Ministry of Defence

Chapter 02 - Configuration management and the CIDA - Leaflet 4800

Previous version of JSP 604 can be found on the Defence Wiki Platform.

JSP 604 is changing, for more information see **Standards as a Service**.

Print or PDF this page

Page Status:

Live

Page identity: Page identity type not identified Page identity not identified
Page type: Page identity type not identified Page identity not identified

Last updated

7/04/2022 by Fosterg443

Rule ownership

1* area responsible for Chapter 02 - Configuration management and the CIDA - Leaflet 4800 is **Ops Co-ordinating Installation Design Authority**.

Contents

1 Last updated
2 Rule ownership
3 Introduction
4 Rationale
5 Benefits and risks
6 Technical controls
6.1 CIDA Application of Configuration Management
6.2 Configuration Management and Planning
6.3 Configuration Identification
6.4 Change Control
6.5 Configuration Status Accounting
6.6 Configuration Audit
7 Related Pages
7.1 Parent Page
7.2 Child Pages
7.3 Sibling Pages
7.4 Signature block
8 Associated documents with Chapter 02 - Configuration management and the CIDA - Leaflet 4800
9 References

Introduction

MOD CIO, directs the use of the following MOD policy documents, JSP 604, Defence Manual for ICT, JSP 440, Defence Manual of Security and Resilience and JSP 945, MOD Policy for Configuration Management [1] and JSP 375, Management of Health and Safety in Defence to ensure MOD ICT installations are compliant with legal requirements, the UK government SPF and meet the mandated requirements for Configuration Management CM, Change Control CC, installation design control and accreditation processes, thus directly delivering the Cabinet Office governance requirement for the provision of an Accreditation process.

1. CM and Planning
2. Configuration identification.
3. Change Control.
4. Configuration status accounting.
5. Configuration audit.

A non-compliant installation will not be accredited for processing and storing MOD information.

Rationale

To ensure compliance with these policies there is a requirement to carry out the following:

1. Certification of new and extant ICT installations is required before ICT systems can be accredited and re-accredited.

2. SCIDA's shall be established and maintained for all ICT facilities. SCIDA Framework Document establishes the delivery requirement for SCIDA's to provide the necessary CM of the physical and environmental aspects of Defence ICT Installations.

Benefits and risks

MOD Installation Standards Policy ensures control over the installation design, site configuration and environment such that the following is ensured, whilst assuring that within a defined site, all security and safety requirements relating to each ICT installation are met and maintained:

1. **Confidentiality** - By ensuring that where appropriate, installations meet the requirements for RADSEC and are maintained under configuration control.
2. **Integrity** - By ensuring that installations will not suffer from or be the cause of electrical interference to other co-located installations (EMC).
3. **Availability** - Optimising operational availability by ensuring that installations are implemented in accordance with relevant standards and good engineering practice, and maintained under effective CM. The aim is to reduce system failure due to poor installation standards and facilitate maintainability, fault rectification and future engineering change.
4. **Resilience** - By ensuring that where appropriate, installations are provided with diversity of location, power, connectivity and cooling to facilitate continuity of service during unforeseen disruptive malfunction.
5. **Flexibility** - By ensuring that correct installation documentation and standards are maintained, that installations and recoveries are conducted in a manner that facilitates future change and that a complete Facility information set is available to future Change Designers.
6. **Economy** - By ensuring that spare capacity is correctly utilised, that additional systems are installed in a manner that makes best use of the site's infrastructure and available space and to co-ordinate change to avoid conflict or promote efficiency such as through combined cross-site duct projects or common works service provision.

Technical controls

CIDA Application of Configuration Management

CIDA Governance is mandated with the responsibility for optimising the maintenance of operational capability, flight safety and electrical security by co-ordinating changes into MOD ICT facilities and by regulating installation standards. CIDA direction applies to all sites, buildings, rooms and mobile/transportable equipment facilities but not to aircraft, ships or submarines.

Day to day activities on a site is normally delegated to the SCIDA except for deployed operations which are usually managed centrally. The application of CM to an MOD ICT system is dependent upon the CIDA Service Level assigned to that system. [2] In accordance with the mandates of JSP 440, the minimum requirement is the granting of Installation Approval by SCIDA.

