

Reference: G-Cloud Support
Site Co-Ordinating Installation Design Authority
Supplementary Services

To Support the G-Cloud framework

- SCIDA Nationwide Support

Installing Confidence

Data Installation and Networking Services Ltd. Registered No 2802029



Contents

Introduction	3
Scope.....	4
1.Establishment of site based SCIDA teams.....	4
2.Baseline package.....	4
3.Change Control	4
4.Configuration Management.....	5
5.Drawing Library	5
6.Configuration Audits	6
7.Wireless Installation.....	6
8.Duct Management	6
9.Subject Matter Experts	6
Site List	6
Out of Scope.....	7
Options.....	7
Resource Structure.....	8
Geographic locations	9
Infrastructure & IT.....	10
Service Levels	10
Baseline Activities	11
Mobilisation	12
Costings	13
Option 1 – SCIDA Resource	13
Option 1a – SCIDA T&S.....	13
Option 1b – Additional CIS Taskings	13
Option 2 – Baseline	13
Option 3 – Change Control.....	13
Option 4&5 – Configuration Management	13
Volumes	14
Experience.....	15
Service Management	15
Assumptions.....	15
Exclusions	15

Introduction

Extracted from JSP604 - Regulations for the Installation of Information Communications Technology (Formally JSP 480)

“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

SCIDAs shall be established and maintained for all ICT facilities. Defence CIDA’s SCIDA Framework Document establishes the delivery requirement for SCIDAs to provide the necessary configuration management of the physical and environmental aspects of Defence ICT Installations.

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 Site CIDA (SCIDA). All MOD facilities shall have a SCIDA, established in accordance with the Defence SCIDA Framework Document and recognised by Defence CIDA. All CIS change at site level must be in accordance with the requirements of JSP 480, 604, 440 and 375 and agreed with the SCIDA.”

Currently not all sites have formal SCIDA coverage.

Without a formal SCIDA process in place, uncontrolled change is taking place and as such there is a risk of 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” which is contrary to the requirements of the HMG Security Policy Framework (SPF).

This proposal provides compliance to the HMG SPF and ensures the responsibilities of the TLBs and any delegated responsibility to the Head of Establishment are met by the provision of Site CIDA resources and associated configuration management processes.

There are obvious risks in relation to uncontrolled change in relation to Health & Safety, Fire Protection and Electrical Safety, as such this proposal seeks to provide protection to the MOD in a timely manner.

We have based our service on the following information:

- JSP604, 440 and 375
- Health & Safety at Work act

Scope

1. Establishment of site based SCIDA teams

The Site CIDA (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 ensuring an assessment of the risk to the Confidentiality, Integrity and Availability of the ICT systems and data has been undertaken and formally recorded

2. Baseline package

SCIDA are responsible for establishing a facilities configuration management baseline, the level of detail held will vary based upon service level applicable to the site. It is unlikely to date that a baseline has been maintained, as such an initial audit will be required.

3. Change Control

All CIS change at site level must be in accordance with the requirements of JSP 480/604 and agreed with the SCIDA

To comply with the requirements of JSP 604:3000 CIS Security Requirements, successful security accreditation of any Information and Communications Technology (ICT) affected by any 'Change' within a MOD site is dependent upon Installation Approval being granted by CIDA. This requirement is satisfied through the issue of a CIDA Certificate of Installation Conformance. On MOD sites this is the responsibility of the SCIDA who will be responsible for Configuration Management (CM) of the ICT systems within their site and keeping Defence CIDA informed of their site CM status.

The CIDA ECR process consists of five parts, each of which has a specific purpose in the Change Control of ICT facilities. The five parts for the ECR process are as follows:

Part 1 ~ Initial Project Information.

Part 2 ~ Change Proposal and Request for Design Endorsement.

Part 3 ~ Design Endorsement of a Change Proposal.

Part 4 ~ Installation Completion Statement.

