Australian Government
Department of Defence
Capability Acquisition and Sustainment Group

# CASG HANDBOOK

# (E&T) 12-2-003 TECHNICAL DATA MANAGEMENT

**VERSION: 1.1**

## Approving Authority:

richard.jones1 Digitally signed by richard.jones1 Date: 2019.08.06 10:15:22 +10'00'

**R.P. JONES**
Director Systems Engineering
for **N.R. BATES**
A/Chief Engineer CASG
Engineering and Technical Function Lead

This CASG Handbook is issued as an Informative Annex to supplement CASG Policy (E&T) 12-2-003 issued under the CASG Manual (CP) 001 – CASG Quality Management System

## Revised Document

CASG Handbook (E&T) 12-2-003 V1.1 updates and replaces DMH (ENG) 12-2-003 Technical Data Management Handbook version 1.0.

# DOCUMENT HISTORY

| Version | Date | Changes[1] |
|---|---|---|
| 1.0 | August 2015 | Original Issue of DMH(ENG) 12-2-003 Developed during 1QMS Program |
| 1.1 | July 2019 | Administrative update to align to FPR Changes. Re-issued as CASG Handbook (E&T) 12-2-003 |
| | | |

**Review Date:** Two years from date of approval.

[1] Major changes to content will also be identified by Change Bars in the left hand margin of the document

# TABLE OF CONTENTS

# ABBREVIATIONS AND DEFINITIONS

## Abbreviations

| | |
|---|---|
| **AGLS** | Australian Government Locator Service |
| **ATE** | Automatic Test Equipment |
| **CASG** | Capability Acquisition and Sustainment Group |
| **CDRL** | Contract Data Requirements List |
| **CI** | Configuration Item |
| **CLC** | Capability Life Cycle |
| **CM** | Configuration Management |
| **COTS** | Commercial Off the Shelf |
| **CSA** | Configuration Status Accounting |
| **DAL** | Data Accession List |
| **DI** | Developmental Item |
| **DID** | Data Item Description |
| **DMS** | Data Management System |
| **DPPM** | Defence Procurement Policy Manual |
| **FIC** | Fundamental Inputs to Capability. |
| **FMA** | Financial Management and Accountability |
| **FMECA** | Failure Mode and Effects Criticality Analysis |
| **FMS** | Foreign Military Sales |
| **FPS** | Function and Performance Specification |
| **GFD** | Government Furnished Data |
| **GFI** | Government Furnished Information |
| **IETM** | Interactive Electronic Technical Manual |
| **IETP** | Interactive Electronic Technical Publication |
| **IT** | Information Technology |
| **ITAR** | International Traffic in Arms Regulations |
| **IP** | Intellectual Property |
| **ISP** | Integrated Support Plan |
| **LCC** | Life Cycle Cost |
| **LIMS** | Logistic Information Management Systems |
| **LOT** | Life of Type |
| **LSA** | Logistic Support Analysis |
| **NAA** | National Archives of Australia |
| **OCD** | Operational Concept Document |
| **OEM** | Original Equipment Manufacturer |
| **OTS** | Off the Shelf |
| **PBS** | Product Breakdown Structure |
| **PES** | Project Execution Strategy |
| **RCM** | Reliability Centred Maintenance |
| **RECMAN** | Records Management Policy Manual |

## Abbreviations (con't)

| | |
|---|---|
| **SOW** | Statement of Work |
| **SS** | System Specification |
| **SSCC** | Support System Constituent Capabilities |
| **SSDESC** | Support System Description |
| **TCD** | Test Concept Document |
| **TD** | Technical Data |
| **TDL** | Technical Data List |
| **TDP** | Technical Data Plan |
| **TDRA** | Technical Data Requirements Analysis |
| **TDSR** | Technical Data and Software Rights |
| **TDT** | Technical Documentation Tree |
| **RTM** | Requirements Traceability Matrix |
| **VCRM** | Verification Cross Reference Matrix |
| **WBS** | Work Breakdown Structure |

## Definitions

| | |
|---|---|
| **Capability Life Cycle** | The Capability Life Cycle is the process of introduction, sustainment, upgrade and replacement of Defence capability, of which Products are the enduring elements. The Defence Capability Portfolio is a collection of Programs that aggregate component Products at varying stages of their individual life cycles. A project is a discrete activity to introduce, upgrade or replace a Product (Interim Capability Life Cycle Manual) |
| **Configuration Item** | A product, allocated components of a product, or both, that satisfies and end user function, has distinct requirements, functionality and/or product relationships, and is designated for distinct control. (EIA-649-C) |
| **Integration** | The bringing together of components and ensuring that they function together. Components can be any combination of subsystems, systems, projects or FIC elements. |
| **Intellectual Property** | Rights relating to:<br>• literary, artistic, industrial, technical and scientific works;<br>• performances of performing artists, phonograms and broadcasts;<br>• inventions in all fields of human endeavour;<br>• registered and unregistered designs including industrial designs;<br>• trade marks, service marks and commercial names and designations;<br>• trade secrets, know-how; and<br>• all other rights from intellectual activity in the industrial, scientific, literary or artistic fields. |
| **Interface** | The boundary where two items are required to pass information between them. |
| **Materiel System** | A subset of the Capability System and is the combination of the Mission System(s) and the Support System. The Materiel System covers those aspects of the Fundamental Inputs to Capability (FIC) that are provided by the acquisition agency. |
| **Mission System** | The Mission System is that element of the Materiel System that directly performs the operational function. Examples include platforms (e.g., ship, tank, or aircraft), distributed systems (e.g., communications network), and discrete systems that integrate into other Mission Systems (e.g., a radar upgrade for a platform). Major components of the Support System (such as simulators, Automatic Test Equipment (ATE) and Logistic Information Management Systems (LIMS)) could also be classified as Mission Systems if the level of management attention to be applied to these components warranted this classification. |
| **Product** | A product is defined as any measurable, tangible, verifiable outcome, result, item or deliverable service, which must be produced or delivered (or both) to complete a project or part of a project. Products include component products. Depending on context, a product may be any component or combination of components in the system from any level or levels in the hierarchy. A product in CASG context is generally part of a capability system, including elements of both the Mission System and the Support System. |
| **Product Technical Data** | Technical Data related directly to a Product of interest. |
| **Support System** | The organisation of hardware, software, materiel, facilities, personnel, processes, and data required to enable the Mission System to be effectively operated and supported so that the Mission System can meet its operational requirements. |
| **System** | An integrated composite of people, products and processes that provides a capability to satisfy a stated need or objective. A system is a combination or assembly of hardware, software, principles, doctrines, methods, ideas, procedures and workforce, or a combination of them, arranged or ordered towards a common objective. |
| **Systems Engineering** | An interdisciplinary approach that encompasses the entire technical effort, and evolves into and verifies an integrated and life-cycle balanced set of systems, people, products, and process solutions that satisfies customer needs. |
| **Technical Data** | Recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term technical data does not include computer software or data incidental to contract administration, such as financial or management information. |
| **Test and Evaluation** | A process to obtain information to support the objective assessment of a capability system with known confidence, and to confirm whether or not a risk is contained within acceptable boundaries across all facets of a system's life cycle. A test is an activity in which a scientific method is used to obtain quantitative or qualitative data relating to the safety, performance, functionality, contractual compliance, and supportability of a system. Evaluation is the analysis of test results to determine (verify) or prove (validate) something. |
| **Validation** | Proof through evaluation of objective evidence that the specified intended end use of a product or system is accomplished in an intended environment. |
| **Verification** | Confirmation through the provision of objective evidence, that specified requirements have been fulfilled. |

# TECHNICAL DATA MANAGEMENT

## REFERENCES

A. *Archives Act 1983 (Cwlth)*
B. AS/NZS ISO 9000 Quality management and quality assurance standards
C. ASDEFCON(Complex) Australian Standard for Defence Contracting (Complex Materiel) Template
D. ASDEFCON(SM) Australian Standard for Defence Contracting (Strategic Materiel) Template
E. ASDEFCON(Support) Australian Standard for Defence Contracting (Support) Template
F. CLCM Defence Capability Life Cycle Manual
G. DEF(AUST) 5629 Production of Military Technical Manuals
H. DEF(AUST) 5664 Work Breakdown Structures for Defence Materiel Projects
I. DEFLOGMAN P2V10C10 Defence Logistics Manual Part 2, Volume 5, Chapter 10 Disposal of Defence Assets
J. DEFLOGMAN P2V5C19 Defence Logistics Manual Part 2, Volume 5, Chapter 19, Procurement of Materiel and Services from the United States of America under the Foreign Military Sales Program
K. DEFLOGMAN PsV10C5 Defence Logistics Manual Part 2, Volume 10, Chapter 5 Acquisition and Management of Technical Data
L. *Designs Act 2003 (Cwlth)*
M. RECMAN Records Management Policy Manual
N. DEFLOGMAN P2V5C28 Defence Logistics Manual Part 2, Volume 5, Chapter 28 Export/supply and import of Defence and dual-use goods and technology and the use of Government end-user assurances
O. CASG Handbook (E&T) 12-3-003 CDD Guide
P. CASG Handbook (E&T) 12-3-005 Functional and Performance Specification (FPS) Development Guide
Q. CASG Handbook (E&T) 12-5-001 Defence Materiel Verification and Validation Guide
R. CASG Policy (E&T) 12-2-003 Acquisition and Management of Technical Data
S. DSPF Defence Security Principles Framework
T. EIA-632 Processes for Engineering a System, American National Standards Institute / Electronic Industries Association
U. EIA-649 National Consensus Standard for Configuration Management
V. *Environment Protection and Biodiversity Conservation Act 1999 (Cwlth)*
W. *Evidence Act 1995 (Cwlth)*
X. *Freedom of Information Act 1982 (Cwlth)*
Y. IPMAN Defence Intellectual Property Manual
Z. MIL-STD-31000 Technical Data Packages
AA. MIL-STD-974 Contractor Integrated Technical Information Service
BB. *Privacy Act 1988*
CC. *Work Health and Safety Act 2011 (Cwlth)*

## INTRODUCTION

1. Technical data is critical to both the acquisition and through-life support of materiel systems. Defence needs to collect and maintain the appropriate technical data with the necessary Intellectual Property (IP) rights, so that the right technical data is available to the right people at the right time in a format that is fit for purpose over its life.

