Strategic Command

Defence Digital

CO-ORDINATING INSTALLATION DESIGN AUTHORITY GOVERNANCE

SCIDA FRAMEWORK

Issue 1.4 dated 2 Nov 21

PLEASE DO NOT ALTER THIS COPY – DOWNLOAD

INSERT SITE NAME

Defence Digital Ops HQ - Assuring missions, enabling Multi-Domain Integration and delivering Information Advantage.

CIDA Governance - Delivering assurance of the physical and environmental aspects of MOD ICT through expert direction, support and oversight - A critical enabler of the SCIDA Enterprise.

SCIDA FRAMEWORK

Contents

Glossary of terms

Term	Explanation
Baseline Activity	Confirmation and validation of the current fixed ICT infrastructure laydown within the SCIDA assigned areas. Baseline activity includes elements such as surveys and updating existing CMDB drawings and documentation. This activity should be completed no later than 24 months after SCIDA appointment, beyond this period future changes to these records are to be captured through the formal change process.
Change	An alteration, addition or removal affecting ICT hardware or supporting infrastructure regarding physical location, environment, or Radio Site Restriction Zones. A change in this context does not include software modification of individual equipment. Such changes may, however, affect the wider Configuration Management duties.
Change Control	Management of a physical change to the fixed ICT infrastructure through a formalised process.
CIDA Governance Audit	An independent audit conducted by CIDA Governance to review the processes, systems and structures employed by the appointed SCIDA by evaluating the current SCIDA support in line with the assigned Service Level and against this Framework.
CIDA Governance	Coordinating Installation Design Authority Governance. Responsible for the optimisation of the maintenance of operational capability and engineering best practice of all ICT, Communications Electronics (CE) engineering and other Electronic systems and their associated infrastructures and environment during their lifespan.
Configuration Management	JSP 945 is the MOD policy for Configuration Management. CIDA Governance adapt this policy into their change and configuration processes. This ensures the appropriate Configuration Control (CC) and Configuration Management (CM) of relevant systems, the co-ordination of engineering change and the regulation of installation standards.
Configuration Management Database	Electronic ICT configuration records held in a shared access repository.
Defence Enterprise SCIDA	DE SCIDA apply the polices directed by CIDA Governance and appoint SCIDA to manage CC and CM of ICT infrastructure across an assigned area of the MOD Estate. DE SCIDA also maintain configuration management drawings and documentation via an organic Drawing Office.
FM Team	Contracted by DIO, The Facilities Management Team is the Principle Contractor responsible for the physical maintenance of MOD site infrastructure. Site dependant, The FM Team may adopt a different title, however the function is the same.
HoE	The Head of Establishment is appointed to manage MOD infrastructure resource within a specific boundary. In some sites this responsibility falls to a military role in a senior appointment. Smaller sites may have an empowered representative with a different role title – Infrastructure Manager, Building Custodian etc.
ICT	Information Communication Technologies used in place of Communication Information Systems (CIS).

SCIDA Audit	A periodic on-site validation of ICT installations carried out by an appointed SCIDA to ensure continuing conformance to CIDA Governance, relevant standards, and wider MOD policy.
SCIDA	Site Co-ordinating Installation Design Authority, appointed to undertake specific SCIDA duties with respect to a single site or group of sites.
Survey	A detailed, pre-planned examination of existing ICT infrastructure to gain an understanding of the current condition of installations, records and procedures. A survey task is normally associated during baseline activities.
TEMPEST	The name given to the phenomenon of unintentional emanations of compromising signals from electronic equipment or systems.

