



Cyber Security Assurance in the Cloud

Service Definition Document

Version Number:	V1.0
Releasable to:	Crown Commercial Service – G-Cloud Framework

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

Table of Contents

1	Cyber Security Assurance in the Cloud.....	5
1.1	Service Overview	5
2	CSAC Components	6
2.1	10 Key Components of our CSAC.....	6
3	CSAC Benefits.....	7
3.1	10 Key Benefits of our CSAC	7
4	CSAC Service Components	8
4.1	Cyber Security Guidance and Consultancy.....	8
4.2	Gap Analysis and Business Development Road Mapping	9
4.3	Cyber Essentials & Cyber Essentials Plus	9
4.4	ISO 27001 Support	9
4.5	ISO 27001 Auditing	9
4.6	MoD Assurance Support	10
4.7	Risk Management consultancy to comply with Government and industry standards.....	10
4.8	Cyber Security staff training to facilitate organisational adoption and compliance	10
5	Further Information.....	11
5.1	Identifying Required Data Security Controls.....	11
5.2	System and Data Threat and Risk Assessments	11
5.3	Compliance with IT Regulations, Laws and Policy	11
5.4	Security Policy and Procedures Production and Reviewing	11
5.5	ISO 27001 Auditing	11
5.6	Compliance to DPA18 and GDPR.....	12
5.7	Supporting System Design and Change Management	12
5.8	Assuring that Policy, Procedures and Processes are being Followed.....	12
5.9	Onboarding Solutions Securely into Cloud Environments	12
6	How CSAC Works	13
7	Business Continuity	14
8	Account Management.....	15
9	Commercial Statement	16

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
CSAC	Cyber Security Assurance in the Cloud
DPA	Data Protection Act
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IT	Information Technology
ITHC	IT Health Check
PM	Project Manager
SD	Service Definition

1 Cyber Security Assurance in the Cloud

1.1 Service Overview

'All ICT systems that handle, store and process protectively marked information, business or operationally critical data, or that are interconnected to cross-government networks or services must undergo a proportionate accreditation process to ensure that the risks to the Confidentiality, Integrity & Availability of the data, system and/or services are properly managed'.

Our Cyber Security Assurance in the Cloud (CSAC) service provides comprehensive world class cyber security consultation, guidance and support designed to protect the Confidentiality, Integrity and Availability of your data and services.

CSAC ensures that your cloud solutions and cloud hosted data are appropriately protected and compliant with government security requirements, law, and wider policies, certifications and accreditations.

Contained within our service is the production and reviewing of all required security artefacts, auditing of procedures and processes providing increased confidence that services are fully accreditable for the security environments where they will operate.

2 CSAC Components

2.1 10 Key Components of our CSAC

- Cyber Security guidance and consultancy including SME support.
- Gap Analysis and Business Development Road Mapping.
- Cyber Essentials Support for Cloud based Systems.
- Cyber Essentials Plus Support for Cloud based System.
- ISO 27001 Accreditation support for Cloud based Systems.
- ISO 27001 Internal Auditing services.
- MoD Assurance Support for Cloud based Systems.
- Risk Management consultancy to comply with Government and industry standards.
- Cyber Security staff training to facilitate organisational adoption and compliance.
- Compliance to industry standards, Government, MoD, NCSC, NIST policy/guidance.

Cadmidium

3 CSAC Benefits

3.1 10 Key Benefits of our CSAC

- Confidence that your systems and data are protected appropriately.
- Reduction of the risk of system and data compromise.
- Creation of Cyber Solutions compliant with regulations, laws, security policy.
- Confidence of an accreditable solution during the design process.
- Generation of all required security related documents.
- Assurance that required procedures and processes are being followed.
- Solutions can be deployed quickly and securely.
- Reducing risk of fines caused by mishandling of personal data.
- Increased confidence and trust amongst your partners and customers.
- Accredited systems to MoD standards, opening further opportunities for business.

