the CSA should be based the nature of the product, the environment in which the product will be operated, the

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

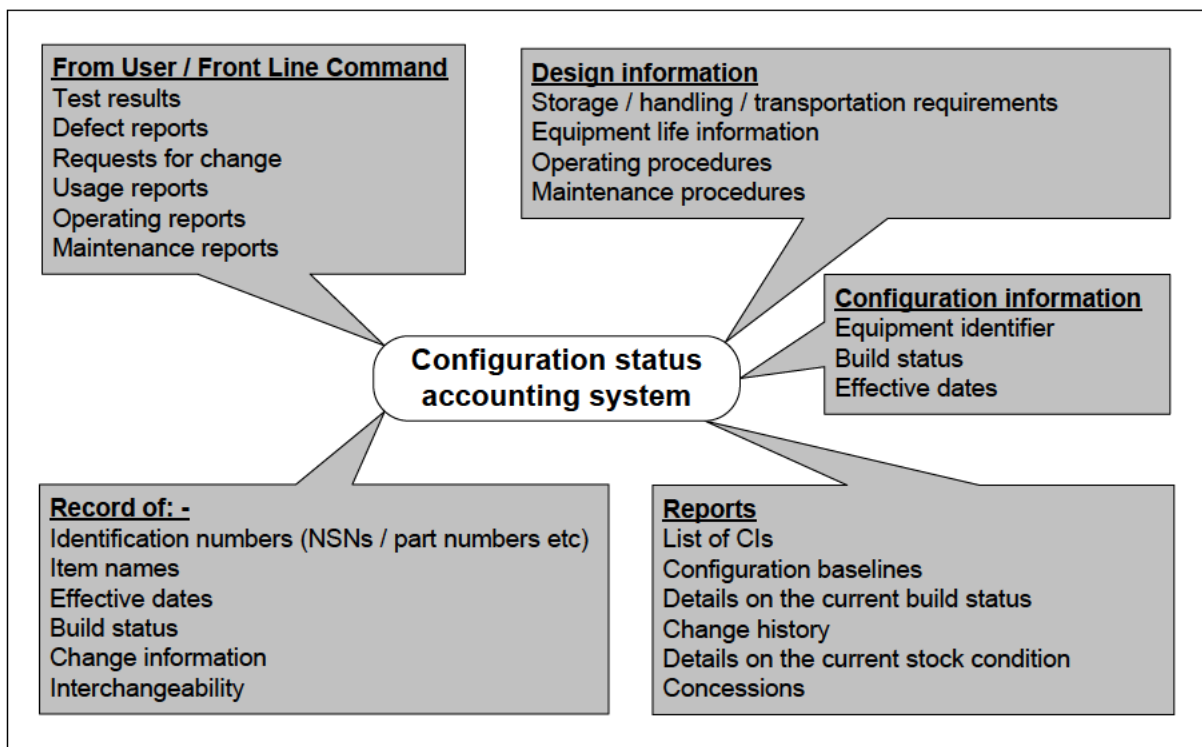
anticipated volume and complexity of change activity and the information requirements of the project. See the information examples in Figure 9: Through Life CSA System

CONCEPT PHASE CSA

71. Several documents will be produced during the concept phase that will require configuration management, namely:

- a. The User Requirements Document (URD).
- b. An outline System Requirements Document (SRD).
- c. Configuration management planning.

Figure 9: Inputs and outputs of a configuration status accounting system



ASSESSMENT PHASE CSA

72. The assessment phase “down selects” to a single technological option, hence the configuration status accounting activities will be focused upon the documents from the concept phase that will be updated and implemented.

DEMONSTRATION PHASE CSA

73. During the demonstration phase, a product structure is created and dynamically updated as the products’ requirements documents and detailed configuration documents are generated, released and a baseline set. The configuration status accounting system will need to capture information on:

- a. Product configuration information: requirements; standards; specifications; design information; CI identification; etc.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- b. Manufacturing.
- c. Testing and verification procedures.
- d. Change activity and history of the proposed and incorporated change requests.
- e. The effect of any change.
- f. Status and history of variants.

74. If the design of the product evolves, a record of the release of each product configuration information document, and subsequent revision to update the design baseline, is entered into the configuration accounting system. The accompanying data of this record's release will detail the applicability of the updates.

75. The following documented ,configuration management information can require updating and implementation to reflect the evolving design of the product;

- a. SRD.
- b. Maintain URD.
- c. Configuration Management Plan.
- d. Requirements acceptance criteria.

MANUFACTURE PHASE CSA

76. The information produced during the previous stages should be available for the manufacture phase. The information recorded in the database from the manufacture phase should include:

- a. The as built configuration of each product CI (by Serial number) including installation and removal of serialised and lot numbered components.
- b. The identities and product unit Serial numbers, which constitute the applicability of each approved major engineering change; the identifiers of the changes that have been released for any specific Serial numbered unit of a product.
- c. Superseded configuration records that reflect prior configurations of the product.

DELIVERY TO THE AUTHORITY

77. The delivery of a product to the Authority should meet the requirements of the Contract Data Requirements. Other considerations during the delivery of a product may include:

- a. Delivery dates.
- b. Installation configuration.
- c. Warranty expiration dates for each unit delivered or installed.
- d. Service agreement type and expiration.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- e. Training requirements.

IN-SERVICE PHASE

78. Configuration status accounting during the in-service phase will vary greatly depending on the support implications / requirements; and any legal requirements placed on the type of product to support capability to fulfil operational requirements. The additional information shall be maintained on the configuration status accounting system during the in-service phase:

- a. As-maintained and as-notified baseline of the product.
- b. Product operation and maintenance information revision status.
- c. Information change requests and change notices.
- d. Restrictions or concessions on use of the product.
- e. Product performance degradation.
- f. Training requirements.

DISPOSAL PHASE

79. Configuration status accounting during the disposal of a product in a cost effective and safe manner will depend on:

- a. If disposal of the product has adverse environmental implications.
- b. If the product requires a replacement.
- c. If the product is to be salvaged.

Note: The disposal of some product will have legal and contractual implications that must be considered.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

80. Typical status accounting throughout the CADMID cycle is shown in Table 2:

Table 2: Typical Status Accounting Information throughout the CADMID Cycle.

Life Cycle Phase	C	A	D	M	I	D
Typical CSA Information And Activity Which Is Tailored To Suit Product And Project						
User Requirements Document (URD).	●	●	●	●	●	●
System Requirements Document (SRD).		●	●	●	●	●
Product structure / hierarchy information.		●	●	●	●	●
Functional baseline.		●	●	●	●	●
Design baseline.			●	●	●	
Product baseline.			●	●	●	●
Configuration documentation.		●	●	●	●	●
Configuration documentation change proposals.		●	●	●	●	●
Configuration documentation change records.		●	●	●	●	●
Change request proposal.	●	●	●	●	●	
Change request records.	●	●	●	●	●	
Product change request proposal.	●	●	●	●	●	
Product change request records.	●	●	●	●	●	
Concession and variance records.		●	●	●	●	●
Verification / audit reports and actions.		●	●	●	●	●
Usage records.			●	●	●	●
Shelf life records.			●	●	●	●
Product operation information / records.			●	●	●	●
Product maintenance information / records.			●	●	●	●
Restrictions (operational / facilities / etc).			●	●	●	●
Product replacement information.			●	●	●	●
Product interchangeability information.			●	●	●	●
Product interface information.			●	●	●	●
Product safety restrictions.			●	●	●	●
Product environmental restrictions.			●	●	●	●
Product salvage information.	●	●	●	●	●	●

CONFIGURATION STATUS ACCOUNTING - RECORDS AND REPORTS

81. Configuration status accounting records are created during the configuration identification and change management activities. These records capture the process of configuration change and the product configuration information associated with contractual deliverable configuration Items; and continues for all subsequent In-Service baseline changes.

82. Throughout the product lifecycle the integrity and retrieval of configuration status records are to be protected from corruption / un-authorized change and retained in systems that permit retrieval and provide a means for disaster recovery. (ISO 10007).

