

Technical Assurance in the Cloud (TAC)

Service Definition Document

Version Number:	V1.0
Releasable to:	Crown Commercial Services, G-Cloud Framework

Cadmidium Services Ltd
Tel 01242 861459
services@cadmidium.co.uk
www.cadmidium.com

Table of Contents

1	Technical Assurance in The Cloud.....	5
1.1	Service Overview	5
2	TAC Components.....	6
2.1	10 Key Components of our TAC Service	6
3	TAC Service Benefits.....	7
3.1	10 Key Benefits of our TAC Service	7
4	How TAC Works	8
4.1	Scoping	10
4.2	Design.....	10
4.3	Build	10
4.4	Managed Change	10
4.5	Inspect	11
5	Business Continuity	12
6	Account Management.....	13
7	Commercial Statement	14

Table of Figures

FIGURE 1 – TAC ACCREDITATION SUPPORT – END TO END PROCESS.....	9
--	---

Confidentiality Statement

This document, or any information contained within it, must not be provided, or issued to any third party without the prior written consent of Cadmium Services Limited. This restriction does not apply to 'copies' for the sole use of customer staff involved in this project.

Document Issue

Version	Author	Comment/Reason	Date
1.0	Cadmidium Services	Creation & Publication	14/11/2025

*Any designs contained in this document are the Intellectual Property of
Cadmidium Services Limited*

Glossary

Acronym	Description
CAS(S)	NSCC Commodity Assured Service (CAS) scheme
CPNI	Centre for the Protection of National Infrastructure
TAC	Technical Assurance in the Cloud
GFX	Government Furnished Equipment
ICT	Information and Communications Technology
IDA	Installation Design Authority
ISO	International Organisation for Standardisation
IT	Information Technology
NATO	North Atlantic Treaty Organisation
SCIDA	Site Co-ordinating Installation Design Authority
SD	Service Definition
SME	Subject Matter Expert

1 Technical Assurance in The Cloud

1.1 Service Overview

All Cloud systems, that store and process protectively marked information, business, or operationally critical data, or that are interconnected to cross-government networks or services must be installed to standards. Any change should be managed, controlled, and documented and systems should be delivered compliant and in accordance with JSP 604.

Our Technical Assurance in the Cloud (TAC) services provide comprehensive engineering activity to manage change effectively to ensure Confidentiality, Integrity, Availability, Flexibility, Resilience and Economy of your data and services, our compliant change management service uses the Engineering Change process as laid down in JSP 604 Leaflet 4800.

TAC ensures that your cloud solutions, cloud hosted data & equipment are appropriately installed, and compliant with government requirements, law, and wider MOD policies.

Contained within our service are offerings for each stage of engineering activity in the Cloud.

2 TAC Components

2.1 10 Key Components of our TAC Service

- **Design compliance review, GFX identification & Assurance.**
Review of Design proposals and as fitted packs to ensure compliance.
- **SCIDA qualified inspections to ensure JSP 604, JSP 440 & SDIP 29/2 compliance.**
Against JSP 604 Leaflet 4800, ensuring compliance and the specification of remediation requirements.
- **IDA service.**
Experienced, able to produce viable designs focused on customer and ISO/JSP requirements.
- **Provide TEMPEST Solutions to sensitive data installations.**
Detailed designs and/or solution considerations to ensure installation compliance and supply the Risk Owner with information on their system or installations risk profile iaw JSP 440.
- **Provide a full auditable record of a change.**
Managed Engineering change request process, providing a unique (ECR) iaw JSP 604 Leaflet 4800, Ch 4.
- **Engineering documentation scrutiny, for physical installation design proposals.**
Technical authority providing scrutiny of as fitted packs, identification of noncompliance and GFX requirements.
- **Provide governance, policy, advice, and guidance regarding installation standards.**
Project Support professionals able to advise on JSP's, BSEN, electrical and H&S publications
- **Specialist compliant installation service Providing all aspects of MOD data processing.**
Telecom engineers able to install conformant rack mountable equipment in varied ICT environments.
- **Provide Auditing facility in accordance with JSP 604 Vol 2 Leaflet 4800, and ISO 27001 requirements.**
Conduct inspections, audit functions on installations.
- **Decommissioning and disposal service – Equipment & Data.**
Physical removal of decommissioned cloud \ data centre equipment & data, CAS(S) & CPNI approved.