Part 5 ~ Certificate of Installation Conformance

In addition, all changes affecting Radio Site Restriction zones, for sites occupied by Microwave Links, Navigation Aids, Radars and Radios or similar C-E equipment must be separately notified to MOD-RSP in accordance with JSP604

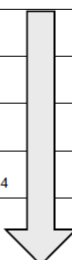


4. Configuration Management

JSP 886, Vol 7, Part 8.12 ~ “Configuration Management” defines Configuration Management (CM) as a management discipline that applies technical and administrative direction to the development, production and support life-cycle of a configuration item. The discipline is applicable to hardware, infrastructure, software, processed materials, services and related technical documentation. CM is an integral part of life-cycle management, and is applicable to the support of projects from concept through to design, development, procurement, production, installation, operation and maintenance and to the disposal of products.

The main objective of CM is to document and provide full visibility of the product’s present configuration and on the status of achievement of its physical and functional requirements. A further objective is that everyone working on the project at any time in its life-cycle uses correct and accurate documentation.

Configuration Management (CM) requires resources and thus must be directed where the gain is most tangible. The CIDA Service Levels for MOD facilities are designed to ensure that areas with the highest business importance are afforded the most significant protection

Table 2-2 Minimum SCIDA CM Requirement

Item	Activity	Service Level 1	Service Level 2	Service Level 3
1	SCIDA Advice			
2	Change Control Process			Note 1
3	Maintain Drawings &			Note 3
4	Conduct SCIDA Inspections			Note 5
5	Establish the Facility's CM Baseline			
Notes: 1. Notification of all Change (ECR Pt 1 or equivalent) is mandatory. The need for ECR Pts 2 – 5 will be determined by SCIDA. Decisions not to proceed to ECR Part 5 will require a form of written design endorsement to the Design Agency and written installation conformance to the Security Accreditor. 2. Create & maintain TEMPEST drawings for all ICT systems processing information at SECRET or higher. IDA 'As Fitted' Drawings, or alternatively CM Drawings, are to be held. 3. IDA 'As Fitted' Drawings may be held. 4. Mandatory yearly Inspection of all ICT systems by SCIDA. 5. Mandatory 2 yearly inspection of all ICT systems by SCIDA. 6. Inspections by SCIDA on request from site.				

5. Drawing Library

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 in JSP604

Service Level 1 – Requirement to maintain a full drawing CM system (+ SL2 + SL3)

Service Level 2 – Create & Maintain Tempest drawings (+SL3)

Service Level 3 – As Fitted drawings may be held

6. Configuration Audits

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. Baseline records will be updated accordingly.

7. Wireless Installation

As per JSP604, ALL wireless installations are to be the subject of SCIDA control.

All requirements to apply change to Radio Frequency (RF) emitters/receivers on MOD sites must include an early application, in accordance with JSP 604:3032 Radio Site Clearance to MOD-RSP for approval, Radio Site Clearance and amendment of the Register of Radio Sites (RRS). Information on any RF propagation path safeguarding requirements must be included in these applications to enable protection, for each site, against degradation by future development or installation.

8. Duct Management

As per JSP604, ALL cross site ducting and cables are to be subject to CM and will be treated as Service Level 2 as a minimum.

9. Subject Matter Experts

The SCIDA resource is available to support CIS planning meetings, contractor technical meetings, scope definitions, non-conformance meetings etc on behalf of the Head of Establishment, undertaking an SME role in the CIS environment.

Out of Scope

There is no requirement to cover :-

Sites already under ISS SCIDA contract provision
PFI Sites such as Aspire and Holdfast

However, the resource would still be available to provide subject matter expert type support if required.

Options

The following options have been offered as a comprehensive solution to the requirements of the scope, it is recommended all options are taken as without full service provision the requirements of the SPF are not met.