83. Configuration status accounting reports provide the details and status of the configuration items (CIs) that are associated with the contractual deliverable product / system baseline. Records and reports are required for In-Service configuration management.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

84. The Configuration status accounting records for the deliverable Product Baseline (PBL) should be certified for accuracy by the Supplier / Design Organisation responsible for each CI, prior to the approval for production and before acceptance of the Authority's Representative.
85. A complete product Configuration status accounting record should provide an overview of the constituent CIs by means of a family tree, to a level of detail agreed by the Delivery Team Leader and as defined in the contract conditions.
86. Commercial database package output should be compatible with the Authority's data import requirements. The format of the deliverable CSR should be compatible with the Authority's data import requirements, as specified in the contract.
87. The Configuration status accounting records and reference systems should:
- a. Provide a record for each CI by reference to part numbers, drawings lists and specifications of the planned, current and all earlier approved baselines including, where applicable, those of variants and those of ancillary items such as change / modification sets and kits, special tools, handling equipment, special to type test equipment and packaging.
 - b. Identify any feature in the product with safety or operational implications that may require special tests or examinations.
 - c. Provide a product breakdown structure showing the relationship of all the CIs making up the product by reference to drawings list numbers and/or an illustrated parts catalogue.
 - d. Identify Non-Development / Commercial-off-the-shelf (COTS) & Government Furnished Assets (GFA) Items.
 - e. Enable higher level CIs to be cross-referred to the subsidiary and associated CIs.
 - f. List all items used in support of the product, such as special tools, design tools and models, special to type test equipment, handling equipment and packaging.
 - g. Provide a baseline for each CI from which to define the subsequent as-fitted and future modification states of the product throughout its service life.
 - h. Record the change status of the product by providing a reference to the change record of each CI, for all authorised modifications, amendments and system changes.

CONFIGURATION AUDIT

88. Configuration Audit is a formal examination to verify that the requirements of the product configuration information are realised by the product / system Configuration Items (CIs). There are two types of audit:
- a. Functional Configuration Audit (FCA).
 - b. Physical Configuration Audit (PCA).

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

89. Benefits of Configuration audit include:
- a. Validation for the integrity of the configuration documentation.
 - b. Verification of consistency between a product and its configuration documentation.
 - c. Determination that an adequate process is in place to provide continuing control of the configuration.

DELIVERY TEAM INTERACTION WITH SUPPLIER CONFIGURATION AUDIT

90. The need for configuration audit is part of the contracted CM conditions; see MOD Policy in Chapter 1. The review of Supplier configuration audits reports of product or system CIs can help to obtain assurances for product verification.

91. The configuration audit schedule should be compatible with the availability information. eg engineering data, specifications, manuals, hardware / software product design information and reports.

FUNCTIONAL CONFIGURATION AUDIT

92. A Functional Configuration audit (FCA) consists of the formal examination of test data and quality assurance records for a CI, prior to acceptance of the Product Baseline, to verify that the CI has achieved the performance and functional characteristics specified in the associated requirements configuration documentation.

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

94. By the end of the Assessment Phase and during the Demonstration Phase; Functional Configuration Audit (FCA) of CIs should be established, the results of which should be recorded and any action required taken.

95. During development a product usually goes through a series of builds, each version being progressively built towards the production model. Each model is tested against the conformance requirements as the functionality is progressively developed. During this development the following points may be considered:

- a. If a 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.
 - b. For complex System CIs, the FCA may be completed in increments. In such cases, a final FCA can be conducted to ensure that all the requirements have been satisfied.
 - c. In cases where CI verification can only be completed after system integration and testing, the final FCA can be conducted along with the PCA.
96. The FCA can include a requirement to review the following test information:
- a. Compliance test procedures.
 - b. Results from the compliance tests.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- c. Test plans, specifications, descriptions, procedures and reports for the CI.
 - d. A complete list of the successfully accomplished tests during which pre-acceptance data is recorded.
 - e. A complete list of tests required by the test requirements but not yet performed, ie, to be performed as a system or subsystem test.
 - f. Pre-production test results.
 - g. An audit of formal test plans, specifications and procedures and compared against official test data. The results will be verified for completeness and accuracy.
 - h. Interface requirements and the testing.
 - i. All changes to product design and to test equipment to ensure that they have all been incorporated and completed.
 - j. Design Reviews and Critical Design Review minutes; to ensure that all findings have been incorporated and completed.
97. An FCA audit report should be produced to detail the findings that should include:
- a. Test procedures and reports viewed and any deficiencies found.
 - b. Completion dates for all discrepancies for agreement at the post audit meeting.

PHYSICAL CONFIGURATION AUDIT

98. A Physical Configuration Audit (PCA) is the formal examination of the as-built configuration of a CI against its design documentation to ensure that the CI conforms to its specified physical requirements.
99. PCA should be established against the proposed production CI, (First Article Inspection) to assure that 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.
100. 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.
101. The Configuration Change Management control mechanism should be considered for audit to ensure that it correctly controls all internal and external changes.
102. The PCA should:
- a. Determine that the acceptance testing requirements prescribed by the documentation is adequate for the acceptance of CI production units by quality assurance activities;
 - b. Include detailed audit of product design documentation, specifications, technical data, and tests utilised in the production of the CI, and consider operation and support documentation.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- 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 configuration is reflected by this documentation.
 - d. For Computer Software CIs (CSCIs) the product specification, Interface Design Document and Version Description Document should be considered by the PCA.
103. PCA considerations should assure that:
- a. Product design information and associated manufacturing processes are incorporated into the CI.
 - b. Release records identify all relevant product design information.
 - c. Outstanding changes to the product is recorded within relevant product design information.
104. CI configuration information and audit reference information can include:
- a. FCA report.
 - b. CI specification / design information – drawing Part Number.
 - c. Identification - Part Number with possible Serial Number.
 - d. Identification - approved nomenclature / nameplates.
 - e. A list of CI approved and outstanding changes.
 - f. List of concessions against the CI.
 - g. Acceptance test procedures and associated test data.
 - h. Operating and support publications, including all Maintenance manuals.
 - i. Quality Assurance records for each CI.
 - j. Complete shortage list.
 - k. Recommended Spares List.
 - l. Release documentation.
 - m. Proposed – Certification of Design.
 - n. Draft Configuration Status Records.

SOFTWARE CONFIGURATION AUDIT

105. The CM principles apply equally to hardware and software development and change management. The following software considerations should also be considered by CA:
- a. Compare detailed design descriptions with the software listing for accuracy and completeness.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- b. Examine CSCI delivery media (disks, tapes, etc.) to ensure conformance with the software requirements specifications.
- c. Review the annotated listings for compliance with approved coding standards.
- d. Review all required operation and support documents for completeness, correctness, incorporation of comments made at critical Design Review, and adequacy to operate and support the CSCI(s).
- e. Ensure that configuration documentation details the relationship of the CSCI to the parts, components or assemblies and that executable data is properly described. For Firmware, ensure that the information completely describes the requirements for installation of the CSCI into the programmable parts or assemblies and that this information has been properly implemented. Where follow-on Acquisition of the firmware items is intended, ensure that the documentation has been accomplished to the level of detail necessary for the intended procurement.
- f. Using deliverable or Authority owned support software, assure by demonstration that each CSCI can be generated. The regenerated CSCI shall be compared to the actual CSCI delivery media to ensure that it is identical.

FINAL CONFERENCE

106. The Authority's Authorised Representative should summarise the findings of the PCA from their perspective, and should identify all relevant remedial actions and corrective action (Discrepancies). A summary report should be available to all Authority's and Supplier team members.

107. All outstanding contractual requirements should be reviewed and any liability issues resolved.

108. The Supplier representative should summarise the Supplier's reactions and acceptance of the Authority actions on the Supplier in respect of:

- a. Certification of the CI.
- b. Outstanding contractual issues in respect to the CI.
- c. Outstanding liability issues (if any).

109. Post PCA actions:

- a. The Supplier should be notified in writing by the Authority of acceptance or rejection of the PCA, the PCA status and comments, criticisms to be corrected, or rejection of the PCA and requirements for re-accomplishment.
- b. The Supplier should, after completion of the PCA, publish and distribute copies of the PCA as specified in the contract.

110. The Product configuration management design and operational information should be sealed for Production initiation.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

CONFIGURATION AUDITS OF (NON-CONTRACTED) IN-SERVICE CHANGE

111. When not contracted with a Supplier / Design Organisation, the Delivery Team Leader is responsible for Configuration Audit of In-Service changes affecting the CI functional, physical and operational characteristics. In addition to the configuration audit guidance given above, see the Functional Configuration Audit Checklist in Table 3, and the Physical Configuration Audit Checklist at Table 4 below.