CIDA Governance Team Contacts

Address:

CIDA Governance
Blumlein Building
Blandford Camp
Dorset DT11 8RH

Contacts:

Appointment	Name	Details
CIDA Governance TL	Mr Andrew Goss	S4B: 0300 157 6996 Email: Andrew.Goss455@mod.gov.uk
CIDA Governance 1	Mr Gregory Ramsden	S4B: 0300 152 8206 Email: Gregory.ramsden101@mod.gov.uk
CIDA Governance 2	Mr David Richardson	S4B: 0300 165 4160 Email: David.Richardson505@mod.gov.uk
CIDA Governance 4	Mr David Butler	S4B: 0300 154 5956 Email: David.Butler131@mod.gov.uk

CIDA Governance Group Mailbox: **UKStratComDD-OPS-CS-DS-CIDAGrp@mod.gov.uk**

Appointed SCIDA contact (to be completed by the SCIDA)

Address:

Telephone contacts:

Email contacts:

Introduction

1. In compliance with legal requirements the HMG Security Policy Framework[1] and the Cabinet Office Information Assurance Governance Framework, CDIO, through D CBM J6 Executive Group, established the MOD CIS Resilience Policy and Recovery Strategy and the DSO published JSP 440[2]. These MOD policy documents mandate Information and Communications Technology (ICT) security, resilience, Configuration Management (CM), Change Control (CC), installation design control and accreditation processes, thus directly delivering the Cabinet Office governance requirement for compliance with BS ISO/IEC 27002, the provision of an accreditation process and the use of ITIL best practice.

2. Responsibility for the implementation of security policy and standards is formally delegated to TLB Holders by the Permanent Undersecretary. In turn, TLBs appoint Principal Security Advisors with responsibility for the systems that the TLB is the information owner of.

CIDA Governance and SCIDA

3. To ensure the correct physical and environmental aspects of all MOD ICT fixed infrastructure are installed in a safe and secure manner, the lead authority is Coordinating Installation Design Authority (CIDA) Governance who are a sub-department of the Defence Digital Operations Pillar. CIDA Governance provide direction to the Defence Digital Defence Enterprise Site Coordinating Installation Design Authority (DE SCIDA) and other contracted SCIDA resources to ensure that all MOD ICT installations are compliant with JSP 604 Leaflet 4800[3] and other associated standards.

4. Each site is appointed a SCIDA from SCIDA resource, a periodically updated list of appointed SCIDA is available on DefNet. JSP 604 Leaflet 4800 Ch 1 details the roles and responsibilities of a SCIDA and Ch 4 defines the CC procedures that they implement. The appointed SCIDA will provide support aligned to the assigned Service Level of that area.

Service Levels

5. In some situations, an MOD site is assigned a specific Service Level or more commonly a site can be divided into Service Levels allocated to buildings, rooms or even to isolated ICT systems within a facility. The Service Levels are assigned to ensure that the relevant level of SCIDA support is afforded to all facilities and the areas with specific business requirements exposed to higher risk from change activity are given the maximum level of support. This approach gives the greatest benefit to operational capability, safety, and security.

6. Three Service Levels have been devised to reflect the degree of SCIDA support activity required to comply with the requirements. Service Levels are assigned to areas through consultation between the Head of Establishment (HOE) or designated representative and the SCIDA. Depending on various factors a Service Level is subject to change by agreement of all relevant parties. Additional to managing ICT infrastructure change through a formalised process, SCIDAs will maintain Configuration Management Database (CMDB) documentation where required, deliver a planned program of configuration management tasks and conduct periodic facility audits that correlate to the assigned Service Levels. SCIDA audit forecasts and resultant reports will be communicated

[1] HMG Security Policy Framework Version 1.1 dated May 2018

[2] JSP 440 - The Defence Manual of Security

[3] JSP 604 Leaflet 4800 - CIDA Governance Installation Regulations

with site HoE or representative directly. In the absence of a HoE or appointed representative, the SCIDA will inform a nominated equivalent. Table 1 details the three Service Levels, allocation criteria and SCIDA activity associated to each level:

a. **Table 1**.