2. Technical data includes technical know-how and information reduced to material form (including digital form) relating to a materiel system, and includes data, manuals, handbooks, designs, standards, specifications, reports, writings, models, sketches, plans, drawings, calculations, software documentation and source code, test results and other items describing or providing information relating to the materiel system. Product data of a more general nature (e.g. general catalogues and brochures etc.) is not considered technical data. The term technical data does not include computer executable code (which forms part of the product) or data related to organisational and contract administration such as financial or management information.

3. The requirement for technical data is first considered in the Strategy and Concepts Phase of the Capability Life Cycle. Analysis during the development of the materiel system support concepts and requirements will begin to shape the technical data and IP rights required to meet the support system constituent capabilities of an acquisition project.

## SCOPE

4. This Handbook is intended as a guide to assist Capability Acquisition and Sustainment Group (CASG) personnel to manage technical data and related IP associated with materiel systems acquisition and sustainment. This Handbook should be read in conjunction with the related documents referenced above.

## HANDBOOK OVERVIEW

5. The range of information considered to be technical data can be shown as a hierarchy of information categories illustrated by Figure 1. Technical data does not include financial, contract management and administrative data (e.g. contract master schedules, project management plans, risk management plans, contract status reports and meeting agendas/minutes etc.).

6. Technical data (Figure 1) can be considered as belonging to three broad categories (with some overlap) which are described by:

a. **Technical Product Definition Information.** Information that describes the product's performance, functional and physical attributes, including requirements and design information. Product definition information provides the technical basis for actions taken during all product life cycle phases, for product validation and for product operational information. Product definition information provides the basis for effective identification of materiel and ADF inventory cataloguing.

b. **Technical Product Operational Information.** Information that is derived from the product definition information. Product operational information consists of procedures and technical information needed by operators and support personnel to operate, maintain and dispose of the product.

c. **Technical Associated Information.** Information generated as part of the product development, delivery and lifecycle management process, but is not clearly definable as either product definition information or product operational information.

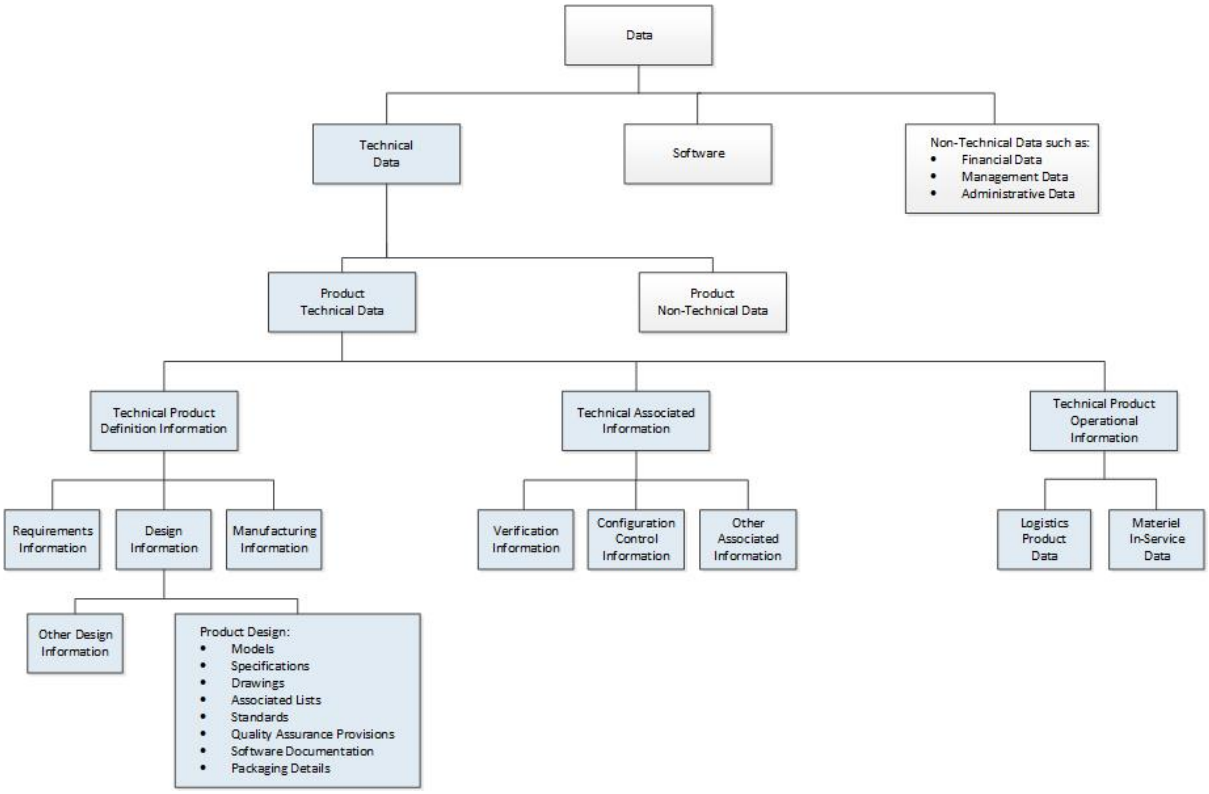


**Figure 1 – Hierarchy of Technical Data Categories**[2]

7. Some of the uses and typical examples of product technical data are listed in Table 1. This is list is not exhaustive and provides only a subset of technical data items as examples.

**Note:** Project and engineering managers should be aware that terms such as 'technical data', 'product data' and 'TDP' are often imprecise in their definition, not necessarily equivalent and often used inconsistently.

[2] This figure is based on the data structure illustrated in MIL-STD-31000B.

**Table 1 – Typical Uses for Product Technical Data**

| | Information Category | Use | Typical Examples |
|---|---|---|---|
| **Technical Product Definition Information** | **Requirements Information** | Captures and documents:<br>• how a system/component will be used,<br>• what functions must be performed,<br>• level of performance required,<br>• which constraints will apply, and<br>• traceability of requirements through the product hierarchy. | Operational Concept Documents<br>Function and Performance Specifications<br>System Specifications<br>Support System Specifications<br>Software Requirements Specifications<br>Requirements Traceability Matrices |
| | **Design Information** | Captures, documents and records:<br>• how a design was performed,<br>• why certain design decisions are made, and<br>• what components were selected and why. | Logical models<br>Product Models<br>Product Drawings<br>Software Design Descriptions<br>Design Documentation<br>System Architecture Description<br>Trade Study Reports<br>Safety Data Sheets<br>Codification Data |
| | **Manufacturing Information** | Documents and records:<br>• what will be manufactured,<br>• how it will be manufactured,<br>• components required for manufacture, and<br>• any specific processes required. | Circuit Schematics<br>Printed Circuit Board Layout Files<br>Assembly Drawings<br>Parts Lists<br>Bills of Material<br>Engineering Drawings<br>Computer Software Source Code |
| **Technical Associated Information** | **Verification Information** | Captures, documents and records:<br>• validation and verification concepts,<br>• validation and verification planning,<br>• validation procedures and results,<br>• verification procedures and results, and<br>• traceability from requirements to validation and verification results. | Test Concept Documents<br>Test & Evaluation/Acceptance Master Plans<br>Acceptance Test Plans, Procedures, Reports & Results<br>Test Procedures & Results<br>Verification Cross Reference Matrices |
| | **Configuration Control Information** | Documents and records:<br>• system or component configuration,<br>• configuration at specific instances such as:<br>o baseline,<br>o version release or upgrade, or<br>o product issue, and<br>• constituent parts and processes. | Master Record Indices<br>Configuration Status Accounting Reports<br>Engineering Drawings<br>Parts Lists<br>Software Version Description Documents<br>Configuration Identifiers<br>Configuration Baselines |
| | **Other Associated Information** | Captures, documents and records:<br>• associated information not in verification or configuration control categories. | GIDEP Notices of Obsolete Parts<br>Suppliers Notices of Obsolete Parts<br>Disposal Information |
| **Technical Product Operational Information** | **Logistics Product Data** | Documents and records:<br>• system or component availability and reliability,<br>• sparing analysis,<br>• preventive/corrective maintenance procedures<br>• repair/replace procedures,<br>• support & test equipment requirements,<br>• software support requirements, and<br>• training needs. | Failure Modes & Effect Criticality Analyses<br>Reliability Centred Maintenance Reports<br>Level of Repair Analyses<br>Logistic Support Analyses<br>Training Needs Analysis Reports<br>Support & Test Equipment Plans and Provisioning Lists<br>Support Plans |
| | **Materiel In-Service Data** | Documents, defines or provides:<br>• spares holdings and usage,<br>• technical publications,<br>• training records,<br>• electronic manuals,<br>• servicing frequencies and inspection criteria,<br>• determination of materiel useability<br>• interactive electronic manuals, and<br>• system and component availability records | Codification Data<br>Spares Lists<br>Publication Packages<br>Operator, Maintenance Manuals<br>Servicing and Inspection Instructions<br>Software Operator / User Manuals<br>Maintenance Management System Data<br>Interactive Electronic Technical Manuals<br>Defect Reports<br>Training Materials<br>Operator/Maintainer Training Courses |

## How much Technical Data?

8. One of the fundamental issues involving technical data is how much is required. Technical data is a resource with an associated cost. If technical data is insufficient or inadequate then Life Cycle Cost (LCC) may increase as support functions may not be able to be performed or may not be performed efficiently and cost effectively (**Error! Reference source not found.**). In addition, insufficient technical data may adversely impact on risk identification and management. However, too much technical data can result in excessive costs and demands on Commonwealth resources and may create an adversarial and unhelpful relationship with the contractor(s) and/or supplier(s).

9. Often requirements for technical data have to be identified early in the Capability Life Cycle when the materiel system's product breakdown structure is not completely known (e.g. before contract award). Attempting to obtain as much data as possible is to be avoided without significant consideration of known materiel system details.