Table 3: Functional Configuration Audit Checklist

Functional Configuration Audit (FCA) Checklist			
CI Description _____		Date: _____	
CI/CSCI Identifier: _____		Release No. _____	
Requirements	Yes	No	NA
1. Facilities for Conducting FCA Available.			
2. Audit Team members have been identified and informed of audit.			
3. Audit Team members are aware of their responsibilities.			
4. General Requirements Specification (GRS) or all of the following two documents: Software Requirements Specification (SRS), System Specification (SS).			
5. Waiver or Deviation List Prepared.			
6. Verification Test Procedures Submitted (Test transactions).			
7. Verification Test Procedures Reviewed and Approved (Test transactions).			
8. Verification Testing Completed and results available (System Qualification Test).			
9. Verification Test Data and Results Reviewed and Approved.			
10. Test Results submitted (if available or applicable).			
11. Verification Testing Witnessed.			
12. Test Readiness Review I and II (TRR I and TRR II) completed.			
13. Test Readiness Review I and II (TRR I and TRR II) minutes and open action items from past reviews available.			
14. Copy of baseline and database change requests with their associated status accounting records along with all design (<i>Problem Reports and Deficiency Reports (PRs and DRs), etc.</i>) provided.			
15. Other inputs as specified by the functional requirements and planning documents.			
Signature of FCA Team Members: Date: _____ _____ _____ _____			
<input type="checkbox"/> Results reviewed satisfy the requirements and are accepted (See attached comments). <input type="checkbox"/> Results reviewed do not satisfy requirements (See attached comments and list of deficiencies).			
Approved by: Date: _____			

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Table 4: Physical Configuration Audit Checklist

PHYSICAL CONFIGURATION AUDIT (PCA) - CHECKLIST	
For Assessment of:	
Agency Name:	
Project Name:	
Phase/Release:	
Date:	

Criteria	Yes / No / NA
a. Is the Physical Configuration Audit (PCA) Plan comprehensive and complete?	
b. Has the PCA Plan been reviewed and approved by the designated approvers?	
c. Is PCA methodology feasible?	
d. Is documented methodology for the PCA unambiguous?	
e. Were all entry criteria satisfied prior to starting the PCA?	
f. Were all mandatory inputs complete and available prior to starting the PCA?	
g. Has the impact of pending change orders been assessed?	
h. Is the physical configuration of the system under examination and the system used for the Functional Configuration Audit (FCA) consistent?	
i. If the physical configuration of the system under examination and the system used for the FCA are inconsistent, has it been demonstrated that the differences do not degrade the functional characteristics of the configuration item?	
j. Has documentation that records the baseline configuration of the system been compared to the released system to verify that the documentation actually reflects the released system?	
k. If there are inconsistencies between the documentation that records the baseline configuration of the system and the released system, have the inconsistencies been documented and accepted?	
l. Has documentation that records the baseline configuration of the system been reviewed for format and completeness?	
m. Is the documentation that records the baseline configuration of the system and the released system consistent with the documented design?	
n. Does actual system delivery media conform to specifications?	
o. Is the documentation that records the baseline configuration of the system and the released system consistent with build records, confirming that the system has been build in accordance with specifications?	
p. Have all major problems and risks been identified and documented?	
q. If there are major problems and risks, are there plans to accept, address, or mitigate those problems and risks?	
r. Have all PCA exit criteria been satisfied?	

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

CHAPTER 3: CONFIGURATION MANAGEMENT GUIDANCE

PART 1: CONFIGURATION MANAGEMENT PLAN – RECOMMENDED CONTENTS

1. This table of contents is a guide to a typical CM Plan, and must be tailored to suit the requirements of the project. The suggested contents of the sections, although detailed, are not exhaustive and some of the suggested inputs to the CMP may not be required and should be omitted. Omissions should be justified.

1. **Introduction.** This section should:
 - Provide a programme overview
 - Define the purpose and scope of the CMP and the extent of the CM to be applied to the activities associated with the project and product;
 - Detail the security instructions that are specific to CM, which must reflect the requirements of the Security Management Plan.
 - Contain information on any special features of the materiel, or the project programme, which have a bearing on CM.
2. **Organisation and Responsibilities.** This section should:
 - Detail the programme organisation and list the points of contact in the project involved with CM, including; Front Line Command, the Delivery Team, the Supplier – and Design Organisation.
 - Identify the configuration management organisation and configuration change Authority for contracted product development and detail the organisational responsibilities
 - Identify the relationships between the Delivery Team, the Supplier and Design Organisation, for the provision of CM during product development.
 - Identify the In-Service - Configuration Control Authority and any subsidiary Configuration Management Committee(s); i.e. Configuration Control Board (CCB) and subsidiary Configuration Control Committee (CCC).
 - Detail the roles and responsibilities of the CCB and any subsidiary CCC.
 - Identify the In-Service relationships between the Delivery Team, the Supplier and Design Organisation, for the provision of CM.
3. **Organisation CM Processes and Resources.**
 - List or detail the policies and directives for the CM of the product.
 - Identify the change procedures throughout the development of the URD and SRD, the development of the deliverable product and or the In-service change and Disposal.
 - List or detail the procedures used by the delivery team for the CM; eg. see Chapter 2, Figure 1.
 - Identify the facilities such as, technical data models, databases and information systems with direct and indirect implication for the products CM.
4. **Programme and Project Management.** This section should:
 - Detail the schedule and list the CM milestones of the programme project taken from the Through Life Management Plan
 - Define the constraints on the CM of the product.
 - Define the assumptions made when developing the CMP.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- Define the product dependencies
- Identify the Contractual CM requirements in accordance with MOD CM policy and the specific requirements for the Domain systems.
- Detail the requirements for the transfer or availability of product configuration information from the Supplier to the Authority.

Note: Projects may contract for the supplier to manage the CM information throughout the life of the project. In this case detail the requirements for the availability of product configuration information In-Service.

5 Configuration Identification and Documentation. This section should:

- Detail the Delivery Teams involvement in the Selection of Configuration Items (CI)
- Detail the Delivery Teams requirements for product / system CIs; see configuration items.
- Detail how Configuration Items (CI) will be identified; including Configuration Item of Supply for NATO Codification, (NATO Stock Number).

6. Configuration Change Control. This section shall define as a minimum the requirements for:

- Change Control
- Change Classifications
- Change Control Forms
- Problem Resolution Tracking
- System Change Requests
- System Change Requests Priorities
- Configuration Management Libraries
- Release Management
- Version Control
- For more details see Configuration Change Control

7. Interface Control and Management. This section should include:

- The arrangements for the use of non developmental items (NDI) and government furnished Information (GFI) and Government Furnished Equipment (GFE);
- Details of other projects and products which may be affected by changes to the product CIs and arrangements for the co-ordination and exchange of information;
- Methodologies to be adopted for the identification, control and documenting of equipment external interfaces;
- Relationships between databases for co-ordinating CM between products and different equipment at the platform or system level;
- Arrangements for co-ordination with other project requirements, e.g. Standardisation, codification and LSA (Logistic Support Analysis).

8. Configuration Status Accounting. This section should:

- Define how the project will ensure that the configuration activities are managed throughout the life cycle of the project and should reference the processes for collecting, recording, processing and maintaining all product configuration information.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- Including details on:
 - Formats and data elements for all configuration documentation;
 - Specification, outline, installation and information drawings, where relevant.
 - Design review records and certificates;
 - Concessions;
 - Computer software documentation;
 - Proposed authorised change proposals;
 - Correlation of change proposals on interfacing CIs;
 - Formal review periodicity and the means for being viewed remotely by all authorised personnel;
 - Archive and Retrieval of all product configuration information.
 - For more information, see *Configuration Status Accounting*.

9. Baseline Management.

- This section shall define how and when baselines will be established and reviewed. see *Configuration Baselines*.

9. CM Repositories and Data Management. This section should:

- Describe the tools and methodologies for storing / handling the configuration management information and should cover:
- Description of all data media;
- How the management of data shall be controlled and verified throughout the product life cycle;
- Data ownership at working and organisational levels;
- Technical publication and user data;
- Data storage details, including access / limitation to data and prevention of data loss;

10. Support Software.

- Describe how any software will be configuration managed and how this is related to the hardware, with reference to Supplier Software Configuration Management Plan, where requested and available.

11. Configuration Auditing. This section should:

- Describe how Supplier Functional and Physical configuration audit reporting is to be managed, including:
- Review of Functional Configuration Audits (FCA) and the Physical Configuration Audits (PCA).
- Format for the reporting of the results of the FCA and PCA.
- Schedules for Supplier configuration audits, including the relevant design reviews up to Product / system acceptance.
- Schedules for Delivery Team In-Service configuration audits.
- For more information see – *Configuration Audits*.

12. Configuration Documents Maintenance.

- Detail the instructions for the management of CM documents, including the CMP, with the means and methods of review, change control, change

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

authority, approved signatures, publication and issue.

13. Training.

- This section shall describe how training requirements will be identified, developed, carried out and ensure that training meets requirements.