Cadmidium

4 CSAC Service Components

Our CSAC Service Components cover a range of services, which include, but are not limited to:

- Cyber Security guidance and consultancy including SME support.
- Gap Analysis and Business Development Road Mapping.
- Cyber Essentials Support for Cloud based Systems.
- Cyber Essentials Plus Support for Cloud based System.
- ISO 27001 Accreditation support for Cloud based Systems.
- ISO 27001 Internal Auditing services.
- MoD Assurance Support for Cloud based Systems.
- Risk Management consultancy to comply with Government and industry standards.
- Cyber Security staff training to facilitate organisational adoption and compliance.
- Compliance to industry standards, Government, MoD, NCSC, NIST policy/guidance.

4.1 Cyber Security Guidance and Consultancy

In the complex dynamic and fluid Cyber environment that government departments operate within, it is critical to understand the Cyber Security policies and necessary procedures to ensure the right approach is taken when considering a cloud-based solution, to ensure the data processed and held is protected sufficiently.

Where sensitive data is to be processed the threats are manifold and the process to mitigate the threat is paramount.

Our Cyber Security consultants work with you to navigate the complex world of Cyber Security protection enabling you to understand the timescales, effort and activity required to get cloud-based solutions hosted and secured to the relevant standards, as well as obtaining the required level of assurance.

4.2 Gap Analysis and Business Development Road Mapping

Our process ensures that we develop a full understanding of our customers' requirements, ensuring mutual agreement of actions required and timelines.

- Discovery & Gap Analysis - This phase ensures that all requirements and dependencies are fully captured and documented, with required actions, roles and responsibilities all clearly defined and agreed with our customer.
- Road Map - This outlines the activity to be undertaken to achieve the requirements and objectives set between us and our customers, within the agreed timescale.

4.3 Cyber Essentials & Cyber Essentials Plus

For many companies, Cyber Essentials is the first step to achieving Cyber Security Assurance. Cadmidium have a 3-part standard process for supporting Companies in achieving their Cyber Essentials and Cyber Essentials Plus submissions.

- Gap Analysis. This will identify any areas where improvement is needed in order to meet the accreditation criteria required.
- Review and Submission. Cadmidium will work with you to uplift your knowledge and provide the required evidence asked by the certifying body.
- Final Submission. Cadmidium will support you with any alterations and additional feedback required for final approval.

4.4 ISO 27001 Support

Achieving ISO 27001 can be a daunting process. Cadmidium offers SME support to its customers throughout the entire process. This can include a combination of different phases:

- Gap Analysis between the AS-IS state and the required standards.
- SME review of current documentation.
- SME support in generating required policies and procedures.
- Internal Auditing of ISO 27001 clauses.

4.5 ISO 27001 Auditing

Maintaining ISO 27001 can be a daunting process, with significant demand on certain resource roles. Cadmidium offers SME support to its customers through the provision of qualified Auditors, who can conduct internal audits to ensure continued compliance and to prepare for external accreditor audits.

4.6 MoD Assurance Support

Cadmidium provide support to customers wishing to achieve UK Ministry of Defence Cyber Security Assurance, and their supply chain.

The Assurance journey is a 2-Stage process for the development, collation, and presentation of information to a UK Government Security Assessor. This forms the basis of evidence for an assessment of a company's capability to protect UK Government sensitive information.

Cadmidium provides support and guidance throughout this process in the form of:

- Gap Analysis
- Business Architecture & Modelling
- Business Change
- TLB & Stakeholder Engagement
- Documentation
- Submission

4.7 Risk Management consultancy to comply with Government and industry standards.

Cadmidium provide support to customers wishing to build a successful risk management system which enables and supports their business, while complying with the requirements of government and industry standards.

4.8 Cyber Security staff training to facilitate organisational adoption and compliance

Cadmidium provide support to customers wishing to build a cyber security compliant business. Cadmidium understand that this can involve a significant amount of business change and offer SME training and knowledge transfer sessions to ensure that the changes are adopted and maintained internally.