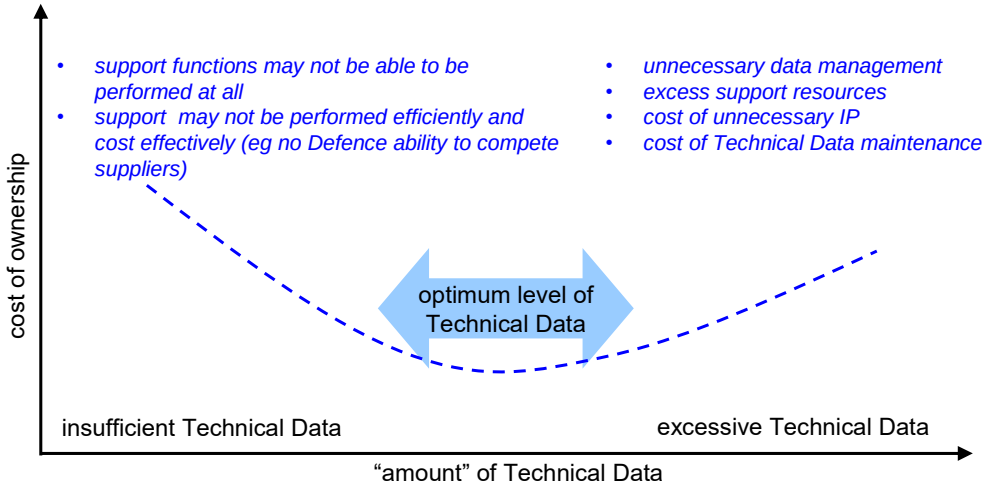


**Figure 2 – Optimum Level of Technical Data**

# TECHNICAL DATA MANAGEMENT

## Technical Data Management Activities

10. Technical Data Management includes the following activities, as shown in Figure 3, although the extent and depth of involvement by CASG staff will vary based on acquisition, sustainment and contracting arrangements:

a. identification of technical data requirements, including content and any required format, through a Technical Data Requirements Analysis (TDRA);

b. acquisition and creation of technical data, including consideration of the IP rights associated with technical data;

c. verification, validation and acceptance of technical data;

d. storage, maintenance and configuration control of technical data;

e. use, distribution and exchange of technical data; and

f. archiving and disposal of technical data.

11. Technical data management also includes:

a. understanding, obtaining and protecting Commonwealth owned data and associated IP rights (as well as rights licenced by third parties to the Commonwealth);

b. retaining the ability to achieve future competition goals;

c. maximising options for product support; and

d. enabling performance of downstream life cycle functions.

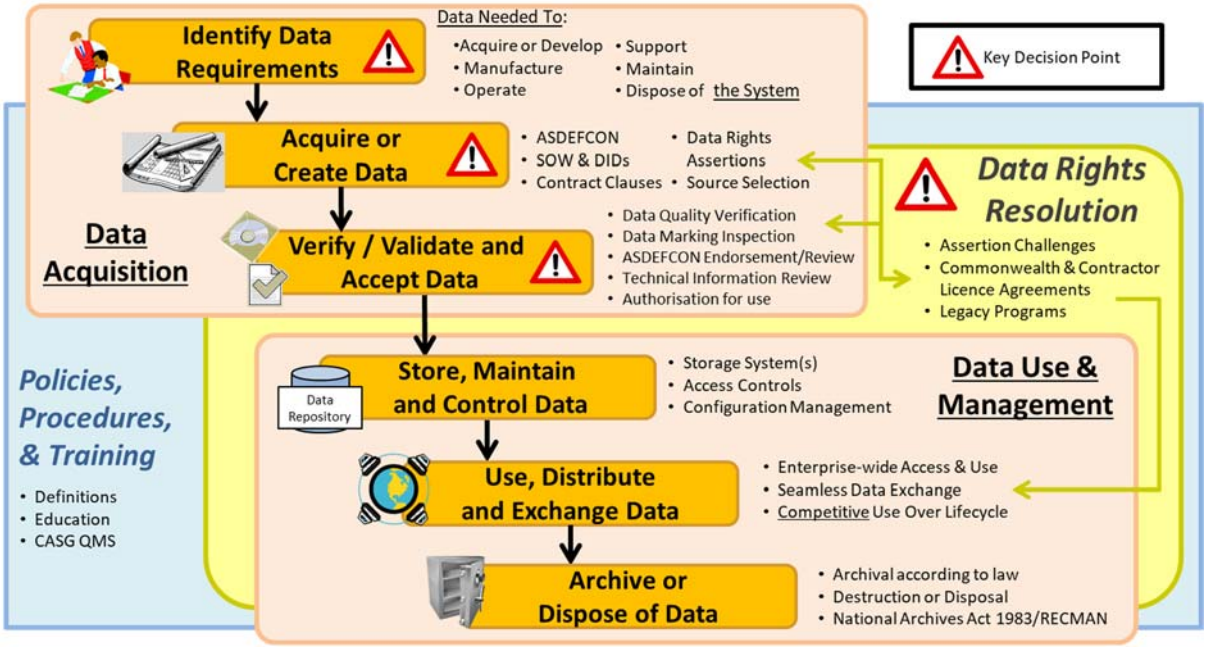


**Figure 3 – Technical Data Management Activities**

## Technical Data in the Capability Life Cycle

### Life Cycle Phases Overview

12. The Capability Life Cycle (CLC) has four phases as shown in **Error! Reference source not found.**. CASG provides a Materiel System as a component of the Capability System, and also has coordination responsibilities with providers of other elements of the Fundamental Inputs to Capability.

13. Defence's understanding and requirements for technical data can change throughout the CLC, evolving as the state of the system design and associated support concepts develop.

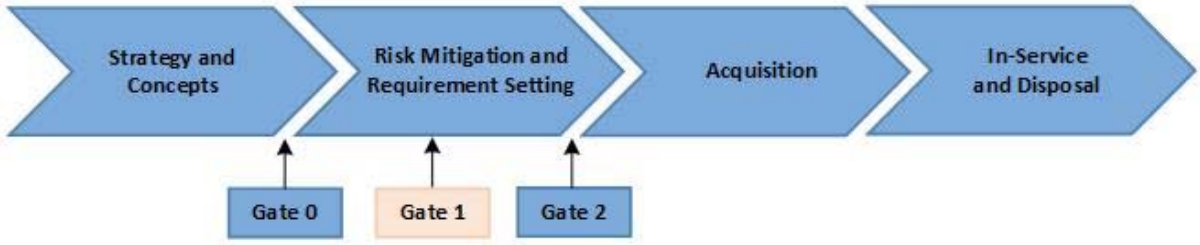


**Figure 4 – Capability Life Cycle Phases**

14. Technical data management activities occur across all phases of the CLC. Some activities are more likely to occur during certain CLC phases than others. For example, acquisition or creation of technical data occurs predominantly during the Acquisition phase of a Materiel System.

15. **Error! Reference source not found.** identifies the CLC phases during which the information category of technical data is most likely to be generated. Refer to the Capability Life Cycle Manual for detailed information on the approach to capability development in Defence.

**Table 2 – Information Categories of Technical Data generated during the CLC**

| Information Category | CLC Phases | | | |
|---|---|---|---|---|
| | Strategy & Concepts | Risk Mitigation & Requirements Setting | Acquisition | In-Service & Disposal |
| Requirements Information | ✓ | ✓ | ✓ | ✓ |
| Design Information | | ✓ | ✓ | ✓ |
| Manufacturing Information | | ✓ | ✓ | ✓ |
| Verification Information | | ✓ | ✓ | ✓ |
| Configuration Control Information | | ✓ | ✓ | ✓ |
| Logistics Product Data | | | ✓ | ✓ |
| Materiel In-Service Data | | | ✓ | ✓ |

**Strategy and Concepts Phase**

16. The Strategy and Concepts Phase identifies capability needs to meet the Defence missions set out in strategic guidance.

17. Decisions during this phase, in particular in relation to support concepts and the execution strategy, will influence the nature of technical data required to cost-effectively support the materiel system through life.

**Risk Mitigation and Requirements Setting Phase**

18. Technical data created during this phase will mainly comprise requirements information, and possibly some preliminary design information and/or verification information. This includes information that provides evidence of technical suitability of potential solutions.

19. During this Phase, an Operational Concept Document (OCD) and Function and Performance Specification (FPS) or equivalent are developed, along with strategies and plans for project execution and through-life support, ready for implementation in later phases. The OCD includes key information on the support concept, which becomes a key driver for determining the necessary Technical Data. The information in these documents allows for the development of draft contracts and other agreements for the acquisition of the capability. In the early stages of this Phase, it may not be possible to perform a comprehensive TDRA, however, there may be enough information to commence identification and some definition of initial technical data requirements.

20. Proposed solutions evolve through interaction between Defence and industry and the technical data requirements and overall approach will be revised based on these proposals. Considerations also include the potential re-use of existing Defence or Allied data which will become Government Furnished Date or Information under a contract, with associated benefits and risks. By the end of this phase there should be sufficient understanding of the requirements to enter into contractual negotiations for the acquisition, with technical data provisions appropriate for the acquisition, transition and through life support (including disposal) of the system.

**Acquisition Phase**

21. Final technical data requirements will be negotiated and included in the contract. The contract should also reflect any restrictions, limitations, or licensing obligations applying to technical data. Acquisition includes not only the mission system(s), but also the support system. Support analysis is conducted in this phase to identify the operating and support tasks and the data necessary to be able to perform them.

22. The full scope of the technical data requirements evolves during the acquisition phase, typically with a baseline established at contract award and achieving maturity by Support System Detailed Design Review.

23. In this phase, the system design will be finalised and the full scope of technical data will be known and should be reviewed against the TDRA.

### In-Service and Disposal Phase

24. During the In-Service and Disposal Phase, the focus for technical data management shifts to its use, access, means of distribution and controlled evolution through system changes. Often, the users of technical data will be organisations other than the acquisition agency and acquisition (or original) contactor. Requirements for access, means of distribution and control of technical data need to be understood and evolved (refer to CASG Handbook (E&T) 12-2-002 *Configuration Management* for guidance on configuration control of technical data).

25. Support arrangements need to consider the ongoing support for technical Data including its management, storage, maintenance and evolution.