14. Appendices.

- Glossary of Terms.
- Acronyms and Abbreviations.
- Reference Documents.
- Detail the reference specifications, standards, manuals and other publications applicable to the CM of the project and product. Each document shall be completely identified by title, document number, version number, issuing authority and date of issue.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

PART 2: SELECTION CRITERIA - CONFIGURATION ITEMS

1. The selection criteria for CIs shall include, but is not limited to:
 - a. **Safety.**
 - Where the failure of the CI causes a risk to personnel safety.
 - Where the failure of the CI would affect the safety of the product
 - b. **Criticality.**
 - Where the sole failure of the CI causes product failure.
 - Where the failure of the CI would critically affect the system, causing the system to become unavailable or unable to achieve mission objectives.
 - Where the CI is important to the operation of the product.
 - Where the CI is important for interfaces to one, or more, other systems.
 - c. **Complexity.**
 - Where the CI is complex or an integral part of the system.
 - Where the CI has a long lead-time for manufacture.
 - d. **Costs and Purchasing Functionality and Performance.**
 - Items which have significant financial impact or are difficult to procure or manufacture relative to state-of-the-art techniques.
 - Items which are used in large quantities (typically, at least 10 per cent of the configured items electronic parts count).
 - e. **Functionality and Performance.**
 - Where the failure of the CI would affect the system causing the system to become unavailable or unable to achieve mission objectives, or cause extensive/expensive maintenance and repair.
 - Where the failure of the CI would prevent the Acquisition of data to evaluate system safety, availability, mission success, or need for maintenance/repair.
 - Where the failure of the CI has stringent performance requirement(s) in its intended application relative to state-of-the-art techniques for the item.
 - f. **Integration, Interchangeability and Status as a Replaceable Item.**
 - Items that are used in more than one position in a product.
 - Items that are used in more than one product or project.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- Products, where items at different issues are interchangeable, but control is required.
 - Products, where items at different issues are incompatible.
- g. **Integrated Logistic Support (ILS).**
- Items that have a known operating life, shelf life, or environmental exposure. This could be vibration, thermal, or a limitation which warrants controlled surveillance specified conditions.
 - Items which are known to require special handling, transportation, storage and/or test precautions.
 - Items that have a limited and predictable useful life and could be considered for replacement on a pre-planned basis for reliability, safety or economic reasons.
2. While identifying CIs the following topics must be taken into consideration:
- a. **Define product structure and select sub-elements to be managed.**
- b. **Assign Unique Identifiers.**
- Adopt a structured numbering system that can trace physical or functional dependencies through the hierarchy.
 - Assign serial and lot numbers, as necessary, to differentiate individual units and groups of units, respectively.
 - Control of all variants or issues of each product and possible fit of CIs.
 - NATO Stock Numbering.
- c. **Marking of Products.**
- Wherever possible, products CIs should be marked or labelled with the manufacturer's reference / part number; variant number.
 - Products CIs should be identified by NSN or in accordance with the unique identification requirements of the contract.
- d. **Define Products Attributes.**
- Functional parameters.
 - Physical parameters.
 - Interfaces with other items and products.
 - Life of products.
 - Conduct review and co-ordination of configuration documentation and if required obtain Front Line Command (customer) review and approval.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- Establish release process; release configuration documentation; authorise use.
- Baseline configuration documentation for internal design control and, as applicable, for configuration change management.
- Ensure marking or labelling of products and documentation with applicable identifiers enabling correlation between the products, configuration documentation and associated data.
- Select configuration documentation types and formats.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

PART 3: CONFIGURATION CHANGE MANAGEMENT RESPONSIBILITIES (EXAMPLE)

OBJECTIVES

1. To ensure that all proposed change to systems, platforms and equipment are justified, developed, estimated, provisioned, assessed, validated, and reconciled to the allocated budget, before formal approval by the Authority's Configuration Change (Dispositioning) Authority.

CONFIGURATION CHANGE AUTHORITY

2. The In-Service Configuration Change Authority is usually the platform Delivery Team Leader supported by the Configuration Control Board (CCB)².

RESPONSIBILITIES

3. The Responsibilities of the Configuration Change Authority - CCB is generally to:
 - a. Consider and make decisions on proposed changes to the equipment, specification or its design which affect project performance, cost, timescales or delivery.
 - b. Approve and define the limits of delegated authority to any subsidiary committee(s).
 - c. Resolve differences between the MOD, the Supplier and the Design Organisation if not the contractor, arising from the specification.
 - d. Discuss issues of liability with Supplier and MOD Commercial Branch; refer concurrence of issues for settlement with MOD Commercial Director.
 - e. Authorise the supplier to proceed with approved changes.
 - f. Advise all Stakeholders of the decisions or recommendations of the Dispositioning Authority.
 - g. Report on all matters on CM business, and produce minutes, circulating to all interested parties, including those affected by consequential actions, interchangeability, costs, spares or common parts.
 - h. Ensure the preparation and maintenance of the Configuration Status Accounting Record for the CI or Master Record Index.
 - i. Agree and record product or system Configuration Baseline
4. The responsibilities of a Subsidiary Change Management Committee is generally to;
 - a. Provide a forum for dealing with technical and associated matters.
 - b. Take decisions within delegated levels of authority.

² 1. The CCB can be supported by subsidiary change management committee (s) or personnel who have delegated authority to manage and approve changes within technical, cost and other risks constraints.

2. The levels of authority required to disposition and authorise change must recognise the impact of proposed change to the safety, complexity and integrity of the product or system.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- c. Make recommendations to the Dispositioning Authority where delegations are exceeded.
- d. Assess Consequential actions, including affects on Common parts, Interchangeability and Interfaces (including interface with aircraft, Logistics, etc) and initiate activities where applicable.
- e. Acceptance of Design Records off contract.
- f. Conduct the gathering of cost elements for the Engineering Change when required by project.
- g. Recommend and manage the point of embodiment of authorised change, ensuing required; spares provision, "In-service", production support requirements including technical publications.
- h. Planning, tooling, test equipment or gauging requirements, trials etc.
- i. Evaluate materiel, stock, and advance ordering.
- j. Ensure availability of Engineering Change Advance Data Pack.
- k. Manage Salvage Actions.

Note: An Equipment Manager may undertake the responsibilities of the subsidiary change management committee and report directly to the Configuration Change Authority - CCB.

COMPOSITION

- 5. The CCB should comprise of a Chairman supported by persons having specialist knowledge of the business under discussion that may include representation from:
 - a. Production Engineering.
 - b. Manufacturing.
 - c. Specialist adviser(s).
 - d. Representative(s) of the Service users.
 - e. Representative(s) of the Design Organisation.
 - f. Representative(s) of the Suppliers affected.
 - g. Representative(s) MOD Commercial.
 - h. Front Line Command – customer support.
 - i. Quality Assurance.
 - j. Configuration Management.
 - k. Technical Secretary as required.
- 6. The Composition of subsidiary Change Management Committee is usually

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- a. Delivery Team Leader (Chairman).
- b. Delivery team Quality Representative.
- c. Representative(s) of the Design Organisation.
- d. Supplier production representatives.

CONFIGURATION MANAGER

7. The role of a Configuration Manager / CM Focal Point is generally to:
 - a. Ensure the maintenance of the Configuration Status Accounting Records or Master Record Index.
 - b. Support to the Delivery Team Leader, with the assurances required by the Support Solution Envelope (SSE) 2.5, for Initial and Main Gate approvals.
 - c. Ensure that MOD CM policy requirements are clearly translated into contractual requirements.
 - d. Ensure that potential CM risks are included in the project Risk Register and managed accordingly.
 - e. Progress and submit a Problem Report - Request for Change (RFC) to the CCB or subsidiary committee.
 - f. Record RFC that fail to be approved for progression to an Engineering Change Proposal (ECP)/ Modification change proposal.
 - g. Submit Engineering Change Proposal (s) to the Configuration Change Authority - CCB or subsidiary committee for Disposition.
 - h. Monitor and record the progress of Configuration Change Authority - CCB authorised changes and progress Engineering Change Notices.
 - i. Monitor the verification for the implementation of change – modifications by stakeholders.

Note: Approved ECP are developed into Engineering Change Notices that support the implementation of approved modifications.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

PART 4: CONFIGURATION MANAGEMENT (SUPPORT MATURITY LEVELS)

1. The development of configuration management documentation can be assessed during the programme lifecycle using the 9 Support Maturity Levels (SML) detailed below, supporting the Integrated Logistic Support SML(s) defined in JSP 886 Volume 7, Part 2 Chapter 2.
2. To enable the Delivery Team to assess the maturity against success criteria, the measures of effectiveness for each SML detailed below; is to be agreed with the Supplier and included in the development or support contract.