SCIDA SERVICE LEVEL	SERVICE LEVEL ALLOCATION CRITERIA SITE/FACILITY/SYSTEM	SCIDA CHANGE CONTROL	MINIMUM MANDATORY AUDIT FREQUENCY	CM DOCUMENT REQUIREMENT	SCIDA SUPPORT ACTIVITY
1	1. **Directly** supporting operational capability. 2. **Any** installation of voice and data equipment accredited above SECRET. 3. A high population* of voice and data equipment accredited at SECRET. 4. Supporting flight or maritime safety.	1. Establish a CMDB Baseline and maintain through a formal change process accordingly. 2. Full ECR process mandatory. JSP 604 Leaflet 4800 Ch 4 details the ECR process.	12 months.	Establish and maintain a minimum CMDB data set specific to the level of protective marking inclusive of TEMPEST coupling zones.	1. Manage the ECR process (or equivalent). 2. Implement measures to prevent unauthorised change. 3. Maintain the CMDB and associated documentation. 4. Conduct mandatory audits.
2	1. Not directly supporting operational capability. 2. A low population* of data processing equipment accredited at SECRET. 3. A high population* of voice and data equipment accredited OFFICIAL and below.	1. Establish a CMDB Baseline and maintain through a formal change process accordingly. 2. Full ECR process mandatory. JSP 604 Leaflet 4800 Ch 4 details the ECR process.	24 months.	Establish and maintain a minimum CMDB data set specific to the level of protective marking inclusive of TEMPEST coupling zones.	1. Manage the ECR process (or equivalent). 2. Implement measures to prevent unauthorised change. 3. Maintain the CMDB and associated documentation. 4. Conduct mandatory audits.
3	1. Not directly supporting operational capability. 2. A low population* of voice and data equipment accredited OFFICIAL and below.	Full ECR process mandatory. JSP 604 Leaflet 4800 Ch 4 details the ECR process.	Sample audit at the discretion of the SCIDA and relevant stakeholders.	A drawing set maintained for new installations/changes.	1. Manage the ECR process (or equivalent). 2. Implement measures to prevent unauthorised change. 3. Conduct inspections as required.

* The appointed SCIDA is to evaluate the population and allocate a Service Level accordingly.

Minimum CMDB data sets

7. The minimum CMDB data sets differ between Service Levels, Table 2 details the requirements for each:

a. **Table 2**:

	Service levels		
Documentation	**1**	**2**	**3**
Building floor plans detailing telecommunications outlet locations and ICT cable containment runs	M	M	D
Network Equipment Room and Data Centre layout plans	M	M	D
Rack face layouts (cabinet faceplans)	M	M	D
Cable straight line diagrams (schematics)	M	M	D
Site plans detailing ICT outside plant (pits and ducts)	M	M	D
All formal change process documentation	M	M	M
Building elevation plans, wall views etc	D	D	D

M = Mandated
D = Desirable

CIDA Governance audits

8. To evaluate if the correct level of SCIDA support to the assigned Service Level is maintained, CIDA Governance audit against five core SCIDA processes:

a. **Process 1** - Establish and Maintain a CMDB baseline.

b. **Process 2** - Employ and maintain a formal Change Control process.

c. **Process 3** - Update drawings, associated configuration documents and other relevant information.

d. **Process 4** - Provide SCIDA advice.

e. **Process 5** - Conduct SCIDA audits relevant to assigned service level(s).

9. To assist in the standardisation of the SCIDA audits, these processes are broken down into sub-requirements which are expanded in the tables below:

a. **Table 3:**

Process 1 – Establish and Maintain a Configuration Management Database Baseline		
Requirement	**Item**	**Sub-Requirement**
A primary requirement of the SCIDA is to understand the ICT infrastructure and installations in their appointed area. Each facility or system requires to be surveyed to gain an understanding of the state of inherited installations, CMDB records and procedures. This baseline activity is to be	1.1	Include and carry out baseline activities within business as usual routine SCIDA audits.
	1.2	Update CMDB documents with the relevant drawing office.

undertaken during routine SCIDA audits and so carried out incrementally with full completion not exceeding 24 months of area appointment. Details of the baseline activities are to be included on the SCIDA audit reports, any non-conformances are to be highlighted to the relevant risk owner for inclusion on the site risk register and risk numbers allocated for future reference.	1.3	Include baseline activities on SCIDA Audit reports.
	1.4	Non-conformances identified during the baseline surveys are highlighted to the relevant risk holder as required.