5 Further Information

5.1 Identifying Required Data Security Controls

Having a design for a cloud hosted solution is just 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 CSAC service enables the correct and appropriate level of controls to be applied, be they ISO27001, National Cyber Security Centre, best practice, or specific customer requirements.

5.2 System and Data Threat and Risk Assessments

Good Cyber security means understanding the threat landscape driven by the sensitivity and quantity of data that you and your system will be processing and holding within the cloud. Our CSAC service assesses the threat landscape, determines the risks present and identifies appropriate countermeasures to be taken to protect the data.

5.3 Compliance with IT Regulations, Laws and Policy

All businesses must comply to certain laws and regulations, as well as specific governmental department policy. Our CSAC service provides guidance and assesses solutions to ensure that all appropriate IT regulations, laws and governmental department policy are adhered to thereby mitigating the possibility of facing legal prosecution and fines, as well as ensuring a secure solution that meets governmental department requirements.

5.4 Security Policy and Procedures Production and Reviewing

All solutions must have the required security policies and procedures in place to provide assurance that the solution is secure and fit for purpose. Our CSAC draws upon many years of experience of producing and reviewing such documentation to ensure that the documentation is produced quickly, accurately and to the necessary detail.

5.5 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 CSAC service audits 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.

5.6 Compliance to DPA18 and GDPR

All solutions that hold and process personal data of UK individuals must adhere to DPA18 and for EU individuals, GDPR must be adhered to. Failure to do this can result in hefty, and company crippling, fines. Our CSAC service ensures that the required documentation, policy, procedures, and controls are in place to meet the requirements of DPA18 and GDPR.

5.7 Supporting System Design and Change Management

Solutions should be designed from the start to be secure. This avoids the “bolting” on of security features post the design phase which delays delivery, costs more and can lead to a less than ideal solution. Our CSAC service works with design teams to ensure that the required security controls are in place based on the data that will be present, the location of the data, where the data will be accessed from and any data exchange requirements.

Once a solution is in place it will require changes to be made through its life to keep it in line with changing business needs and address new policy and vulnerabilities. It is vital that any changes that could affect the security of the solution are assessed and that all changes are made in such a way that the security of the solution is not compromised. Our CSAC service provides guidance and assesses a change management process to ensure all changes are carried out securely. All proposed changes to a solution are assessed to determine if there will be an impact to security and where this is the case alternate solutions are provided.

5.8 Assuring that Policy, Procedures and Processes are being Followed

Having the required policy, procedures, and processes to manage and run a solution is one thing but these must be followed correctly to support the overall security of the solution. Our CSAC service carries out audits to determine the adherence to policy, procedures and processes and identify any areas that require attention.

5.9 Onboarding Solutions Securely into Cloud Environments

When onboarding a solution into a cloud environment, it is essential that this is performed in such a way that the security of the solution or the data is not compromised. Our CSAC service provides guidance on how onboarding into cloud environments can be achieved securely and also produces the required supporting policy and procedures.

6 How CSAC Works

Our CSAC service is focused upon ensuring our customers can gain accreditation of their solutions through the appropriate and correct application of Security controls.

The ten components of CSAC can be bought as a single service or separately based upon your needs.

- Cyber Security guidance and consultancy including SME support.
- Gap Analysis and Business Development Road Mapping.
- Cyber Essentials Support for Cloud based Systems.
- Cyber Essentials Plus Support for Cloud based System.
- ISO 27001 Accreditation support for Cloud based Systems.
- ISO 27001 Internal Auditing services.
- MoD Assurance Support for Cloud based Systems.
- Risk Management consultancy to comply with Government and industry standards.
- Cyber Security staff training to facilitate organisational adoption and compliance.
- Compliance to industry standards, Government, MoD, NCSC, NIST policy/guidance.

Upon initial service request, a detailed plan will be developed to meet your requirements. This plan will identify the appropriate components of service required to meet your needs and will provide a timeline, resources, and overall price.

7 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.

8 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.

9 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