SUCCESS CRITERIA

3. See Configuration Management Policy Statement in Section 1.

Support Maturity Level	Measure of Effectiveness	Risk If Not in Place
1. URD Defined	<ul style="list-style-type: none"> a. CM strategy - planning supporting Initial Gate is established in accordance with JSP 886 Volume 7 Part 8.12 Chapter 2. b. CM is identified in the URD as a contract requirement. c. The principles of CM are used to support stakeholder engagement and requirements capture for the User Requirements Document (URD). d. The URD is Baselined during Concept and Technology Review (CTR) and Authorised for release. e. CM is considered and evaluated by the requirements of the Support Solution Envelope (SSE 2.5) for Initial Gate. f. High Level Supplier plans in response to ITT are evaluated for Supplier management intent to develop products under CM control in accordance with the Policy requirements in Chapter 1. 	<p>The requirements for CM will not be identified or included in contracts. Ineffective development and Baseline for ITT and Contract requirements. No visibility or initial assurance assessment for Supplier CM.</p>
2. Contractual SRD Defined	<ul style="list-style-type: none"> a. CM planning to support Main Gate and Demonstration / Manufacture phases is established in accordance with Chapter 2. b. The Functional Baseline is established for initial System Requirements Document (SRD) c. Baseline CM documentation is identified in the contract data requirements list to support the System Requirements Review (SRR) and development of the SRD. d. The System of Systems Approach for CI integration at initial design is considered. e. CM is considered and evaluated by the requirements of the Support Solution Envelope (SSE 2.5) for Main Gate. 	<p>The CM requirements will not be identified or included as part of the contract conditions. The Supplier's Responsibilities for CM will not be understood / defined. The System / product design will not meet the expectations of the Front Line Commands as detailed in the URD.</p>
3. Preliminary Design Review	<ul style="list-style-type: none"> a. Changes to the URD resulting from any SRD constraints are understood, managed and implemented. b. The SRD is Baselined for Preliminary Design Review (PDR). c. The System of Systems Approach for CI integration is considered for the preliminary design. d. Initial disposal considerations for Configuration Items (CIs). 	<p>Loss of traceability between SRD and URD requirements. The product design status will be unknown and the design development will be undisciplined. System CIs integration issues can require product re-design with associated impacts to the programme.</p>
4. Critical Design	<ul style="list-style-type: none"> a. CM processes identified in CM planning are implemented by Demonstration phase. b. Configuration Items are identified and Allocated to the product / system architecture from the agreement during 	<p>The product design status will be unknown and design development will be undisciplined.</p>

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Review	<p>the System Design Review, (SDR).</p> <p>c. Product configuration information is configured and baselined for SDR.</p> <p>d. Product configuration information is managed throughout the product design - demonstration phase.</p> <p>e. Configuration Items (CIs) requiring special considerations such as life restrictions or disposal are considered for Unique Identification.</p>	Without the formal identification and documentation of CIs, CM and known product structure is not plausible.
5. Support Solution Validated	<p>a. CM processes identified in CM planning are implemented by Demonstration and initial Manufacture phases.</p> <p>b. The product / system design documentation is Baselined for Critical Design Review (CDR) and design freeze.</p> <p>c. Initial Functional Configuration Audit reports available from the Supplier.</p> <p>d. Operational elements of the product or system may be considered at this time for Initial Integrated Logistic Support (ILS) considerations.</p> <p>e. Disposal requirements are considered and identified within System / product configuration information.</p>	<p>The product design status will be unknown and the design development will be undisciplined.</p> <p>Without the formal identification and documentation of CIs, CM and known product structure is not plausible.</p>
6. Logistic Support Date	<p>a. CM processes identified in CM planning are implemented within the Manufacture phase.</p> <p>b. Whole System / Product configuration information has a configuration baselined for Test / Trial Readiness Review (TRR).</p> <p>c. Integrated Test and Evaluation and Acceptance (ITEAP) requirements are established and available in accordance with planned arrangements</p> <p>d. Physical Configuration Audit reports are available from the Supplier for evaluation.</p> <p>e. Configured Operational information is available to support the Logistic Support date.</p> <p>f. CIs are identified under the NATO Codification requirements when designated as an Item of Supply for management by the MOD Joint Supply Chain.</p>	<p>The product design status will be unknown and the design development will be undisciplined.</p> <p>Without the formal identification and documentation of CIs, CM and known product structure is not plausible.</p>
7. In-Service Date	<p>a. Platform, Systems and Product configuration information supports the Deliverable Baseline for In-Service use.</p> <p>b. Required product configuration information is delivered in accordance with the requirements of the Contract Data Requirement List (CDRL) or made available to the Authority's Representative to support In-Service use and management requirements.</p> <p>c. Configuration Management procedures are identified to manage In-service design integrity and configuration status accounting requirements.</p> <p>d. Logistic Information Repository (LIR) data being populated with data generated from system / product configuration information in accordance with In-Service requirements.</p> <p>e. Delivery Team CM planning for the In-Service phase reflects the MOD Regulatory and Domain requirements for In-Service configuration management and maintenance of design integrity.</p>	<p>The design status will be unknown and the acceptance of the system / product against the contract requirements may not be possible.</p> <p>Information to support systems safety cases will not be available.</p> <p>Design will be uncontrolled and operational compatibility unknown.</p> <p>Logistic Information Repository data will be incomplete.</p>
8. In-Service Support Reviews	<p>a. CM processes as required by MOD Regulatory Authorities and Domain requirements are implemented during the In-service phase.</p> <p>b. Contractual CM requirements and Supplier CM processes as detailed in CM planning are implemented during the In-service phase.</p> <p>c. Submarine and Surface Ship definition Databases are maintained and supported by configuration management process; to assure only authorised changes to the Platform,</p>	<p>Design integrity may be compromised.</p> <p>The loss of Baseline configuration information can lead to the need for costly corrective action to establish the required information for continued use or further development.</p>

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

	<p>system and product baselines.</p> <p>d. Master Record Index documentation or similar configuration status records are maintained and supported by configuration management process to assure only authorised changes to the Platform, system and product baselines.</p>	
9. Out of Service Date	<p>a. Product definition information – Configuration Status Accounting data and operational information is archived in accordance with Regulatory and Authority requirements, eg. Configuration datum packs, and Technical Publications.</p> <p>b. Configuration Items (CI)s requiring special disposal considerations are identifiable from the Product structure and traceable to enable effective management in accordance with the disposal plan.</p>	<p>The loss of configuration information creates difficulties for the sale of MOD products. Possible environmental and safety impacts associated with product non traceability.</p>

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

**PART 5: CONFIGURATION MANAGEMENT ACTIVITIES FOR PROGRAM REVIEW
AND ILS SUPPORT**

**SUPPORT MATURITY LEVEL 1 – USER REQUIREMENTS DEFINITION, CONCEPT
PHASE AND CONCEPT TECHNOLOGY REVIEW**

Objectives

1. To baseline the User Requirements Document (URD) and establish the technology maturity strategy.
2. Determine the Contractual Configuration Management conditions for the Concept Phase, for Initial Gate approval and the Assessment Phase.
3. Provision of a CM assurance statement for the Support Solution Envelope (SSE 2.5) - Configuration Management (CM) Initial Gate.

Supporting Activities

4. Consider any Concept study recommendations and the need for the System of Systems Approach to meet URD capability requirements.
5. Define and support the ILS strategy for the project, including.
6. The agreement of the Work Breakdown Structure.
7. The Development of the support strategy as part of the overall Procurement Strategy, against the programme baseline(s).

CM Activities

8. Produce the Delivery Team Configuration Management (CM) Plan for the Concept and Assessment Phases with a Strategy for through life CM.

Note: This planning can be referenced in support of the Initial Gate Assurance - SSE 2.5.

9. Baseline the URD - to include Regulatory requirements and constraints.
10. Define the CM requirements for the Concept study documentation and data files.
11. Ensure MOD internal "version control" of Concept study data files and documentation.
12. Define the CM contractual requirements for Invitation to Tender or Notice (ITT) / (ITN) in accordance with Policy requirements in Part 1 of this JSP and consider the need for a Deliverable CM plan from the contractor.
13. Consider the CM requirements for Pre-Contract Award Evaluation (PCA/E) should this be required under the programme strategy.
14. Advise the levels of access (security requirements) to be considered in Supplier CM planning.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

15. Where previously arranged for ITT / ITN undertake PCAE of the Supplier responses and planning for configuration management, recognising the scope and the life of the contract.