3 TAC Service Benefits

3.1 10 Key Benefits of our TAC Service

- **Confidentiality**, provide advice and guidance to RADSEC requirements. Where applicable during project initiation/start-up and through the life of the installation processes.
- **Integrity**, by ensuring good practices to counter any EMC. Inspection and design review to ensure EMC interference from adjacent installations or hostile intent.
- **Availability**, optimising successful Configuration Management in accordance with relevant standards. Fully managed engineering change process aligned to JSP 604 Leaflet 4800.
- **Resilience**, by providing assurance to the IDA. Guidance to ensure that where appropriate, installations are provided with diversity of location, power, connectivity, and cooling to facilitate continuity of service during unforeseen disruptive malfunction.
- **Flexibility**, by ensuring that all documents are maintained & updated. Including that of installation standards, cloud facility installation documents are available and kept up to date and available for future ICT installations.
- **Economy**, by ensuring spare capacity is identified and correctly utilised. Full service including any site combined facility such as pit and duct cross site connectivity paths.
- **Design Assurance SMEs**. Technical experts with varied skilled backgrounds in the SCIDA environment including Risk Management and Risk Balance Case documentation.
- **Project support** to main Gate and onward to Gate 6 (HOTO). Full and dedicated Project "Tiger Team" support through all phases of Project, specialising in delivery of service and solving complex GFX issues and the decommissioning as well as disposal of data and equipment.
- **Auditable trail for the CyDr (DIAS)**. Enabling audits - Service Desk support, including drawing office, plus a Front Door for New Engineering Change Requests (ECR), policy, governance, advice, and guidance provision and ECR registry.
- **Provide an ISO 9001:2015 quality managed technical service**. Auditable process which gives assurance to the customer. Qualified Engineers with suitable knowledge skills and experience delivering technical assurance, auditing facility iaw JSP 604, ISO 27001.

4 How TAC Works

In the complex dynamic and fluid Cloud environment that MOD Maritime/Land/Air and government departments operate within, it is critical to understand the process & necessary procedures to ensure the right approach is taken to Project delivery of a cloud-based solution, to ensure the data centre environment is to standard.

Our Engineering & Technology consultants work with you to navigate the complex world of the Cloud enabling you to understand the timescales, effort and activity required to get cloud-based solutions hosted and secured to the relevant government standard, as well as obtaining the required level of assurance.

This service component encompasses the whole change lifecycle for a secure capability hosting within government cloud environments.

There are 5 phases to this component.

- **Phase 1 – Scope** - Assessing the as is cloud state, identifying GFX requirements, capturing rack face layouts and identification of spare capacity – early intervention will prevent delays later.
- **Phase 2 – Design** – Offering an in-house design service or scrutiny of existing designs to identify JSP 604 Leaflet 4800, JSP 440 & SDIP 29 compliance at an early stage.
- **Phase 3 – Build** – Ensure data centre Cloud equipment is installed to standards. Cadmidium can commission and install equipment.
- **Phase 4 – Managed Change** – Our change process is aligned directly to JSP 604 Leaflet 4800, Cadmidium can offer a full SCIDA service and provide a fully managed service from service introduction through to decommissioning.
- **Phase 5 – Inspect** – Full inspection and auditing can be conducted on request to ensure compliance.