26. The TDRA conducted during the Acquisition Phase will need to be reviewed and updated In-Service. Support contracts will need to consider the technical data required to address the required services and the associated IP rights. Technical data requirements need to be regularly reviewed and reassessed for any change in mission system role, configuration and operating environment, change to the support strategy, or any change in support arrangements outside of the agreed support strategy.

27. Technical data will be needed to support disposal activities. Technical data will also need to be archived or destroyed. Technical data generated during this phase will mainly be Configuration Control information as well as safety, security and environmental compliance related data with the exception of a re-sale/gifting which will require a wider range of information.

## Identification – Technical Data Requirements Analysis

### Introduction

28. Technical data requirements analysis (TDRA) is an ongoing activity that evolves with the system design across the lifecycle. Technical data is needed to:

a. support the acquisition of a product;

b. operate and sustain the product over its Life-of-Type (LOT) under changing operational, technical and business environments;

c. support the materiel assurance process;

d. support future re-competition for item acquisition, upgrades and sustainment activities in the interest of achieving cost savings, where this is identified as part of an overall PES and support strategy; and

e. support the disposal of a product.

29. The TDRA should:

a. identify the nature of activities that will be undertaken for a project or product;

b. identify the technical data needed for a project or product throughout its life cycle;

c. Identify the IP rights required by the Commonwealth with respect to contractor supplied or generated technical data by reference to the identified purpose or use of that technical data;

d. ensure that technical data requirements are progressively refined and reviewed prior to each major decision point in the Capability Life Cycle;

e. consider technical data (and associated IP) from the perspective of total cost of asset ownership[3]; and

f. consider any specific naming conventions for identifying Configuration Items, components

[3] Potential long-term cost savings from being able to compete sustainment activities need to be balanced against the up-front costs of acquiring additional technical data and associated rights.

and associated data[4].

30. In-service, technical data is one of the fundamental support resources needed for each of the Support System Constituent Capabilities (SSCC), i.e. Operating Support, Engineering Support, Maintenance Support, Supply Support and Training Support. A deliberate process of Logistic Support Analysis (LSA)[5] should be used to define support system requirements and identify and analyse support tasks and associated data for each SSCC.

31. The TDRA process will:

a. define the system requiring technical data;

b. identify activities that require technical data;

c. identify the required type and content of technical data;

d. identify the users of technical data;

e. identify the IP rights required by the Commonwealth in relation to technical data; and

f. define the required format for the technical data.

**System Definition**

32. A Capability System is the necessary combination of the Fundamental Inputs to Capability (FIC) to achieve the required effect (capability). The Materiel System is a component of the Capability System which is the combination of one or more Mission Systems and the Support System (shown in Figure 6) and it covers those aspects of the FIC that are supplied by the acquisition agency.

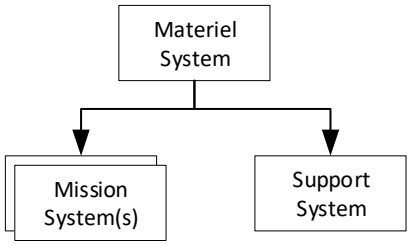


**Figure 6 – Materiel System Breakdown**

33. The mission system is that element of the capability that directly performs the operational function. Examples include platforms (e.g. ship, tank, or aircraft), distributed systems (e.g. communications network) and discrete systems that integrate into other mission systems (e.g. a radar upgrade for a platform). Major support system components (such as simulators, automatic test equipment and logistic information management systems) could also be classified as mission systems if the level of management attention to be applied to these components warranted this classification.

34. The support system is the organisation of hardware, software, materiel, facilities, personnel, processes, and data required to enable the mission system to be operated effectively and supported so that the mission system can meet its operational requirements. A support system also includes the support required for support system components. The support system embraces the support responsibilities undertaken by Defence and in-service support contractors, subcontractors or other suppliers.

35. Any system (mission or support) can be represented by a structured hierarchy of component products, the Product Breakdown Structure (PBS), as shown in Figure 7. A product is any tangible item, which is produced or delivered (or both) to complete a project or part of a project. A product may be any component or combination of components in the system from any level or levels in the hierarchy, including support and training equipment.

---

4 The S series international standards provide guidance on these aspects.

5 Further guidance on LSA is contained in Materiel Logistics function policies and guidance.

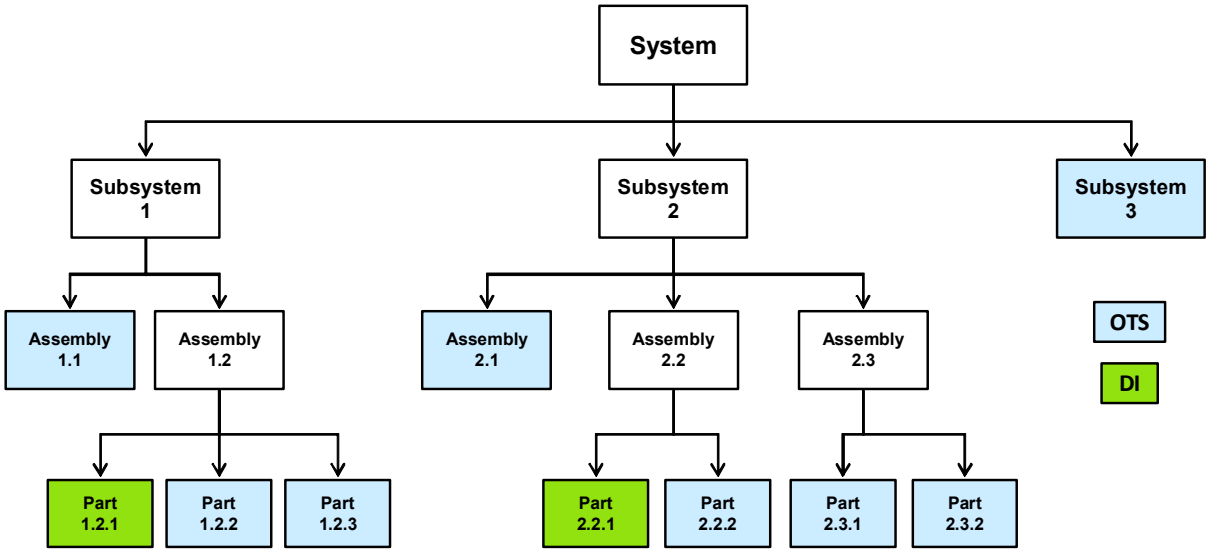


**Figure 7 – Example of Product Breakdown Structure**

36. The lowest level elements of a PBS would consist of raw materials used to manufacture a product. In practice, the branches of the structure end with off-the-shelf (OTS) or developmental item (DI) components (**Error! Reference source not found.**). The system is effectively assembled from these lowest level components. Lowest level components have no further decomposition and can occur at any level in the hierarchy. Components at any level may be a Configuration Item (CI).

37. The PBS is developed progressively from concept through implementation, and can only be completely defined after the conclusion of detailed design. Early versions of the PBS will be used to help scope the system, frame the associated work requirements and form the basis of a contract Work Breakdown Structure (WBS). The technical data needed for a system will be established progressively as the PBS and system solution evolve. The PBS will continue to evolve over the full service life of the system until final disposal.

**Technical Data Associated with a System**

38. The acquisition and support concept for the materiel system and its components will provide the foundation to identify the associated technical data needed by Defence. In lieu of a detailed support concept, a broader support strategy should be documented. It identifies the expected activities for each component that will be conducted by Defence, or another organisation on Defence's behalf. These expected activities will define the requirement for specific technical data and identify the organisations that need to use it.

39. All the components in a system's PBS hierarchy, including those that just represent the integration of lower level components, will have associated technical data. Defence needs some of this technical data to address the activities Defence expects to conduct, or to provide technical data to organisations conducting current or future activities on Defence's behalf.

40. The application of acquisition and support concepts to each component in the hierarchy, particularly lowest level components, will determine the types and quantity of technical data required. Issues to be resolved include what level of maintenance is required for a component and which organisation will perform the specified maintenance.

41. As an example of the types or information category of technical data that may be required, the following acquisition strategies and support concepts for a subset of the PBS components in Figure 7 could be as follows:

a. Assembly 1.1 is an off-the-shelf component acquired from a supplier; installed, tested and accepted by Defence who will also conduct all operational maintenance.

b. Assembly 1.2 is a developmental component as it consists of a combination of a developmental item and off-the-shelf components in Parts 1.2.1, 1.2.2 and 1.2.3.

c. Part 1.2.1 is a developmental item component which has been developed by a contractor on

Defence's behalf. Defence plans to implement upgrades and re-manufacture them at 5 year intervals throughout the LOT with the original or alternative contractor. This component will be maintained and supported by Defence throughout its LOT. Defence expect to contract elements of this support, including to the original contractor.

d. Parts 1.2.2 and 1.2.3 are off-the-shelf components acquired from a supplier; installed and tested by Defence who will also conduct operational maintenance.

42. Only the top level system component and subsystem 1 components have been considered for brevity as they will be sufficient to demonstrate technical data requirements. Based on the example system and product breakdown shown in Figure 7, Table 3 lists the information categories and examples of typical technical data that could be associated with this subset of the PBS. The examples in Table 3 are not exhaustive but it serves to illustrate the types of technical data that may be required for a system structure as shown in Figure 7.