16. Evaluate Supplier high level CM planning in response to ITT / ITN to assure management intent from the Supplier, to develop products under configuration control.

17. Provide assurance recommendation for the Initial Gate Support Solution Envelope (SSE 2.5) following review of Supplier CM Planning in response to ITT / ITN and CM planning by the Delivery Team.

Note: Where Supplier responses to ITT / ITN are not available – it may be possible to evaluate any relevant, available Supplier CM planning from similar type contracts to gain a level of assurance for SSE 2.5. Support Maturity Level 2 - Contract Initial System Requirements Definition during the Assessment Phase and System Requirements Review.

SUPPORT MATURITY LEVEL 2 - CONTRACT INITIAL SYSTEM REQUIREMENTS DEFINITION DURING THE ASSESSMENT PHASE AND SYSTEM REQUIREMENTS REVIEW

Objective

18. To establish an agreed Initial System Requirements Baseline that recognises the maturity and understanding of the system requirements, constraints, performance, technology maturity and systems management activities.

19. Ensure that the Preliminary Design system requirements are traceable to the user requirements.

Supporting Activities

20. Evaluate Product / System Functional Baseline as expressed in the Initial System Requirements Document (SRD) and check against the User Requirements Document (URD).

CM Activities

21. Assure that the Supplier's product documentation and Initial SRD is configured and identified with links to the Functional Baseline.

22. Review and update Delivery Team CM planning & Information knowledge Management requirements for the Demonstration and Manufacture Phases and identify the MOD interaction with the Supplier for the acceptance of the product configuration Baseline for In-Service use. Develop a CM Strategy for the In-Service and Disposal phases.

23. Establish Delivery Team CM planning links to co-ordinated plans for Acquisition; ie:

- a. Requirements Acceptance Management Plan (RAMP).
- b. Through Life Management Plan (TLMP).
- c. Master Data Assumptions List.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- d. User Requirements Document (URD).

Note: CM Planning by the Delivery Team can be referenced in support of the Main Gate Assurances for SSE 2.5 – Configuration Management.

SUPPORT MATURITY LEVEL 3 - PRELIMINARY DESIGN REVIEW & SUPPORT TO MAIN GATE

Objective

24. To agree product CIs and initial system design as detailed by updated SRD against which contracts are placed and evaluated to assure a whole system product and process assessment to ensure that the proposed system solution under review can proceed into detailed design and meet the stated performance requirements in the SRD.

Supporting Activities

25. Review initial product / system design against the updated SRD Baseline.
26. Communicate with the Customer where the SRD requirements affect expectation as detailed by the URD and obtain from MOD Customer (Front Line Command), a view whether identified deficiencies against URD requirements are acceptable.
27. Consider Interoperability requirements and support to Standardisation.
28. Define and support the ILS strategy for the project, considering the co-ordination of all related disciplines and elements that may impact on development and delivery of fully supportable equipment, in conformance with DEFSTAN 00-600 & MOD Policies.
29. Establish ILS requirements for contract and logistic support date and recognise in configuration documentation.

Notes:

1. The Font Line Command has ownership of URD
2. The Deliver Team has ownership of the SRD, used as the basis for product and system acceptance.
3. The SRD provides a quality check on the fitness for purpose of the evolving URD by helping to address omissions and ambiguities in the URD.

CM Activities & Contract Considerations

30. Ensure that the CM requirements established for ITT / ITN in accordance with the Policy requirements in Part 1 of this JSP are reflected in the contract requirements for product design / manufacture and acceptance by the MOD delivery Team.
31. Advise of the levels of access (security requirements) for Supplier CM planning.
32. Undertake a review of the Supplier planned arrangements for configuration management during the Demonstration and Manufacture Phases for product development, delivery and required In-Service information.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

33. Identify the product configuration information required to support appropriate design reviews and to support the product acceptance from Supplier for In-Service use. Possible use if Contract Requirements Data List (CDRL).
34. Define or agree the format for the deliverable product configuration information and Configuration Status Record (CSR) or Master Record Index (MRI) is to be supplied.
35. Identify Non-Development Items e.g. COTS products and products provided as Government Furnished Assets / Equipment (GFA / GFE). Identify the configuration status of GFA / GFE products and Test facilities.
36. Items designated for NATO re-procurement for MOD supply chain; are to be identified by an NATO Supply Code for Manufacture (NSCM), the NATO Stock No. (NSN) or NATO Standard Stock No (NSSN) (Refer to DEFCON 117).
37. Arrange the transfer of Product Configuration Information where a MOD Organisation requires a Configuration Status Accounting (CSA) Baseline for In-Service use.
38. Where significant CM risk is identified, arrange Risk Based Surveillance with a Registered GQAR Organisation to review the management system associated with the perceived risk.

SYSTEM DESIGN REVIEW (NON-SUPPORT MATURITY LEVEL)

Objective

39. To approve and baseline architectural design and System performance measures, assess if the proposed system solution can be reasonably expected to meet the SRD and fulfil the Concept of Operations (CONEMP) after the recommendations from the Main Gate review and the views of industry, related suppliers and supporting systems stakeholders have been consulted.

Supporting Activities

40. Refine and agree the SRD and Architecture models and assumptions based upon outputs from the contractor's system engineering process.
41. Communication with the Customer - (Front Line Command) where change(s) to requirements through SRD constraints affect expectation as detailed by the URD.
42. Record Trade-off decisions and record non-compliances / variance to the Requirements and Acceptance Documentation.
43. Development of Integrated Test and Evaluation Plan (ITEAP).
44. Consideration of Integrated Logistic Support (ILS) requirements in Design Reviews.

CM Activities

45. Ensure that the linkage between the versions of the ITEAP and Validation and Verification Requirements Matrix is supported by Configuration Management (CM).
46. Assure the CM control and CM status for the outline ITEAP.
47. Initial evaluation and identification of CIs that require tracking through life.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

48. Review CI product documentation to assess the functional and physical characteristics.
49. Initial evaluation and identification of CIs that require special consideration for disposal.
50. Review initial Product Breakdown Structure of Configuration Items (CIs).

SUPPORT MATURITY LEVEL 4 - CRITICAL DESIGN REVIEW

Objective

51. To baseline System design for manufacture / production. Assesses the technical solution during the Critical Design Review (CDR) to ensure it has a reasonable expectation of meeting the URD and the SRD.

Supporting Activities

52. System Design Baseline - Agree product / system Configuration Item(s) (CIs) within Product Baseline for manufacture.
53. Consider the CI functional and physical - interface characteristic to support System of Systems integration requirements.
54. Assure that compatibility is maintained between the product CIs and other interfacing system / platform CIs to support system integration (possibly software to hardware integration) and the System of Systems Approach.
55. Agree scope of product / system testing for product / system acceptance, (review of ITEAP).
56. Consideration of ILS requirements during Critical Design Review and in any subsequent Configuration Change Proposals (usually presented by the Contractor using Engineering Change Proposals).
57. Consider interoperability requirement and support to Standardisation.

CM Activities

58. Assure version compatibility (as reported) between products / System CIs.
59. Evaluation and Identification of CIs that require tracking through life.
60. Evaluation and identification of CIs that require special consideration for disposal.
61. Review initial Functional Configuration Audit CI (test reports) from the Supplier; to gain assurance that the CI functional characteristics meet the URD and SRD requirements.
62. Review First Article Inspection reports to gain assurance that the CI physical characteristics meet the design requirements.
63. Review CI product breakdown structure to assure compatibility with URD and ILS requirements.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

64. Review CI product documentation to assess and agree functional and physical characteristics.
65. Co-ordinate exchange of information, with other Delivery team(s) about system that can be affected by revised requirement.
66. Assure system Interface requirements - Review Interface Control Document against the CI product Breakdown structure.
67. Initiate Configuration Change Management Committee (CCMC) - A Configuration Change Management Committee (CCMC) is a formal gathering to discuss support matters post Logistic Support Date (LSD) and to authorise changes to the product, associated elements or the support.
68. Ensure correct Interaction between the Configuration Change Committee and the Configuration Control Board via integrated Terms of Reference.

Integrated Logistic Support

69. The MOD Integration Logistic Support Manager (MILSM) will usually ensure that supportability aspects are represented at design reviews and during the product acceptance process.

Manage Logistic Configuration

70. This activity includes the creation of a plan to manage the configuration and identification of the tools and management skills required for the creation and maintenance of the TLS configuration. It needs to address:
 - a. Plan configuration management.
 - b. Specify configuration.
 - c. Configuration Change Management.
 - d. Maintenance of the configuration status record.
 - e. ILS Configuration audits.
 - f. Verification and feedback.