Cadmium - Open

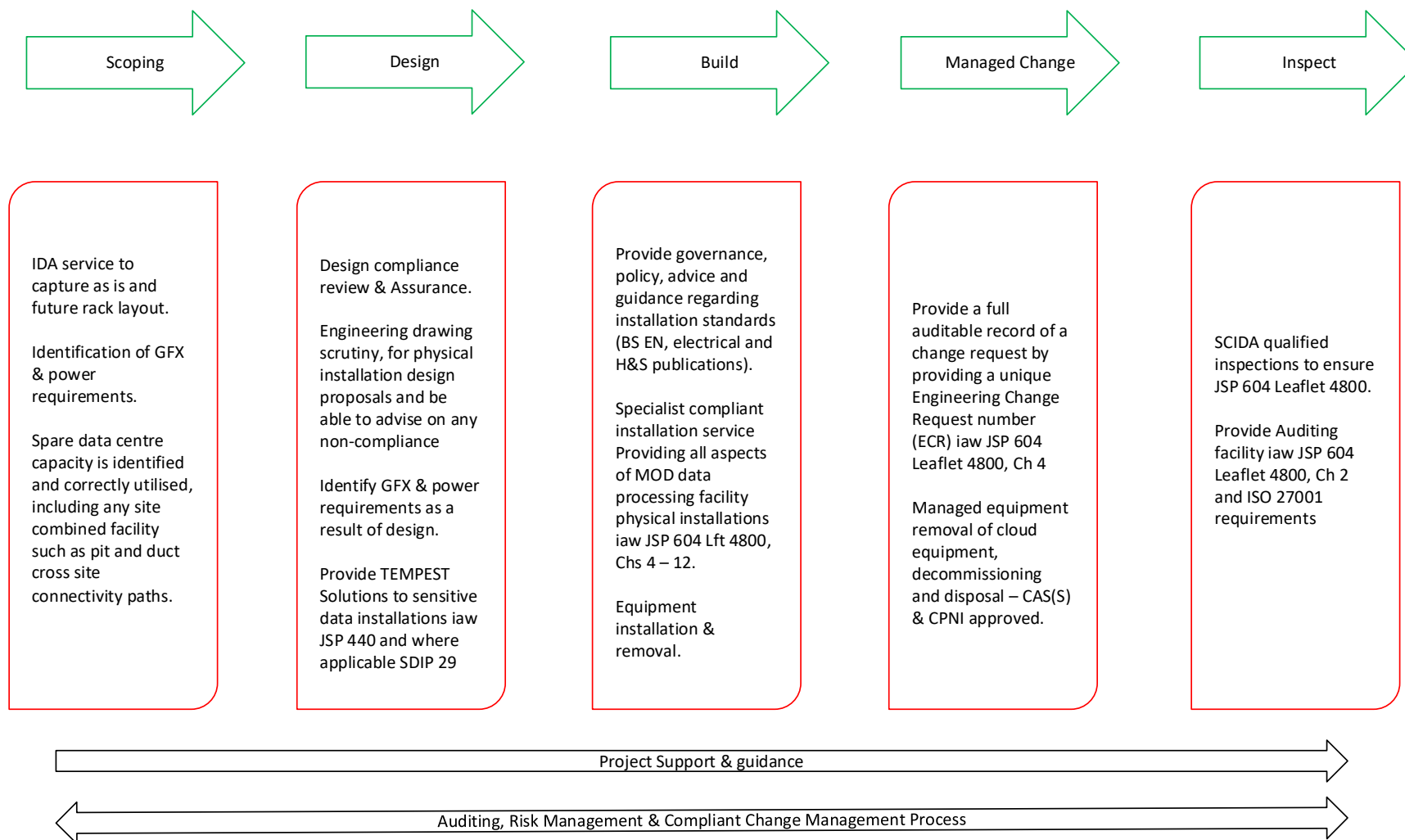


Figure 1 – TAC Accreditation support – End to End process

4.1 Scoping

Having a design for a cloud hosted solution is part of the journey to a successful cloud implementation. Understanding your data will enable an assessment of the manifold threats that need to be contained and controlled with appropriate countermeasures. Our TAC service enables the correct and appropriate level of controls to be applied, ISO27001, National Cyber Security Centre, best practice, or specific customer requirements.