**Table 3 – Examples of Technical Data associated with a System Breakdown Structure**

| Product | Technical Data | |
|---|---|---|
| | **Information Category** | **Examples** |
| System | Requirements | Function & Performance Specification, System Specification, Support System Specification |
| | Design | System Architecture Description, Logical and Physical Models of the Solution, System Design Document, Trade Study Reports |
| | Verification | Test & Evaluation Master Plan, Acceptance Test Procedure and Results |
| | Configuration Control | Master Record Index, Baseline Configurations |
| Subsystem 1 | Requirements | Subsystem Specification, Requirements Traceability Matrix |
| | Design | Design Documentation, Functional Models |
| | Verification | Acceptance Test Procedure, Report and Result |
| | Configuration Control | Allocated and Product Baseline Configurations |
| Assembly 1.1 | Requirements | Procurement Specification |
| | Design | Product Models, Engineering Drawings (External Interfaces) |
| | Verification | Acceptance and Production Test Procedures and Results |
| | Configuration Control | Product Baseline Configuration |
| | Installation | Software Version Descriptions, Installation Drawings |
| | Logistics Product Data | FMECA Reports, Interactive Electronic Technical Manuals, Maintainer Training Courses |
| | Material In Service Data | Spares Lists, Demand Data from Field Requisitions, Item Prognostics & Diagnostics Information |
| Assembly 1.2 | Requirements | Development Specification |
| | Design | Design/Development Documentation |
| | Verification | Acceptance Test Procedures and Results |
| | Configuration Control | Product Baseline Configuration |
| | Manufacturing | Assembly Drawings, Bill of Materials |
| | Logistics Product Data | FMECA Reports, RCM Reports, Support & Test Equipment Provisioning Lists, Interactive Electronic Technical Manuals, Maintainer Training Needs Analysis Reports, Maintainer Training Courses |
| | Material In Service Data | Item Prognostics & Diagnostics Information, Field Quality Deficiency Reports, Field Supply Deficiency Reports |

**Table 3 – Examples of Technical Data associated with a System Breakdown Structure *con't***

| | | |
|---|---|---|
| Part 1.2.1 | Requirements | Development Specification |
| | Design | Design/Development Documentation |
| | Verification | Acceptance and Production Test Procedures and Results |
| | Configuration Control | Product Baseline Configuration |
| | Manufacturing | Assembly Drawings, Software Version Descriptions, Bill of Materials |
| | Logistics Product Data | FMECA Reports, RCM Reports, Support & Test Equipment Provisioning Lists, Interactive Electronic Technical Manuals, Maintainer Training Needs Analysis Reports, Maintainer Training Courses |
| | Material In Service Data | Spares Lists, Demand Data from Field Requisitions Item Prognostics & Diagnostics Information, Field Quality Deficiency Reports, Field Supply Deficiency Reports, Servicing and Inspection Instructions |
| Parts 1.2.2 & 1.2.3 | Requirements | Procurement Specification |
| | Design | Product Models, Engineering Drawings (External Interfaces) |
| | Verification | Production Test Results, Certificates of Conformance |
| | Configuration Control | Product Baseline Configuration |
| | Logistics Product Data | Support & Test Equipment Provisioning Lists, Interactive Electronic Technical Manuals, Maintainer Training Courses |
| | Material In Service Data | Spares Lists, Demand Data from Field Requisitions, Item Prognostics & Diagnostics Information |

**Activities Requiring Technical Data**

43. For a particular system or product, activities for which Defence, or its contractors, may require technical data include:

a. operating the product;

b. installing or configuring the product;

c. interfacing and integrating the product with other platforms or systems (including removal);

d. conducting operational level maintenance on the product;

e. conducting intermediate or deeper level maintenance on the product;

f. undertaking training in relation to the product;

g. rectifying defects;

h. conducting emergency repair of the product;

i. conducting verification and validation for system acceptance, ongoing maintenance and operational test and evaluation activities in respect of the product;

j. transporting the product or component spares and consumables;

k. placing the product in storage in a non-operational state;

l. decommissioning and disposing of the product or elements of the product;

m. modifying or upgrading a product;

n. manufacturing a new or existing product (typically by a third party).

44. The technical data requirements for a component in the hierarchy will be driven primarily by the operational and support concepts for the system and the expectations for the future evolution of the system.

45. Expected activities and their associated technical data requirements need to be determined for components at the appropriate level of the PBS hierarchy (see Figure 8). These definitions should be captured in Section 5.6 of the Operational Concept Document and also in the Function and Performance Specification for Support system requirements.

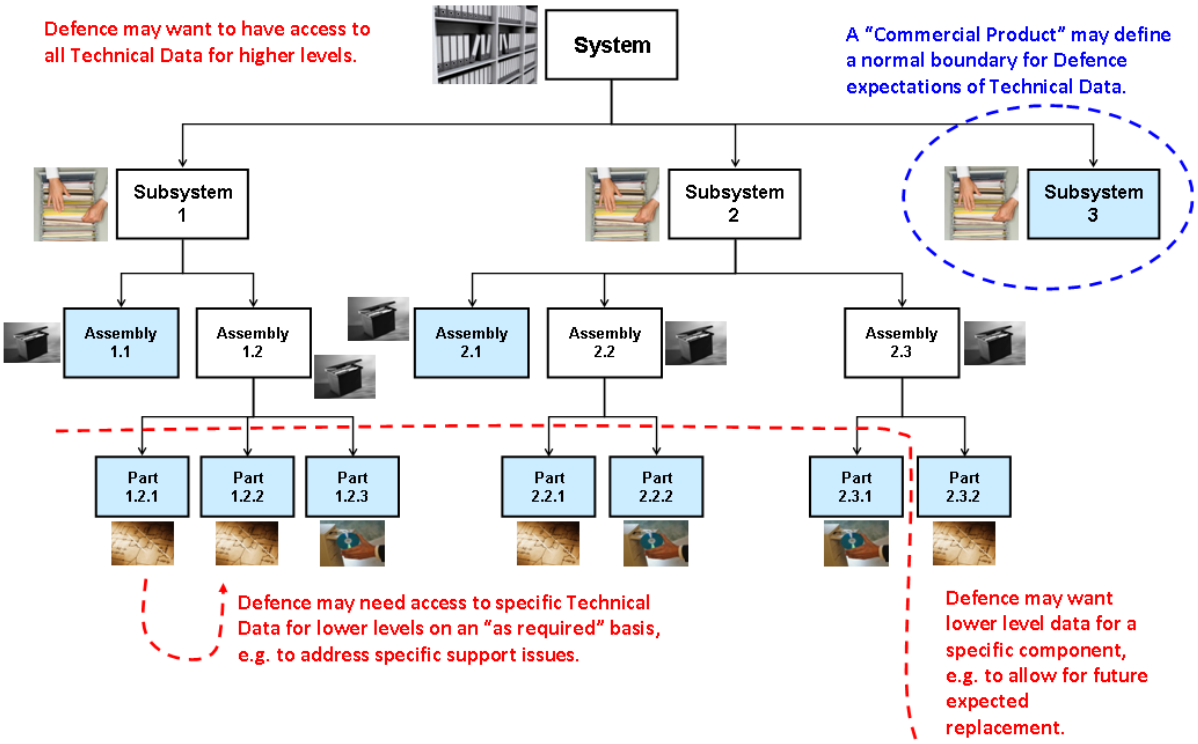


**Figure 8 – Technical Data Requirements depend on Acquisition Needs, Support Concepts and Business Needs**

### Technical Data Associated with Support

46. Technical data is a pivotal component of the support system, critical for the safe and effective operation of the overall capability and to ensure the support system optimises the mission system's availability. Figure 9 illustrates that each of the support system constituent capabilities includes technical data as a key contributor to resources. Typical examples of technical data associated with support are shown in Table 4.

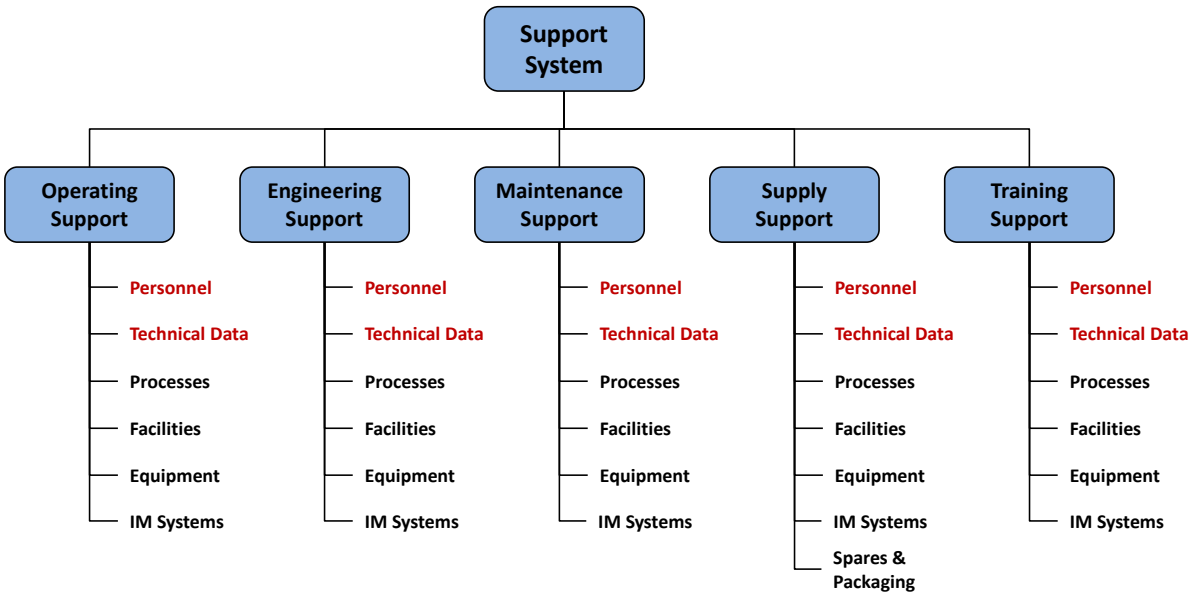


**Figure 9 – Support System Constituent Capabilities and Resources**

**Table 4 – Examples of Technical Data associated with**

**Support System Constituent Capabilities**

| Constituent Capability | Technical Data | |
|---|---|---|
| | Example | Expected Activities |
| Operating Support | Operator Manuals<br>Handbooks<br>Simulations<br>Standards | Operation |
| Engineering Support | Specifications<br>Engineering Drawings<br>Models<br>Plans<br>Databases<br>Design Data<br>Test Results<br>CM Records<br>Analyses | Installation & Configuration<br>Verification & Validation<br>Technical Integrity<br>Integration |
| | | Modification<br>Development<br>Manufacturing |
| Maintenance Support | Maintenance Manuals<br>Handbooks<br>Records<br>Reports<br>Calibration Reports | Installation & Configuration<br>Operational Maintenance<br>Disposal (not by Sale or Gift) |
| | | Non-Operational Maintenance<br>Emergency Repair |
| Supply Support | Databases<br>Reports<br>Drawings<br>Handbooks<br>Plans<br>Calibration Reports | Installation & Configuration<br>Operational Maintenance<br>Disposal (not by Sale or Gift) |
| | | Non-Operational Maintenance<br>Emergency Repair<br>Disposal by Sale or Gift |
| Training Support | Training Materials<br>Presentations<br>Handbooks<br>Models<br>Simulations | Training |

47. Once the system is in-service, one or more organisations will provide each support system constituent capability as a support service. The activities needed to address the support system constituent capabilities are normally provided through one or more support service contracts. Each service is provided for the identified system components (i.e. one or more elements of the product hierarchy in Figure 7), by an appropriate organisation, using the relevant technical data. These organisations may include the operational unit, CASG, original contractor, other support contractors or subcontractors and third parties, each one requiring access to relevant technical data.