Acceptance of Support Recommendation

71. The ILS deliverables shall be reviewed to ensure that the ILS / SA tasks have been completed correctly; the logistic data is consistent with the design data and complete as well as being compatible with the proposed maintenance concept. The theoretical support recommendations shall be reviewed throughout the project in line with the increasing level of design definition. The final acceptance shall form part of the Factory Acceptance Process and shall be aimed at ensuring the support recommendations are appropriate and traceable to the actual design configuration being delivered.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

SUPPORT MATURITY LEVEL 5 AND 6 SUPPORT SOLUTION VALIDATION, LOGISTIC SUPPORT DATE AND TEST READINESS REVIEW (TRR)

Objective

72. Whole system is assessed for readiness to undergo trial or test in the appropriate environment. A TRR can take place at any time but usually only once the whole system can be brought together.

Supporting Activities

73. Ensure that the linkage between the versions of the ITEAP and Validation and Verification Requirements Matrix.

74. Ensure required Interaction between the Contractor and Delivery Team e.g. via Local Technical Committee to support product / system acceptance.

CM Activities

75. Assess Contractor's Class 1 Engineering Change Proposal(s) (ECP) that are designated to request change(s) affecting fit, form & function once the product baseline is agreed at CDR.

Note: An ECP shall be a Class I if the product Configuration Baselines, once established, are affected to the extent that the contract requirements are not met, or change to the Product Baseline, once established, impacts one or more of the following:

- a. Government Furnished Equipment (GFE).
- b. Safety (to include safety critical software).
- c. Security.
- d. Deliverable computer software.
- e. Compatibility or interoperability with interfacing items.
- f. Delivered operational and maintenance manuals.
- g. Interchangeability or replace-ability.
- h. Skills, manning, training, biomedical factors or human engineering design.

76. A Class 1 ECP is to be evaluated, rejected or agreed by the Delivery Team Leader or his representative with this decision communicated to the Contractor's CCB.

(Reference Def Stan 05-57 Issue 6).

SUPPORT MATURITY LEVEL 7 - IN-SERVICE DATE & DELIVERABLE PRODUCT ACCEPTANCE

Objective

77. Product, system acceptance against SRD, ITEAP and contract requirements.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Supporting Activities

78. Ensure that requirements of the ITEAP and Validation and Verification Requirements Matrix (V&V RM) are satisfied by product CIs.

CM Activities

79. Ensure that the Configuration Status Record (MRI / DIS) for the Product Baseline is certified for accuracy by the Supplier / Design Authority, prior to approval for production and before transfer off contract to In-service use.

80. Review Supplier Functional and Physical Audit Reports to support product acceptance.

81. Establish formal CM processes to manage the configuration of the project team's In-Service documentation.

82. Update CM planning to recognise In-Service configuration change management via Alterations and Additions and Modifications.

83. Configuration control of the datum pack as detailed in the Configuration Management Plan.

Integrated Logistic Support and Acceptance

84. The ILS deliverables are usually reviewed by the MOD Integration Logistic Support Manager (MILSM) to ensure that the ILS / SA tasks have been completed correctly; the logistic data is consistent with the design data and complete as well as being compatible with the proposed maintenance concept. The theoretical support recommendations shall be reviewed throughout the project in line with the increasing level of design definition. The final acceptance shall form part of the Factory Acceptance Process and shall be aimed at ensuring the support recommendations are appropriate and traceable to the actual design configuration being delivered.

SUPPORT MATURITY LEVEL 8 - IN-SERVICE SUPPORT REVIEW - RESPONSIBILITY FOR REVISED CAPABILITY AND DESIGN INTEGRITY (MODIFICATION OF CONFIGURATION BASELINES)

Objectives

85. Ensure that compatibility is maintained between the product CIs and those in any interfacing product, system and platform.

86. After the design is accepted for In-service use - Subsequent changes to the delivered product (physical, functional & operational requirements) shall be changed in accordance with planned arrangements with design changes authorised by the Delivery team Leader.

Supporting Activities

87. Maintain ownership of SRD and the Delivered product baseline that provides the basis for product / system configuration changes.

88. Established the MOD in the role of the Decider and the Supplier as the Provider once the product has been accepted from the Development contract for In-Service use.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

89. Establish an In-Service Configuration Control Board (CCB) and where required a supporting subsidiary change management committee or personal who have delegated authority to manage and approve change within technical, cost and other risk constraints.

90. Utilise the Air Domain Modification Proposal Form in Def Stan 05-57, Annex D to manage In-Service configuration change(s). Otherwise utilise other Domain specific requirements detailed in Chapter 2, Table 1 of this JSP.

91. Ensure that supportability aspects are represented at Configuration Change Management Committee & Design Reviews.

CM Activities

92. Update the Deliver Teams through life CM Planning to identify the In-Service change management process and identify the configuration management organisation, including the Configuration Control Board (CCB) and where required the subordinate Committee; responsible for assuring the integrity of the product design In-Service

93. Ensure the correct interaction between the CCB and any subsidiary committee(s) Exemplar Terms of Reference are provided in Section 2 Part 3 of this JSP.

94. The change management process should consider the configuration change management requirements in Chapter 2 of this JSP and ensure the:

- a. The initiation, identification and documentation of the need for change.
- b. The evaluation of the change by CCB or subsidiary committee or person.
- c. Recording and notification of the approval / rejection of configuration.
- d. Implementation planning to ensure that the required product configuration information and materiel is available for release to support the embodiment of an approved modification.
- e. Verification of change.
- f. Feedback to Delivery Team to assure implementation.

95. Maintain the Configuration Status Accounting (CSA) Baseline for In-Service use.

96. Implement a means for recording all changes to all CIs and maintaining traceability between all affected CIs.

97. Maintain Identification of CIs that require tracking through life.

98. Maintain Identification of CIs that require special consideration for disposal.

99. Consider Obsolescence issues of Non-Development Items e.g. COTS products during the evaluation of modification proposals.

100. Co-ordinate an exchange of information, with other project teams who have products that can be affected by changes to product / platform Configured Items.

101. Use formal CM processes to manage the configuration of the project team's internal documentation.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

Configuration Status Accounting (CSA)

102. Ensure CSA is capable of recognising the potential for impact on interfacing CIs and track the progress of changes necessary to retain compatibility.

103. Maintain systems / tools to capture the information that defines product configuration. (Product Breakdown Structure & CI - Build of Materiel).

104. Review the sentencing of Concessions under Def Stan 05-61 Part 1 where Concessions are to be considered as part of the CSA records.

Functional & Physical Configuration Auditing

105. Review Configuration audit reports for assurance of formal verification of product requirements and ensure recorded within the Configuration Status Accounting (CSA)

In-Service Contract Considerations

106. Make recommendations for CM contract conditions in accordance with Part 1 of this JSP.

107. Make recommendations for the Domain Specific CM contract conditions, e.g. Defence Standards and MAA RA 5000 Series.

108. Ensure that Supplier CM planning interface with MOD Domain change management requirements and contract standards.

109. Identify within the Contract Requirements Data List (CDRL) the CM documentation required to support appropriate In-Service design reviews and to support the transfer of the product from Supplier to Under Ministry Control.

110. Define requirements for updated Configuration Status Record(s) and evaluate for acceptance upon delivery.

111. Where necessary; arrange Risk Based Surveillance with a registered GQAR Organisation to help mitigate identified significant CM risks with a Contractor.

112. Monitor Supplier progress of product development against revised baseline requirements.

113. Review the use of Non-Development Items e.g. COTS products and Government Furnished Equipment (GFE) and update as necessary.