CIDA has no remit to include system or application software in its CM activities. The CIDA CM 'product', therefore, is the physical, in terms of layout, and electrical, in terms of connectivity, facets of all MOD ICT facilities. CIDA discharges its CM responsibilities for MOD ICT facilities by ensuring that the following procedures are adhered to.

Configuration Management and Planning

The ECR process ensures that all activities and processes relating to the installation of MOD ICT are carried out in a controlled and traceable environment.

Configuration Identification

A library of 'As Fitted' drawings, including Site Plans, Location Maps and system documentation is generated from site survey and/or assembled from extant information to form the CM baseline for all MOD ICT. Drawing content and standards are fully documented at Chapter 12.

Change Control

All changes to a CIDA controlled facility must go through a CC procedure to obtain SCIDA endorsement before the change is implemented. Full details are documented at Chapter 4.

Configuration Status Accounting

To facilitate visibility, traceability and the efficient management of evolving configuration, SCIDA maintain records of pertinent data relative to all 'change' of MOD ICT systems that fall within their AOR, and may use a variety of resources, in either paper or digital format, dependent on the volume and content of data that is recorded.

Configuration Audit

To ensure continuing conformance to CIDA requirements, sites must be regularly inspected by the SCIDA. This will be carried out to a 'SCIDA Inspection Plan', with associated Inspection Reports produced. CIDA conducts an assurance regime for all SCIDA/sites, the timing of which being determined by CIDA in consultation with the SCIDA. In combination, the CIDA and SCIDA process constitutes the Configuration Audit.

The frequency of Configuration Audits of MOD ICT systems depends on the 'CIDA Service Level' for the system and is carried out in accordance with the SCIDA Framework Document.

The configuration audit examines the 'As Fitted' product to its configuration documentation to ensure compliance. The audit confirms that the product conforms to the physical and functional requirements through assessment of:

1. The comprehensiveness of the CIDA baseline package.
2. Installation standards and maintainability across the whole site meet CIDA requirements.
3. Common Equipment layout and engineering requirements are being maintained.
4. Information Security requirements of JSP 440 continue to be maintained.
5. The progress of observations and actions raised in previous audit reports.
6. The local procedures intended to prevent unauthorised change.

7. Unauthorised changes that have occurred and where relevant, the organisation responsible.

On completion of a configuration audit, a report of the results, including recommended actions to correct non-compliance, will be issued to all ‘relevant parties’.

Related Pages

Parent Page

- Draft:CIDA installation regulations (Leaflet 4800)

Child Pages

This page has no child pages

Sibling Pages

- Chapter 01 - Responsibilities and definitions of CIDA and associated roles - Leaflet 4800
- Chapter 01 - Responsibilities and definitions of CIDA and associated roles - Leaflet 4800
- Chapter 02 - Configuration management and the CIDA - Leaflet 4800
- Chapter 02 - Configuration management and the CIDA - Leaflet 4800
- Chapter 04 - The CIDA engineering change process - Leaflet 4800
- Chapter 06 - The ICT Physical Environment - Leaflet 4800
- Chapter 07 - The ICT Electrical Environment - Leaflet 4800
- Chapter 08 - Cabling systems - Leaflet 4800
- Chapter 09 - Cable Identification - Leaflet 4800
- Chapter 10 - Cable pathway and cable management systems - Leaflet 4800

... further results

Signature block

Author to sign off: Richardsond505
Author signed by: Not signed (talk)
Author signed date: Not signed
Owner to sign off: Kingsmanp996
Owner signed by: Not signed (talk)
Owner signed date: Not signed
Next review date: No review date identified

Associated documents with Chapter 02 - Configuration management and the CIDA - Leaflet 4800

- SCIDA Framework Document (https://modgovuk.sharepoint.com/:w:/r/teams/20695/_layouts/15/Doc.aspx?sourcedoc=%7B57768159-00D2-4175-85F7-B1F3A3E6CEAB%7D&file=20211102-SCIDA_Framework_Document_v1.4%20FINAL.docx&action=default&mobileredirect=true)

References

1. Part 1, Para 1.2
2. SCIDA Framework Document, Table 1

Retrieved from ‘https://jsp604.r.mil.uk/index.php?title=Chapter_02_-_Configuration_management_and_the_CIDA_-_Leaflet_4800&oldid=40835’

This page was last modified on 7 April 2022, at 19:40.

0 watching users