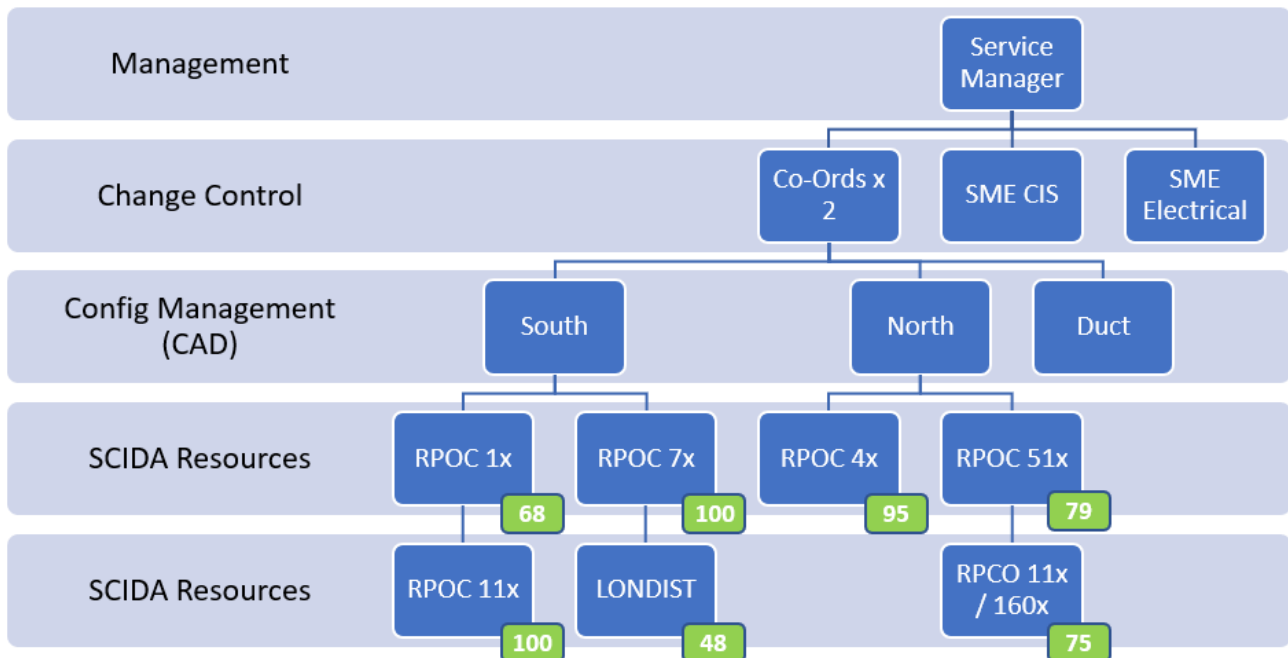
Opt	Title	Scope
1	SCIDA Resources	Regionally based personnel to undertake the SCIDA role
2	Change Control	Central Management of ALL CIS change
3	Configuration Management	Creation and management of a central 'As Fitted' library including TEMPEST drawings
4	Duct Management	Treated as per Service Level 2
5	Baseline	Initial capture of the site baseline information

The risks remain if all options for a full SCIDA service are not provided:-

- Loss or reduction of Confidentiality, Integrity, Availability or Resilience
- Health & Safety
- Fire Protection
- Electrical Safety

Resource Structure

To provide the default coverage we can offer the following resources to be deployed as, when and where required to support G-Cloud deployments.



Infrastructure & IT

It is suggested 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 that to best maximise the availability of the baseline information, drawing libraries and associated change control systems that all users be on the MoDNET network.

As such we have assumed that MOD will provide the team with:-

- Standard laptops
- Desktops
- User accounts
- Appropriate sharepoint storage for drawing library

Service Levels

We would suggest that the following service levels be implemented and reported on to demonstrate the success of the service, we would work with G6 RPOC to finalise the SLA schedule:-

SLA	Scope
10 Days	Respond to ECR1
10 Days	Respond to ECR2
5 Days	Attendance on site for SME work
20 Days	Site Audit
20 Days	Respond to ECR4
95	% of above within SLA

We would recommend regular review meetings to measure the success of the service and to enable the customer to prioritise tasks where the resource is stretched.