SUPPORT MATURITY LEVEL 9 - PRODUCT / SYSTEM DISPOSAL

Objectives

114. Ability to transfer required product configuration Information with products designated for Sale after In-Service use (UK Trade and Investment - Defence and Security Organisation)

115. Ability to meet statutory and business requirements to retrieve product configuration Information and to trace product location.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

CM Tasks

116. Transfer or Archive product configuration information and Configuration Status Accounting information, in accordance with statutory and business requirements.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

PART 6: DEFINITIONS

1. **Acquisition.** The process of requirements setting, procurement management, support management and termination / disposal implying a whole life approach to defence capability (DEFSTAN 05-57).
2. **Acquisition Life Cycle.** The phases of a project that enable the delivery support and disposal of military capability (DEFSTAN 05-57).
3. **Allocated – Design Baseline: [Developmental].** The configuration documentation formally designated at the end of the Assessment phase and before the Demonstration phase. The Allocated - Design Baseline includes:
 - a. The functional characteristics that are allocated from the Functional Baseline Cls.
 - b. The test requirements demonstrating achievement of the functional characteristics.
 - c. The interface characteristics with associated Cls.
 - d. The Design constraints. (DEFSTAN 05-57)
4. **Authority.** Secretary of State for Defence or person (s) duly authorised to act on his behalf or as defined in the contract. (DEFSTAN 05-57)
5. **Change Control** Activities for control of the product after formal approval of its product configuration information. (ISO 10007:2003)
6. **Computer Software Configuration Item (CSCI).** Computer software designated for configuration management. (Allied Configuration Management Publication – ACMP 6)
7. **Computer Software Unit (CSU).** An element, specified in the design of a Computer Software Component (CSC) that may be tested separately (ACMP 6)
8. **Concession.** 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 formally known as a Production Permit / Deviation. (DEFSTAN 05-61 Part 1)
9. **Configuration.** The functional and physical characteristics of materiel as described in its technical documentation and later achieved in the product. (DEFSTAN 05-57).
10. **Configuration Audit.** Checking an item for compliance with its configuration documentation (ACMP 6)
11. **Configuration Baseline.** The approved configuration documentation formally designated at a specific point in the CI life-cycle; that serves as reference for activities throughout the CI product life cycle. (Part ISO 10007). During Product development there are normally three baselines:
 - a. Functional Baseline (FBL).
 - b. Allocated Baseline (ABL): [Developmental].

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

- c. Product Baseline (PBL).
12. **Configuration Control.** The systematic evaluation, coordination, approval or disapproval and dissemination of all proposed changes to a CI and / or its configuration documentation; after formal establishment of its configuration baseline and verifying the implementation of all approved changes (ACMP 6)
13. **Configuration Data.** All data, regardless of form or characteristics, that is subject to configuration management. (ACMP 6).
14. **Configuration Documentation.** The current approved technical documentation for a CI. (ACMP 6).
15. **Configuration Identification.** The process of identifying and documenting the functional and physical characteristics of CI. (ACMP 6)
16. **Configuration Item (CI).** An item designated for configuration management (ACMP 6)
17. **Configuration Management (CM)** A discipline applying technical and administrative direction and surveillance to the following activities:
- a. Configuration Identification and Documentation.
 - b. Configuration Control.
 - c. Configuration status accounting and configuration data management.
 - d. Configuration Audits. (ACMP 6)
18. **Configuration Management Plan (CMP).** The document that formally describes the scope of CM, the CM organization, the CM procedures for the programme as mutually agreed by all stakeholders and those responsible for CM
19. **Configuration Status Accounting (CSA)** The recording and reporting of the information that is needed to manage the configuration effectively, including a list of approved configuration documentation, the status of proposed changes to the configuration and the implementation status of approved changes. (ACMP 6)
20. **Configuration Status Record.** Record produced by the CSA process. It is the source database of configuration information to support the through life programme activities, including programme management, system engineering, manufacturing, software development, logistic support, maintenance and modification. The CSR should describe the status of the CI at any stage in its life cycle. (DEFSTAN 05-57)
21. **Contract Data Requirements List (CDRL).** A list of the data requirements that are authorized for a specific Acquisition; the CDRL forms part of the contract and direct the contractor to prepare and deliver data that satisfies specific approval and acceptance criteria. (ACMP 6)
22. **Design Organisation.** The organization entrusted to design the materiel to approved specifications. (ACMP 6)

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

23. **Design Record.** All information necessary to define the design, manufacture, packaging, testing, installation and servicing of a product. (DEFSTAN 05-57)
24. **Design Review.** A formal, documented engineering management process that is used to subject a design to a systematic critical study. Its purpose is to establish that the design satisfies the specified requirements. (DEFSTAN 05-57)
25. **Developmental Configuration.** The Supplier's technical documentation that defines the evolving configuration (design) during development; it is under the development Supplier's configuration control. (ACMP 6)
26. **Dispositioning Authority.** A person or group of persons, assigned responsibility and authority to make decisions on product configuration as defined in the requirements for product design, realisation, verification, operation and support. Note that a Dispositioning Authority; can also be known as a Configuration Control Board (CCB). Other Relevant interested parties within and outside the organization should be represented on the CCB. (ISO 10007)
27. **Engineering Change.** An alteration in the configuration of a CI and / or its configuration documentation after formal establishment of its configuration baseline. (ACMP 6).
28. **Engineering Change Proposal.** The formal documentation that is prepared to provide information in support an engineering change. (ACMP 6).
29. **Engineering Data.** All information associated with all engineering activities and recorded in documents such as drawings, associated lists, accompanying documents, manufacturer specifications, and standards, prepared by a design activity and relating to the design, manufacture, procurement, test, or inspection of items or services. (ACMP 6)
30. **Functional Baseline (FBL).** The configuration documentation formally designated during the Assessment Phase prescribing all necessary; functional characteristics; test requirements; CI interface characteristics associated with Key lower-level CI if any; and Design constraints. (ACMP 6)
31. **Functional Characteristics.** The initial design expressed in terms of quantitative performance parameters such as range, speed, lethality, reliability, maintainability, safety, and operating, logistics parameters. (ACMP 6)
32. **Functional Configuration Audit.** Formal examination of test data and quality assurance records for a CI, prior to acceptance of the Product Baseline (PBL), to verify that the CI has achieved the performance and functional characteristics specified in configuration documentation. (DEFSTAN 05-57)
33. **Firmware.** An ordered set of instructions and associated data stored in a way that is functionally independent of main storage, usually in a ROM. (ACMP 6)
34. **Formal Engineering Change Proposal (ECP).** The formal documentation that provides engineering information and other data in sufficient detail to support an engineering change proposal, its approval and its contractual authorization. (ACMP 6)
35. **Interface Control.** The delineation of the procedures and documentation, both administrative and technical, necessary for the identification and management of Functional and Physical Characteristics between two or more systems or CI. (ACMP 6)

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

36. **Materiel.** A generic term covering: complete systems, subsystems, assemblies, components, spare parts and material consumables, including computer software and firmware, and their related engineering data and documentation manuals. (ACMP 6)
37. **NATO Stock Number.** A 13–digit numeric data string, which on its own identified an Item of Supply in the NATO inventory. (DEFSTAN 05-57)
38. **Non Developmental Item.** A procured or procurable item available in the commercial market place requiring no modification to meet the requirements of the Authority. (DEFSTAN 05-57)
39. **Part Number.** A set of numbers, letters, symbols, or some combination thereof, assigned to uniquely identify the design of a specific part or item of materiel. (ACMP 6)
40. **Physical Characteristics.** Quantitative and qualitative expressions of material features; such as composition, dimensions, finishes, form, fit, and their respective tolerances. (DEFSTAN 05-57)
41. **Physical Configuration Audit (PCA).** Formal examination of the “as built” configuration of a CI to verify that it conforms to its product configuration documentation. (DEFSTAN 05-57)
42. **Product Baseline (PBL).** The configuration documentation for a CI formally designated at the beginning of Production prescribing:
- a. All necessary physical and functional characteristics of CIs; the selected functional characteristics designated for production acceptance testing.
 - b. The production acceptance tests. (DEFSTAN 05-57)
43. **Product Configuration Information.** Requirements for product design, realization, verification, operation and support. (ISO 10007:2003)
44. **Requirements Baseline.** A documented common understanding of what the product is expected to do (its functional and performance requirements). It defines the capabilities the customer expects to receive from the product. (DEFSTAN 05-57)
45. **Software Release.** A configuration management action whereby a particular version of software is made available for a specific purpose (e.g. released for test). (ACMP 6)
46. **System.** Contains the total package of parts, through sub-systems and includes related facilities, items, material, services, and personnel required for its operation to the degree that it can be considered a self-sufficient item in its intended operational or non-operational and/or support environment. (ACMP 6)
47. **Technical Data.** Recorded information of a technical nature, regardless of form or characteristics; Technical Data may document research, developmental, or engineering work or be used to define a design or process or to procure, support, maintain, or operate materiel. The data may be graphic or pictorial delineation in media such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts. Technical Data does not include computer software. (DEFSTAN 05-57)

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

48. **Technical Review.** A management review conducted at logical transition points, used to determine the contractor's progress and compliance to technical and contractual requirements. (ACMP 6)

49. **Verification.** Confirmation, by objective evidence, that the product meets the physical and functional requirements for which it was designed and conforms to specified requirements.

50. **Version Description Document (VDD).** A Version Description Document (VDD) identifies and describes a version of a Computer Software Configuration Item (CSCI) and identifies, by reference to the applicable Engineering Change Proposal and Notices all changes to the CSCI since the last VDD was issued. (ACMP 6)