b. Tasks related to creating and establishing a baseline can vary depending on the area to be surveyed. The initial full baseline should be a **once only** activity then the maintenance of the CMDB documents are routine, ongoing SCIDA tasks through the formal change process.

c. Table 4:

Process 2 - Employ and maintain a formal change control process		
Requirement	**Item**	**Sub-Requirement**
It is essential to prevent unauthorised change which undermines SCIDA control therefore there is a need to establish and use a robust CC process where the SCIDA is notified of a proposed change at the earliest opportunity. All proposed change must be authorised by the appointed SCIDA. Any change without notifying the SCIDA is classed as an unauthorised change and a breach of MOD policy. The formal CC process maintained by CIDA Governance contains 5 elements; the Engineering Change Request (ECR) model process is provided in JSP 604 Leaflet 4800 Ch 4. Equivalent documentation can be used providing that as a minimum all the information detailed in the formal ECR process documents are included. Changes are to be assessed to ensure compliance with MOD requirements and are not to adversely affect the site, existing systems or other concurrent change(s). Resources may dictate the level of SCIDA CC applied to Service Level 3 areas however in all cases, regardless of Service Level, the change process must be followed.	2.1	A record is to be maintained of every ECR 1, ECR 2, ECR 3, ECR 4 and ECR 5 (or equivalent).
	2.2	On submission of ECR 1, supply drawing requests to change proposers within 10 working days.
	2.3	Within 5-10 working days of the physical change (installation, relocation or removal) assess each completed change for conformance with MOD requirements. This involves a physical inspection and includes an assessment of the documentation supplied for completeness and accuracy.
	2.4	All CM records are to be updated and filed within 5-10 working days of assessing each completed change. This timeframe includes lodging CMDB updates with the relevant drawing office.
	2.5	During protracted installation work the SCIDA is to periodically assess the change to identify potential issues early enough for change proposer resolution prior to the change being completed.
	2.6	If an occasion occurs where the change has been completed without ECR 4 submission and non-conformance has been identified, this is to be highlighted to the relevant risk holder as required and the site risk register updated accordingly.
	2.7	If unauthorised change has been identified, attempts shall be made to prevent reoccurrence. The unauthorised change agent should be identified and the details provided to the relevant site stakeholder.
	2.8	Any local issues with change, installation standards or procedural refusals that cannot be resolved by SCIDA are to be raised to CIDA Governance. This includes organisations unwilling to follow the formal change process or bad installation practice.

d. **Table 5:**

Process 3 – Update drawings, associated configuration documents and other relevant information		
Requirement	**Item**	**Sub-Requirement**
‘As Fitted’ or ‘As Built’ drawings are required in support of CM. For existing installations, they should be current, readily available and provide a complete history of change. To bolster the CM portfolio and to aid with proposed future ICT installations, the SCIDA should engage with the relevant site FM team to gain any relevant drawings. This could include, but not limited to, site plans, underground service plans, building floor plans etc.	3.1	Ensure all necessary CM information is complete, accurate and readily available. CC and CM documents are to be stored electronically in the relevant shared area. All CM drawings are to be filed with the relevant Drawing Office who will maintain and store these in an accessible shared area.
	3.2	Update CM drawings, databases and any other relevant CM documentation as required. This is an ongoing task through the course of SCIDA duties. Updates are to be completed and filed with the relevant Drawing Office within 10 working days.
	3.3	For Service Level 1 and Service Level 2, establish and maintain a record of ‘Approved Routes’ (red/black shared OSP/CMS) that can be referenced for future inspections and proposed new installations.
	3.4	For underground ICT cable proposed installations, follow the formal change process. All requests for cross-site route drawings (if held) are to be provided within 10 working days.
	3.5	Liaise with the site FM Team or equivalent to gain drawings to complement the CMDB.