48. Using a subset of the components identified in the PBS hierarchy shown in Figure 7, an example of the relationship and interaction that may exist between support services and organisations supporting the components of the example system is illustrated in Figure 10.

49. Figure 10 shows that each organisation can provide a varying scope of the different support services for each component in the system. Some issues that require resolution are:

a. identification of support service being provided by each organisation;

b. definition of scope of support being provided by an organisation;

c. interaction between organisations; and

d. required exchange of technical data to support these arrangements.

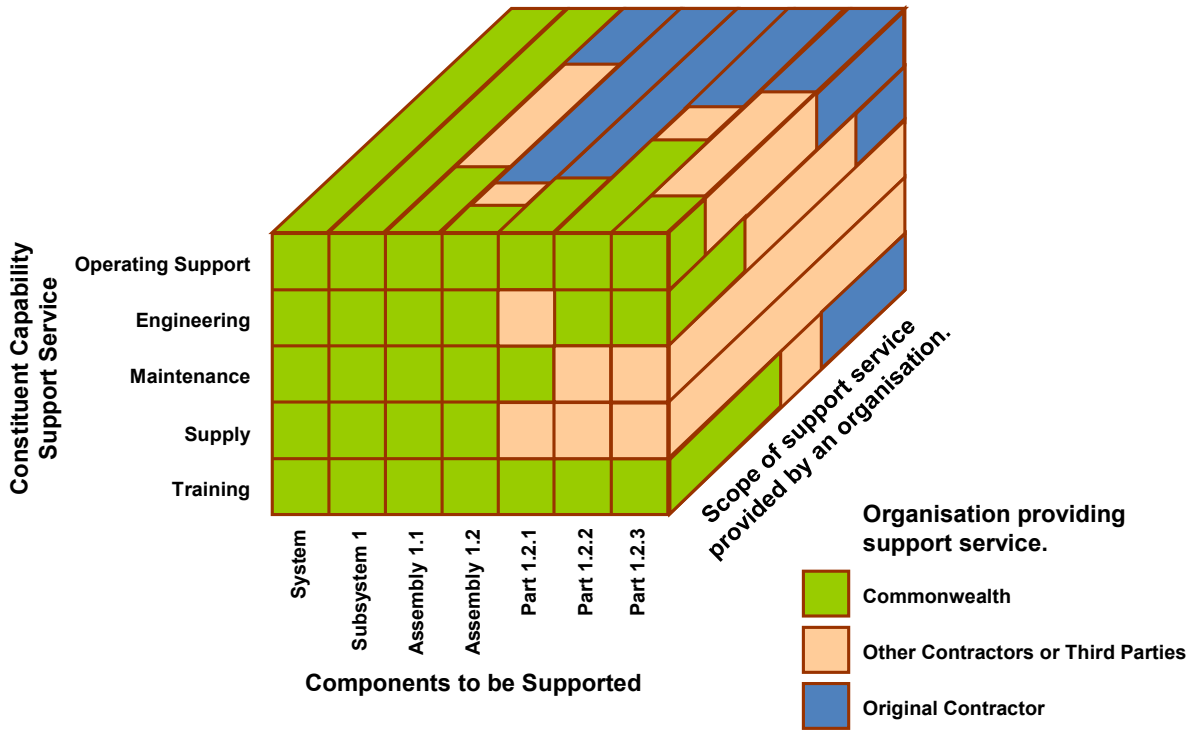


**Figure 10 – Example of Support Services and Organisations for System Components**

50. Technical data obtained under an acquisition contract will generally be provided to the support contractor(s) as Government Furnished Data (GFD) or Government Furnished Information (GFI), unless the support contractor was also the Original Equipment Manufacturer (OEM) (e.g. for off-the-shelf items, it is often 'the norm' for the OEM to provide the required support - in such a case, and where there is no other need for Defence to hold the technical data, the required technical data may primarily relate to product installation, configuration and operation).

51. Each support contractor will generally provide new technical data as part of the services under the Support Contract, which CASG may also need to redistribute for use by other parties. technical data may also come from other sources (e.g. interface data from other projects, technical data from Foreign Military Sales etc.). Figure 11 illustrates the exchange and flow of technical data between the various contractors or organisations.

52. Organisations identified in Figure 10 or Figure 11 need to use relevant technical data to provide the support service defined for the system components. The Commonwealth also has to establish the arrangements that acquire the necessary technical data and/or allow the expected exchange of this technical data between each of the organisations.

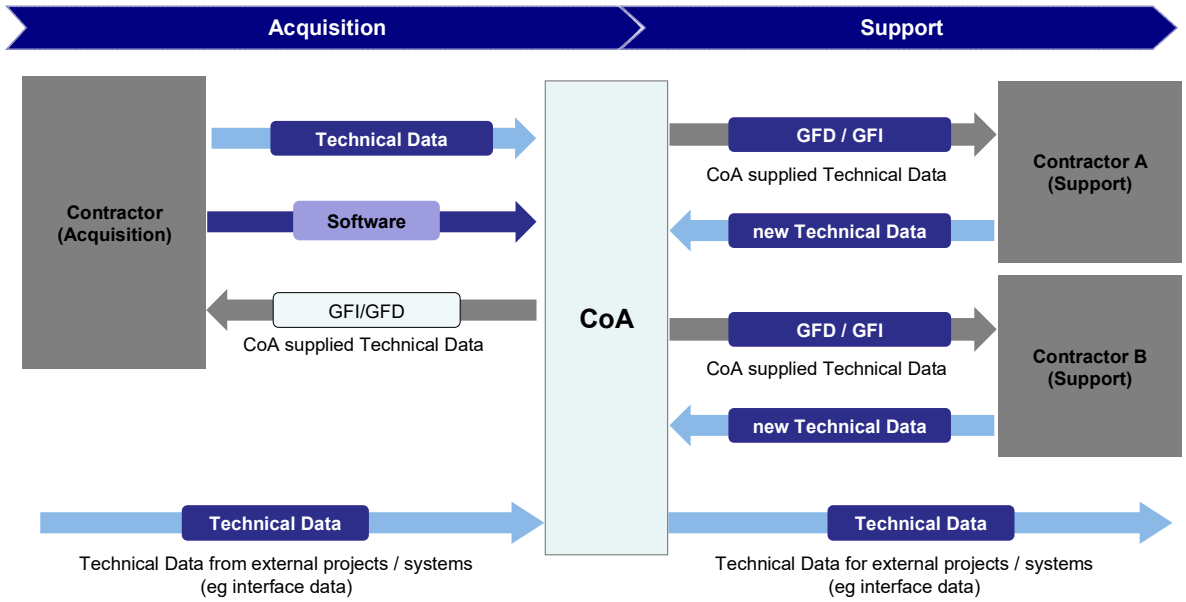


**Figure 11 – Exchange and Flow of Technical Data across a Product Lifecycle**

### Technical Data Formats

53. Technical data may exist in a wide range of formats, some of which may be specified in content and delivery standards. The preferred format for technical data is in electronic formats that that may also be interactive. Where electronic formats are not available, hard copy documents and publications can be used as an alternative. The content and format of technical data will be specified in the contract mostly through Data Item Descriptions (DIDs).

54. Notwithstanding the mode of delivery, the technical data's content format will often be subject to or defined by a published specification or standard. Many of these specifications and standards address the format of technical data, e.g. standards for data models, engineering drawings and technical publications.

55. CASG policy[6] encourages the acquisition of technical data in approved electronic formats employing integrated, open system standards. Where possible this should consider the need to include the source data format to allow editing of content (e.g. drawing tool files, as well as a pdf). Where Defence has a preferred or mandated standard for a type of technical data, these are identified in Annex A. Technical data produced internally by Defence also needs to conform to similar standards. Projects/SPOs should avoid committing Defence to unapproved software applications and/or unapproved file formats.

56. In determining the format to be adopted, factors associated with accessibility, cost, compatibility, suitability, degree of configuration control and any special requirements should be considered. Generally, the higher the degree of configuration control exercised over materiel, the greater the need for a highly automated and integrated digital data management system.

57. In some cases, technical data may only be available in hard copy, particularly for commercial off-the-shelf systems. However, Defence should make all reasonable efforts to gain access to or convert the data to an electronic format.

## Acquisition and Creation of Technical Data

### Rights to Technical Data

58. The IP for technical data delivered under a contract resides with the contractor. The

[6] Refer to CASG Policy (E&T) 12-2-003 - *Acquisition and Management of Technical Data*.

Commonwealth should negotiate the rights to technical data as part of the Conditions of Contract.

59. The Commonwealth's right to technical data is defined in the approved Technical Data List (forming part of the Master Technical Data Index) and the Approved Software List which lists all relevant technical data and software deliverables under the related acquisition contract.

60. The Technical Data and Software Rights (TDSR) schedule of the related contract details any exceptions to the rights of the Commonwealth under the contract. The TDSR schedule lists specific technical data or software where a restriction applies to the Commonwealth's rights under the Conditions of Contract.

61. It is critical to understand the contractual framework relating to technical data when considering technical data requirements as part of the TDRA.

62. Where technical data is acquired, Defence should:

a. define explicitly, through the contract Statement of Work (SOW), the tasks required by contractors that generate or provide the required technical data according to specified content, format and quality; and

b. use current, approved DIDs and a standardised Contract Data Requirements List (CDRL) approach in each contract to manage the delivery of the required technical data.