- Establish terms of reference prior to the start of a project
- Provide the customer with a defined structure for delegation, authority and communication
- Divide the project into manageable stages for more accurate planning
- Ensure resource commitment
- Provide regular management reports
- Hold meetings with management and stakeholders at the vital points in the project.
- Those who will be directly involved with using the results of a project are able to:
 - Participate in all the decision-making on a project
 - If desired, be fully involved in day-to-day progress
- Provide quality checks throughout the project to ensure their requirements are being adequately satisfied.
- Document and monitor change control

Baseline Activities

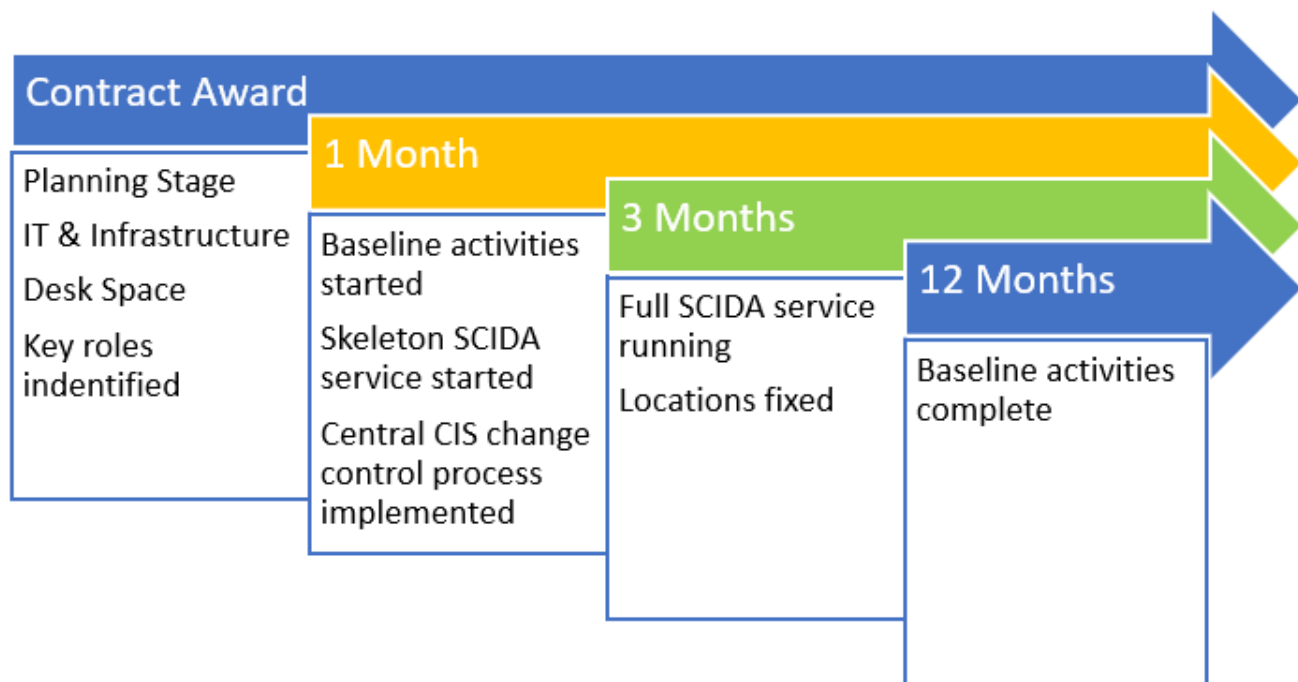
In order to create a baseline documentation set off each site (in line with its service level) the following activities need to be undertaken:-

