Ministry of Defence

# Chapter 01 - Responsibilities and definitions of CIDA and associated roles - 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 01 - Responsibilities and definitions of CIDA and associated roles - Leaflet 4800 is **1* area not identified**.

## Contents



# Introduction

CIDA Governance is a team within the Operations branch of Defence Digital, that is responsible for the MOD Installation Standards applied to the physical and environmental aspects of MOD ICT. MOD CIO, directs the use of the following MOD policy documents, JSP 604, Defence Manual for ICT and JSP 440, Defence Manual of Security and Resilience and JSP 375, Management of Health and Safety in Defence to ensure MOD ICT installations are compliant with legal requirements and the UK government SPF.

# 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. [1]
2. SCIDA's shall be established and maintained for all ICT facilities. The Defence CIDA Governance 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 direction 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, 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.

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

# Technical controls

## Risk

In accordance with UK government SPF, CIDA Governance uses a risk management approach. Risk is assessed to identify the potential impact to MOD business through the loss or reduction of Confidentiality, Integrity, Availability or Resilience from the viewpoint of the physical and environmental aspects of ICT installations.

Identified risk is managed through normal CIDA process [2] or one of the following routes.

1. The problem is rectified to remove the risk.
2. Risk to MOD data is directed to the appropriate system Accreditor [3] for resolution or escalation, as appropriate; or for formal acceptance by the appropriate IRO.
3. Risk to personnel or facilities are directed through the facility management to the Head of Establishment (HOE) for resolution or acceptance.

## Site Co-ordinating Installation Design Authority

To deliver MOD Installation Standards Policy, CIDA support the establishment of site based teams to deliver much of the day to day work. These teams are known as SCIDA. All MOD facilities shall have a SCIDA, established in accordance with the Defence CIDA Governance SCIDA Framework Document. [4] All ICT change at site level must be in accordance with the requirements of JSP 604: Leaflet 4800 and agreed with the SCIDA. For Above Secret (AS) MOD ICT, local SCIDA's shall engage with Defence Sites SCIDA who have additional governance responsibilities of AS systems.

The SCIDA function is to ensure that the full benefits of Physical and Environmental CM for MOD ICT are delivered across sites in accordance with the SCIDA Framework Document or Contract. TLBs are responsible for the provision of SCIDA at their sites with this responsibility normally delegated to the Head of Establishment or site owner. From the viewpoint of co-ordination of change and the regulation of installation standards, a SCIDA should preferably be independent from the organisations who deliver change.

Where a site or facility owner provides a SCIDA to conduct SCIDA provision below that required by MOD and detailed in the Defence CIDA Governance SCIDA Framework Document [5] then an assessment of the risk to the Confidentiality, Integrity and Availability of the ICT systems and data must be undertaken and formally recorded.

The effectiveness of a SCIDA may be evaluated, by Defence CIDA personnel, through formal audit of both the SCIDA and the SCIDA process

## Technical Supervisory Co-ordinating Installation Design Authority

In certain circumstances, a Technical Supervisory Co-ordinating Installation Design Authority (TSCIDA) may supervise the SCIDA(s) in the day to day running of the SCIDA role.

To avoid lengthening chains of responsibility, the appointment of a TSCIDA should be limited to essential situations. A TSCIDA should not be appointed over a SCIDA where an individual is primarily filling the 'Contract Manager' role as opposed to a supervisor role.

# Related Pages

## Parent Page

- Draft:CIDA installation regulations (Leaflet 4800)

## 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 01 - Responsibilities and definitions of CIDA and associated roles - Leaflet 4800

- UK Government Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework)
- Defence ICT Accreditation Guide (https://modgovuk.sharepoint.com/sites/defnet/JFC/Documents/Defence_ICT_Accreditation_Guide.pdf)
- SCIDA Framework Document (https://modgovuk.sharepoint.com/:w:/r/teams/20695/_layouts/15/Doc.aspx?sourcedoc=%7B5776815-00D2-4175-85F7-B1F3A3E6CEAB%7D&file=20211102-SCIDA_Framework_Document_v1.4%20FINAL.docx&action=default&mobileredirect=true)

## References

1. Defence ICT Accreditation Guide Page 7 Para 3
2. CIDA Risk Process (https://modgovuk.sharepoint.com/teams/20695/Technical%20DirectionGuidanceAdvice/Forms/AllItems.aspx?FilterField1=Type_x0020_of_x0020_document&FilterValue1=Guidance%20note&FilterType1=Choice&FilterDisplay1=Guidance%20note&id=%2Fteams%2F20695%2FTechnical%20DirectionGuidanceAdvice%2FCGN_2020-02_Risk%20Management%20and%20the%20ECR%20Process.pdf&parent=%2Fteams%2F20695%2FTechnical%20DirectionGuidanceAdvice)
3. Full accreditation is approved by the Cyber Defence and Risk (CyDR) (https://modgovuk.sharepoint.com/sites/defnet/JFC/Pages/DAIS.aspx) directorate
4. SCIDA Framework Document Page 6 Para 3 and 4
5. SCIDA Framework Document Page 8 Table 1