63. Where technical data is created by Defence or on Defence's behalf, it should:

a. contain all content required to understand, evaluate, operate and support the system throughout its life cycle while optimising total cost of ownership; and

b. be generated according to current approved electronic formats and quality consistent with the requirements of the overall contract.

64. The TDRA is a critical step in the development of the solicitation and contract documentation. The TDRA will assist drafters to determine the technical data requirements to be reflected in the contract documentation to ensure that Defence acquires adequate IP rights to use the technical data for the identified activities (including third-party release).

65. The contractor is required to produce a Technical Data Plan (TDP) that describes the contractor's strategy, plans, methodology, and processes for the identification, assembly, preparation, validation and delivery of technical data. The plan is required to describe a process consistent with meeting the requirements for technical data and the various issues related to data access, incorporating existing data, IP and escrow. The Integrated Support Plan (ISP) and support system Description also provide detail on the management of technical data.

66. As one of the outputs of the contractor's Logistics Support Analysis (LSA) program, the contractor is required to:

a. analyse the types and quantities of technical data needed for each of the SSCC and define the optimal range and quantity of technical data required to meet the support system Functional Baseline; and

b. identify this in the Technical Data List (TDL).

67. The CDRL will identify certain technical data to be delivered, including but not limited to:

a. the technical data format (e.g. 3D model, 2D engineering drawings etc.);

b. key requirements documents such as the System Specification (SS) and Requirements Traceability Matrix (RTM);

c. design descriptions such as the Support System Description (SSDESC);

d. a set of design documentation delivered in accordance with the contractor's Technical Documentation Tree (TDT);

e. publications delivered in accordance with a Publications Tree, including as appropriate Interactive Electronic Technical Manuals (IETMs) and Interactive Electronic Publications (IETPs);

f. codification data (refer electronic Supply Chain Manual and Materiel Logistics policies and

procedures);

g. Verification Cross Reference Matrix (VCRM);

h. Acceptance Plan, Procedures and Reports;

i. Technical Data Plan (TDP);

j. the Technical Data List (TDL); and

k. the (optional) Data Accession List (DAL).

68. The contractor is required to ensure that the TDL is a complete list of the optimised types and quantities of technical data, including the technical data that the Contractor will be providing to the Commonwealth, as well as the technical data that will be provided to, or used by, support contractors and subcontractors. The TDL includes references to other elements as necessary. It is expected that the TDL will be delivered and updated throughout the contract period, with an initial baseline provided at contract signature and subsequent updates delivered at major design milestones (e.g. Detailed Design Review, when the design is mature) and prior to final acceptance.

69. As part of the verification and validation of the support system, the contractor has to demonstrate the effectiveness of the technical data for each of the Support System Constituent Capabilities. Technical data is also considered at key System Reviews (e.g. preliminary design review, support system detailed design review, system acceptance audit).

## Verification, Validation and Acceptance of Technical Data

### Purpose of Verification and Review/Acceptance

70. Technical data verification and acceptance should:

a. ensure verification of content, format and quality of required technical data received from contractor(s) / supplier(s),

b. inspect technical data delivered contractually to ensure it is in accordance with the relevant agreements and contain appropriate distribution statements and/or export control statements;

c. validate the technical data as suitable for its intended purpose, and

d. take appropriate action to acknowledge the suitability or otherwise of the technical data.

### Data Quality Verification

71. Verification of technical data needs to confirm that it meets its defined requirements. Normally, contractor provided technical data needs to be verified against the specific requirements and intended purpose as defined in the contract CDRLs and associated DIDs.

72. Verification of technical data should determine whether it is relevant, accurate, current and correct for the associated product and expected activity. These attributes will be determined by the content of the technical data; therefore, it should be assessed or evaluated by personnel with the appropriate qualifications, competence and authority.

73. Defence needs to have confidence that technical data that is acquired, created or received is adequate, suitable for its intended purpose, relevant to Defence materiel's configuration, role and operating environment, and has been generated and authorised by an appropriate competent organisation before being released for use.

74. Confidence in the accuracy, relevance and completeness of supporting technical data contributes to confidence in the product with which it is associated.

75. In addition to verifying that technical data is supplied with the required content, it should also be delivered in the appropriate format. Technical data should be delivered in approved electronic formats unless there is a specific business case need for an alternative.

### Data Identification Inspection

76. Technical data deliverables should be inspected to ensure each technical data item contains identification to accurately indicate the following, as a minimum:

a. item identification,

b. security classification,

c. FMS or International Traffic in Arms Regulations (ITAR) classification,

d. rights relating to the technical data, including Intellectual Property ownership and authorised use, and

e. any other access restrictions.

77. Electronic data files should have the markings embedded in the digital data itself and on any media or media packaging on which the files are stored.

**Metadata Standard**

78. The National Archives of Australia mandates the method of using metadata (data about data) properties via the AGLS Metadata Standard to describe document entities. The AGLS Metadata Standard details eleven properties of which three are mandatory properties, three are conditional properties and five are recommended properties.

79. **Mandatory Properties.** The mandatory properties are:

a. creator (author);

b. title; and

c. date (or a related property).

80. **Conditional Properties.** The conditional properties are:

a. availability;

b. identifier; and

c. publisher.

81. **Recommended Properties.** The recommended properties are:

a. description;

b. function;

c. language;

d. subject; and

e. type.

**Validation of Technical Data**

82. Validation of technical data is confirmation that the information content is suitable for its intended purpose. For example, validation activities may result in:

a. confirmation that a product can be operated using the delivered technical data;

b. confirmation that a software configuration item can be generated from the associated technical data (i.e. source code and build instructions); or

c. confirmation that a maintenance task can be completed using the technical data provided.

83. Validation of technical data may also form part of broader supportability test and evaluation activities.

**Technical Information Review**

84. Large quantities of technical data related to materiel systems acquired through contract may be received. The technical data will consist of information which may vary in significance from not applicable to Defence's configuration, to critical (such as that directly affecting safety).

85. Technical data should be managed to ensure that data received is sorted quickly and prioritised so that the necessary action may be taken in a timely manner. A review process is required to collect and register technical data as well as to decide on whether it meets contractual requirements.

86. Technical data deliverables should be reviewed against the contractual requirements to verify that the requested items have been supplied. Where a DID has been specified for a technical data deliverable then the supplied item's conformance to that DID should be verified. Technical data requires differing levels of review and acceptance depending on its significance and any requirements in the contract.

## Storage, Maintenance and Control of Technical Data

87. Technical data storage, maintenance and control should:

a. allocate and manage the resources (e.g. personnel, funds) for the maintenance and upkeep of a product's data / configuration management system over its Life-of-Type,

b. use existing Defence integrated infrastructure (unless storage, maintenance and control of technical data is an OEM responsibility under the contract),

c. ensure all changes to technical data are made in a timely manner and documented accordingly in the integrated data environment infrastructure, and

d. implement a Configuration Management (CM) process and system for the control of technical data.

### Storage Systems

88. The Information and Communications Technology (ICT) environment that will be used to store and manage the data is a key consideration in the approach to managing technical data and needs to be aligned to the execution strategy and support concepts. The storage environment could be either Defence's environment or the contractor's.

89. Technical data should be stored and identified such that users can readily search for, locate and access the data when needed. To assure data is well identified and retrievable, appropriate metadata should be used.

### Access Controls and Maintenance

90. Accessibility of data to users with a need for the data throughout the product life cycle is another key consideration. This includes methods to be used to inform the organisations that will be involved in the various life cycle support activities as to what product data exists, where the authoritative information artefacts are stored and maintained and who is entitled to access the technical data.

91. All technical data should be disseminated to appropriate individuals or organisations with the appropriate distribution statement, export control warning notice (where applicable), disposal notice (where applicable), or any other relevant notices, whether produced in hard copy or digital format.

92. Budgeting for maintenance and upkeep of the product data throughout the life cycle is also an important consideration. Such maintenance activities include:

a. incorporation of configuration changes (including changes due to obsolete parts or materials); and/or

b. technology or format refresh.

93. Since the Commonwealth needs its technical data for several decades to match a system Life-of-Type, it is important that technical data be kept in a format and data system that is readily usable. Decisions in these areas are driven by mission requirements; anticipated product life cycle, acquisition and logistics support strategies, sources of supply, and cost. Issues to be considered and addressed with long term retention include:

a. **Data authoring applications.** To ensure technical data is readable for later use or manipulation, Defence may need to also store and retain data authoring or viewing application software to view, revise and print images or refresh data. Over time, data may need to be periodically migrated to current software applications and hardware formats for continued accuracy and availability.

b. **Storage media.** Storage media should not be an issue except where information is not stored in the Defence environment. When data is not stored on the Defence environment, procedures to protect data on any storage media from loss or inadvertent destruction should

be established and applied.

c. **Applications and Data systems.** In some cases, hardware systems may also need to be kept past the normal active life cycle in order to access the data (e.g. retention of microfiche viewers or tape drives that were not technologically current but provided the only method to read or access certain data due to the original storage media).

**Configuration Management**

94. Maintaining integrity of the master technical data item is essential. This can be achieved by using a system of access control so that only authorised personnel can obtain access to the relevant level of technical data which includes embedding notices by way of metadata or other means that identifies the custodian of the master copy.

95. Changes to technical data under CM should be authorised through an approved change control process. The application of CM principles to the acquisition and management of technical data enhances the technical integrity of the data throughout the product's life cycle.

96. Changes to the data should be coordinated with the data sponsor and be identified as changed from the original data.

97. Configuration Management should be applied to a significant portion of, but not necessarily all, technical data. For example, non-technical product data and maintenance management system data may not be under formal change control, however should still be managed as Commonwealth records.

98. Technical data under configuration control should have:

a. unique identifiers for data and documents,

b. effective file and data base management,

c. maintenance of essential file, version and revision relationships,

d. controlling status of and access to digital data, and

e. a defined relationship to one or more specific product definition(s) and/or specific product instance(s).