ISO 27001 Auditing. It is important that an organisations Information Security Management System (ISMS) is aligned with information security best practice. This can be assessed by determining the ISMS compliance to ISO 27001. Our service can audit ISMS's to determine if it is compliant with ISO 27001 and to highlight areas needing attention, as well as recommending appropriate remediation activities, to improve the ISMS.

4.2 Design

During the design process local environmental constraints are often not taken into consideration, rack face layouts may be provided but in many cases resilience from power, power requirements and space are not taken into consideration. Our TAC service assesses the design and can identify GFX requirements at an early stage to help prevent delays in delivery, Cadmidium can design from the ground up or scrutinise existing designs to ensure their compliance against JSP 604 Leaflet 4800, JSP 440 and SDIP 29 where required, this is critical.

4.3 Build

Installations must comply to certain laws and regulations, as well as specific governmental department policy. Our TAC service provides guidance and assesses solutions to ensure that all appropriate IT regulations, laws, and governmental department policy are adhered to thereby providing a secure solution that meets governmental department requirements. Cadmidium have an Engineering capability which can also install new equipment to standards, any build is controlled and managed by the Cadmidium in house SCIDA capability.

4.4 Managed Change

The Cloud environment in any data centre or processing facility must be controlled and follow a defined process. Cadmidium Services can put in place the auditable controls and process necessary, so the environment is controlled through a 5-stage Engineering Change Request (ECR) process aligned to JSP 604 Leaflet 4800 and assessed for compliance. Cadmidium can control, maintain, and control the full process or where required contribute to a stage.

Quite often with the introduction of new Cloud services old data centre equipment may well become redundant as systems are retired. Cadmium offer a full decommissioning service which includes the removal of old equipment and data and arrange disposal which is CAS(C) and CPNI approved.

4.5 Inspect

To ensure the Cloud environment is managed and maintained regular inspections should be scheduled and planned & updated on an annual basis. The inspection regime will ensure continued conformance with standards. Inspections should take place whenever there is a change and regular inspections will identify any unauthorised change.

A full report is provided following any inspection and where necessary a Remedial Action Plan (RAP) will be put into place.

5 Business Continuity

Business continuity encompasses a defined set of planning, preparatory and related activities which are intended to ensure that critical Cyber Security services and functions will continue to operate despite serious incidents or disasters that might otherwise have interrupted them. We have excellent business continuity measures within our organisation, which encompass continuity services to our customers during service engagement.

Our own cloud-based solutions are resilient providing 99.99% availability and access to our data. The passage of Military (UK/NATO at Official Sensitive) information is facilitated through Cadmidium ICT systems being MoD Accredited, enabling us to process and store up to OFFICIAL SENSITIVE. This is supported by our UK Government certified secure facility, enabling storing and processing of data up to and including SECRET, including backups of data critical to the provision of our services.

If required, a detailed business continuity plan will be provided upon engagement.

6 Account Management

Our commercial department handles all account queries covering after sales requests. All G-Cloud enquiries should be directed to:

Cadmidium Commercial

e-mail: commercial@cadmidium.co.uk

During the provision of the CSAC service a dedicated account manager will be appointed and will hold regular meetings with our service buyers to ensure we are delivering to your expectations.

As an ISO 9001:2015 and ISO 27001-2022 company we operate a highly effective Quality and Information Security Management Systems which track and log all customer feedback and opportunities for improvements. Through good account management we will continue to strive to improve our services delivered to our buyers before, during and after engagement.

7 Commercial Statement

Copyright: © Copyright Cadmidium Services Ltd 2026. All rights reserved. Other than for the purpose of evaluation of Services, no part of this document may be reproduced, stored, or transmitted in any form without the prior written permission of Cadmidium Services Ltd.

Cadmidium Services