- **As Fitted capture**
Find, collate and document any existing ECR5 documentation sets. Catalogue and store such that it can be used to form a baseline.
Work with the AP to understand electrical status (if any) of existing CIS cabinets
- **Site Audit**
Attend site and review the information gathered.
Review uncontrolled change
Capture any non-conformances
Create TEMPEST drawings in line with JSP604
Capture Electrical status of cabinets on site
- **Output of the Audit**
Create a Baseline
Based upon service level either create a full CM or an as fitted library for the site
- **Remedials**
Capture of missing information
Update As Built with uncontrolled change
Chase through ECR4 non-conformances

The requirement for SCIDA provision on the site list is instant, as such we recommend that the baseline activities are undertaken in parallel by separate resource to ensure the MOD see the benefit from the SCIDA service as soon as possible.

This allows us to instantly start impacting any urgent SCIDA requirements within the estate using the SCIDA resource being deployed.

Mobilisation



1

Costings

Item	Title	Unit
1	SCIDA Resources	Per Engineer Day
1a	Junior	Per Engineer Day
1b	Senior	Per Engineer Day
2	T&S	Per Engineer Day
3	Configuration Management CAD	Per Day
4	Team Management	Per Day
5	Baseline	Per Engineer Day

Option 1 – SCIDA Resource

Provision of SCIDA engineer(s) as per this proposal.

We have offered two solutions:-

1. Based on an entry level skill set supported by a more senior SCIDA SME
2. More senior regional SCIDA resources without the central SME.

Option 2 – SCIDA T&S

Travel & Subsistence associated with Option 1.

Option 3 – CAD Services

Drawing office functions (CAD) related to Item 1.

Option 4 – Team Management

Relevant on large tasks

Option 5 – Site Baseline activities

Site survey works by cabling engineers to be fed back in to SCIDA

Volumes

There are no customer provided volumetrics, as such we have made assumptions as below.
The costings are based upon a maximum number of activities.

To model the requirement we have created an average job and mapped the activities to time as per the table below, this is for the full lifecycle of a CIS task and the assumption is that you would have multiple tasks at different stages of this process.

Total HOURS	<u>2</u>	<u>1.25</u>	<u>5</u>
Typical touch points vs time vs resource	PMO	CAD	SCIDA
Log & Acknowledge ECR1	0.5		
Review database and respond to ECR1		0.25	0.5
Track upcoming task	0.25		0.25
Log & Acknowledge ECR2	0.5		
Review and respond to ECR2			1
Submit ECR3	0.25		0.25
Log ECR4	0.5		
Review & Respond ECR4			1
Site Visit			1
Update CM Database		1	
SME Assistance			1

The times are an average, not all sites would involve SME assistance or a site visit, this is purely an average model.

Experience

Data Techniques has 15 years working experience installing CIS across all MoD sites.
We are expert in CIS delivery with all works compliant to exacting JSP standards
Our Site Management & Project Management people are CIDA qualified
All our Supervisors are "Black Hat" qualified & accredited
All our site teams have SC clearance, CSCS cards as minimum

Service Management

Data Techniques will assign a service manager to deliver any project. They will be assigned for the duration of the programme, whose responsibilities will include the following:

- Coordinate a works programme
- Prepare of Method Statement and Risk Assessments
- Ensure key milestones are met
- Attend weekly site meetings where necessary
- Ensure that the quality of service is maintained

Assumptions

We have assumed the following:

- Unrestricted access to required areas for the duration of the works
- All works to be carried out during daytime hours 08:00 – 18:00 Monday – Friday

Exclusions

We have not allowed in our response for the following items:

- Out of hours working

We trust our quotation meets with your immediate requirements, however if you require any further information please do not hesitate to contact the undersigned.

Yours faithfully

Richard Green
Defence, Justice and Central Government



m: **07766 467764**
e: **richard.green@datatechniques.co.uk**
w: www.datatechniques.co.uk