**Unique Identification**

99. An identification scheme should be at a level at which technical data will actually be under control (e.g. computer file database elements, illustrations and electronic media). Documents should be assigned unique identifiers so that they can be:

a. correctly associated with the item it supports such that change in the configuration item will change the supporting documentation;

b. referred to precisely, and

c. retrieved when necessary.

100. With emphasis on the acquisition of commercial products and the use of industry methods, it is inappropriate for Defence to specify one format for document identifiers. Generally document identifiers include all or most of the following parameters:

a. date;

b. assigned numeric or alpha numeric identifier unique to the document;

c. version indicator;

d. revision indicator;

e. type of document;

f. title or subject; and

g. sponsor.

**File and Database Management**

101. Digital data files are to be identified to differentiate between similar files and to maintain traceability to specific equipment configurations and document representations. As file naming conventions vary widely among operating systems and application programs, it is necessary to store information about the files (metadata) providing correct relationships and associations for the supporting document management system.

102. Each product should have its own record of the indexes and metadata of the associated technical data subject to the CM process. These records describe the elements of the technical data package and serve a similar function to cataloguing information in libraries. They should allow for efficient electronic searches; provide filtering/reports such as the set of technical data defining the approved configuration of a product; as well as track proposed and approved changes and deviations. It is usual to create a master document index to assist in document version control and referencing.

**Maintenance of Essential File and Version Relationships**

103. To facilitate the proper relationships, the following digital data identification rules should be applied:

a. a unique identifier should be assigned to each file;

b. a unique identifier should be assigned to each document entity;

c. a version identifier should be assigned to each file;

d. a database of the following relationships should be maintained:

   (1) document identifier and its revision level;

   (2) associated document representations, and

   (3) file identifiers and versions.

e. as necessary, multiple versions of files to recreate prior document revisions and provide traceable history of each document should be maintained.

## Use, Distribution and Exchange of Technical Data

104. Before disseminating technical data (particularly to external organisations), Defence's rights to use and distribute technical data need to be understood.

105. Technical data acquired during acquisition will reside on the Defence IT infrastructure, however, depending on the contract, may reside on an external database managed by an industry partner.

106. Regardless of the storage location, the technical data needs to be under configuration control to provide assurance of its currency, accuracy and relevance to the system it is associated with.

**Contractor Data Management System**

107. Where under the conditions of a contract, the contractor is responsible for storage and management of technical data, the project/contract manager should encourage and work with the contractor to implement a Data Management System (if the contractor does not already have a suitable one in-house).

108. The Data Management System (DMS) should:

a. provide a controlled repository for acquired technical data;

b. cater for unclassified data (and classified data if developed under the contract);

c. provide authorised Defence users on-line access to the technical data identified in the acquisition contract.

d. provide access controls to limit access to technical data that may be sensitive between parties (e.g., subcontractor access to prime contractor proprietary data);

e. provide controls to prevent authorised Defence users from replacing or overwriting the configuration controlled versions of technical data inadvertently;

f. where reasonably practicable, allow the technical data to be downloaded by an authorised Defence user for further manipulation (including printing) in the native document format;

g. provide access to both current and historical technical data, including earlier versions of documents and any pertinent comments provided on each of the versions;

h. provide an index of technical data (updated at least weekly), with the index to provide the CDRL Line Number or other reference number (as applicable), title, issue, file name (as applicable), status (e.g., working, draft submission, final submission, Approved, and Accepted), date of most recent change, and location on the DMS;

i. provide the ability for the authorised Defence users to search the database;

j. provide the ability to capture, store, provide access to, and maintain an audit trail of comments provided by the authorised Defence users on technical data; and

k. provide the Defence Project or Sponsor with the ability to electronically:

(1) acknowledge delivery of data, and

(2) provide comment/feedback and/or reject a data delivery.

109. System security aspects of the DMS should be detailed, including:

a. controlled system access;

b. protection against unauthorised access;

c. system administration functions to control data access;

d. file transfer protocols used;

e. meet Defence ICT Security Accreditation requirements is classified data is involved;

f. security classification of material that will be able to be released on the DMS;

g. procedures for the handling, management, transfer, release, etc. of classified material (if required); and

h. procedures for periodic back-up of electronic data, including a list of the data files that should be backed up and how the backup is performed.

110. Administration functions that Defence authorised users may be required to perform should be detailed, including a description of routine administration that needs to be carried out and the actions required to perform administration.

111. Procedures for formal and informal communications should be detailed which may include the following:

a. notification of actions between authorised users;

b. access and navigation of the DMS;

c. downloading, uploading and viewing DMS technical data; and

d. how comments are to be provided for document type (e.g. native file formats etc.).

112. The promotion of data in the DMS from one status to the next (e.g. working, draft submission, final submission, approved and accepted) should be detailed and a point-of-contact provided for assisting Defence authorised users with problem resolution and to answer questions concerning the DMS.

113. DMS users may need training in the use of the DMS, in which case a detailed training plan should be prepared.

## Archival and Disposal of Technical Data

### Overview

114. Disposal of technical data during the Capability Life Cycle concerns the removal of systems or products from the Defence inventory and the phasing out of mission and support system equipment and components from the capability system during the In-Service phase.

115. Whilst inventory may cease to be used and business process tasks completed, the associated technical data will need to be accessible well past the actual point of disposal to support later investigations (e.g. safety incidents) and to meet the retention requirements of the Archives Act 1983.

116. Technical data in any form, created, captured, managed or stored by any Defence personnel or contracted service provider, remains subject to the requirements of the Defence Records Management Policy Manual (RECMAN) and associated Records Authorities for the archive or disposal of Defence records, which states any new electronic records become the primary records and are subject to sentencing and disposal under relevant records authorities, either Australian Government Disposal Authorities (such as Administrative Function Disposal Authority (ADFA) Express) or Defence Records Authorities.

117. Configuration and technical data is also subject to the following Acts in varying degrees:

a. Electronic Transactions Act 1999;

b. Evidence Act 1995;

c. Freedom of Information Act 1982;

d. Privacy Act 1988; and

e. Public Governance, Performance and Accountability (PGPA) Act 2013.

118. The disposal of technical data is a continuous process that extends beyond the life-cycle of a capability system or specific equipment.

119. Technical data will be withdrawn from service at the end of materiel service life. Disposal of technical data is conducted in accordance with Archives Act 1983 and RECMAN. There may be IP rights issues that need to be considered as part of disposal, including licensing and export approval – further guidance can be found in the Defence Procurement Policy Manual (DPPM).

### Legal Archival, Destruction or Disposal

120. Technical data may be identified for disposal where ownership is to be transferred to another operator (including museums). In this case, all requisite configuration documentation and Configuration Status Accounting (CSA) records (including publications and manuals) needs to be identified and collated. IP Rights, ITAR and/or Export Controls related to technical data will need to be resolved before any transfer of data occurs.

121. Technical data records are subject to a systematic program of declassification and transfer of records to the Australian Archives. A document change authority is responsible for the archiving of documents under their control and other obligations with regard to the treatment, preservation and disposal of records.

## Annexes:

A. Technical Data Standards and Formats

# TECHNICAL DATA STANDARDS AND FORMATS

## S1000D Specification

1. It is expected that Defence will work towards a common framework for the application of technical data management to support materiel systems. Where practicable, projects are to adopt and apply S1000D™, *International Specification for Technical Publications utilising a Common Source Database*, business practice and advocate the use of S1000D™ compliant systems for the production of Interactive Electronic Technical Manuals (IETMs) and/or Interactive Electronic Technical Publications (IETPs).

2. The S1000D *International specification for technical publications using a common source database* is a specification for the production of technical publications, using XML for preparing, managing, and using equipment operating and maintenance information.

3. S1000D is part of the S-Series of ILS Specifications.

## File Type Specifications and Standards

4. File types are normally the subject of International Standards Organisation (ISO) standards or specifications, which govern their generic qualities.

5. Projects/SPOs cannot commit Defence to unapproved software applications or file formats. Should this constraint prove to be unavoidable, Projects/SPOs need to commence dialogue with CIOG as soon as the requirement becomes realised.

6. The Project/SPO will be responsible for the initial licencing costs of any software as well as initial sustainment costs, until such time as CIOG commits to sustainment of the application.

## Common File Formats

7. Common file formats that may be contained in technical data are listed in Table A-1.

**Table A-1 – Common File Formats**

| Functional Requirement | File Type | File Extension |
|---|---|---|
| Unstructured Text | Microsoft Word files | .doc<br>.docx |
| General Graphics | TIFF,GIF, JPEG, PNG, BMP, WMF, EMF file formats | .tiff<br>.gif<br>.jpeg<br>.png<br>.bmp<br>.wmf<br>.emf |
| Output Files | General Output File Formats | .pdf<br>.xls<br>.xlsx<br>.rtf |

## Structured Data Standards

8. Standards for structured data are contained in Table A-2.

**Table A-2 – Structured Data Standards**

| Functional Requirement | File Type | File Acronym | Standard/ Specification |
|---|---|---|---|
| Structured Data | Non-Proprietary | SGML | All suppliers of SGML data are to create, validate and exchange instances of data to the Commonwealth against an approved SGML Document Type Definitions (DTD). |
| Structured Data | Non-Proprietary | XML | All suppliers of XML data are to create, validate and exchange instances of data to the Commonwealth against an approved XML DTDs or Schema. |
| Graphical Environments | Computer Graphics Metafile | CGM | All suppliers of CGM data are to create, validate and exchange instances of data to the Commonwealth using software applications that comply with ISO/IEC 8632 Information technology – Computer Graphics - Metafile for the storage and transfer of picture description information. |
| Output Files | Point-in-Time deliverables | PITD | All suppliers are to exchange valid data to the Commonwealth via the exchange medium as contracted/agreed upon by the procurement authority. |
| Data Exchange | Interactive Electronic Technical Publication | IETP | All suppliers of IETP are to exchange deliverables to the Commonwealth as either an electronic exchange via DDN (Data Delivery Note), CD/DVD media or as an ISO image of the IETP into an approved DPN folder. |
| Logistics Data | LSA/LSAR | N/A | All suppliers are to create, validate and exchange LSA/LSAR data in accordance with the contracted agreement. This may be in DEF(AUST) 5692 compliant formats or via Commonwealth access to a contractor LSA repository. |