e. **Table 6:**

Process 4 – Provide SCIDA advice		
Requirement	**Item**	**Sub-Requirement**
To underpin CM at a site, the SCIDA will provide support and advice to all stakeholders. This support will include technical advice to change proposers and change designers on matters of installation standards and associated standards, regulations and policy.	4.1	Respond adequately to all requests to provide technical advice and assistance within 10 working days of receipt. An adequate response is considered an answer to the query or a holding reply to gain external advice on their behalf. The holding response is to give a date or time frame for the reply.
	4.2	Attend and provide input to any relevant boards, meetings, or forums. These could be project meetings, change advisory boards, site periodic infrastructure meetings, siting boards, invitation to tender etc. All relevant meeting minutes or records of decisions which may affect current or future ICT infrastructure are to be held with the CC pack.
	4.3	Establish and maintain relationships with pertinent key stakeholders in the assigned Area of Responsibility (AOR). This could be HoE, FM Team, Estate Team, G6 community etc.

f. **Table 7:**

Process 5 - Conduct SCIDA audits relevant to assigned Service Level(s)		
Requirement	**Item**	**Sub-Requirement**
To ensure continuing conformance to CIDA Governance requirements, sites, facilities, or systems must be regularly inspected by the SCIDA. The frequency of inspection is determined by the assigned Service Level. This will require the creation of a SCIDA inspection program that must be communicated with the HoE or equivalent. Inspections of each area are to assess the current state/condition of the ICT infrastructure, highlight unauthorised change and any deterioration of installation standards i.e. bad practice. This information is to be included in an inspection report. Any non-conformance is to be highlighted in the report with remediation recommendations and suggested resolution timelines.	5.1	Maintain a SCIDA audit program incorporating all sites, facilities, and/or systems in the SCIDA configuration AOR. This should be a live document and the program should clearly articulate the areas to be inspected and the intended period. The program is to be agreed and shared with the HoE or equivalent and other stakeholders.
	5.2	Carry out audits in accordance with the agreed plan.
	5.3	When conducting audits, the SCIDA is to also observe and report on any issues regarding important enabling provisions for ICT Infrastructure. This could include ICT cabinet/NER power provisions or cooling provisions (Air Conditioning (A/C) or Heating Ventilation Air Conditioning (HVAC)).
	5.4	On completion of a planned inspection, within 5-10 working days a submit a comprehensive report to the relevant stakeholders (HoE, FM Team etc).
	5.5	From audit findings, inform the relevant risk holder of any non-conformant installation details and request risk register inclusion with risk numbers for reference in future SCIDA audits.

g. To enhance document security and to streamline the data capture process, SCIDA activities may involve the use of MOD approved IT (Laptop, iPad etc) in secure areas above OFFICIAL protective marking. The SCIDA is to gain advance written approval for use of this equipment in these areas from the relevant site security department.

Service Level assignments

10. The SCIDA configuration boundary covers all aspects of fixed ICT infrastructure within the AOR. Table 8 details the Service Level assignment which is to be completed by the SCIDA and agreed with the HoE or representative. Once agreed this document is to be signed by these parties and held on electronic record in the relevant repository. A signature block is provided in Table 9. A copy of this document is to accompany the Defence Digital site agreement and is to be reviewed and resigned annually. All previous versions are to be archived in the relevant repository for future reference.

a. Table 8 – Service Level Assignments (SCIDA to add/delete rows as required):

Insert site name		
Ser	**Facility/Building/System**	**Assigned Service Level**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		
32.		
33.		

b. **Table 9:**

The signatures below acknowledge that:

1. The Service Level(s) detailed in Table 8 have been agreed with the HoE (or representative) and the appointed SCIDA. This document will be reviewed and reissued annually by the appointed SCIDA.

2. The HoE (or representative) has received a signed copy of this document.

HoE or appointed representative		**Appointed SCIDA**	
Name		Name	
Rank/Grade		Rank/Grade	
Appt		Appt	
Date		Date	
Signature		Signature	
Contact e-mail		Contact e-mail	

Notes provided by the SCIDA

11. This para is a free text area for the appointed SCIDA to add any pertinent points they wish to make the HOE or empowered representative aware of. Such points may be:

a. Access to certain key areas.

b. Site support required to carry out SCIDA duties.