Service Definition

Cloud Secure by Design (SbD)

G-Cloud 14

Cloud Support

C3IA Solutions Ltd

Version: 1.0

Dated: 15th Mar 2024

Contents

Contents

Overview

C3IA provides Secure by Design (SbD) engineers and security leads to enable its clients understand and define the cyber security risks for building appropriate and proportionate cyber security controls within digital services including Cloud. C3IA is experienced in supporting organisations applying SbD throughout their programmes, project or platform lifecycle.

Features

- Development of the business case security concepts and requirements
- Creation and sourcing of an appropriate threat assessment
- Identifying roles and defining responsibilities including risk owners
- Adopting and implementing a risk driven approach
- Aligning security outcomes with project scale and pace, including Agile
- Designing usable, proportionate and appropriate security controls
- Assessing and identifying third-party risks
- Providing Cloud and security architectures that minimise the attack surface
- Implementing defence in depth with built-in continuous assurance
- Enabling secure change and configuration management

Benefits

- Enhanced SRO ownership of cyber security risk throughout capability lifecycle
- Increased operational capability, reduced operational risk
- Better managed risk-driven outcomes using NCSC assured services
- Reduced security risk to Cloud services architectures and designs
- Proportionate and pragmatic risk reduction and implementation of security controls
- Improved risk visibility throughout the project lifecycle
- Alignment of Digital and Data with people (Human Factors)
- Reduced capability costs due to evidence-led analysis of security controls
- Reduced security risk throughout the entire ICT lifecycle
- Increased confidence that projects will deliver successful outcomes

Service Characteristics

Security

C3IA will handle, use, and store consumer service data appropriate to the information security risk, data classification and service consumer requirements.

C3IA has authorised capability to work up to MoD Tier 2 within our FSC environment which is managed and controlled in line with MoD and HMG (NPSA) FSC requirements.

Storage of classified information hard copy is in the approved FSC secure enclave, with MoD assessed and certified security processes, facilities and infrastructure. All Secure storage cabinets are NPSA approved with the appropriate locking mechanisms.

When required, classified data is moved through approved courier channels Royal Mail Registered and Tracked Post or, if necessary, via physical escort (2-person rule). Destruction of classified information is in line with HMG guidance (HMG IAS5) subject to the type of Media being destroyed.

In addition to technical security controls 'The Need to Know' caveat is regularly enforced through internal briefing sessions, poster campaigns, regular user training and awareness programmes as well as ensuring updates are promulgated to all staff regarding NPSA and NCSC threat updates and alerts.

Security Incidents are reported immediately in line with the C3IA Security Incident Management Procedure and clients notified as necessary.

On-boarding / Off-boarding processes

Delivery of G-Cloud services will include On-Boarding and Off-Boarding events. All new customers are assigned a dedicated delivery manager overseen by an NCSC Head Consultant.

The On-Boarding meeting will ensure that the scope of the cloud support service is understood and agreed by both parties. The output of this activity is a clear agreement and understanding of:

- The services to be provided (in the form of service provision and project management plans).
- The methodology and resources by which the services will be provided (including specific Technical Requirements).
- The business outcome of the service provision plan.
- How performance will be evaluated, and outcomes accepted.
- All assumptions, dependencies and deliverables are clearly defined.

The Off-Boarding meeting will analyse delivery against the agreed scope of work and deliverables to assess whether the service engagement has achieved its objectives and that the service consumer is satisfied with the work undertaken. The output of this activity is:

- A service consumer agreement that all deliverables have been completed satisfactorily in their entirety through Legal and Contractual acceptance.
- Evaluation of the contract delivery to identify any Lessons Learned and/or inform continual improvement activity.
- Identification and implementation of any enduring requirements i.e. Confidentiality (Security Aspects Letter), Availability for clarification and/or questions related to the service delivered.

Pricing

Pricing is as defined within the G-Cloud Pricing Document and SFIA Rate Card.

Service Management

C3IA's Service Management system, its Processes and Procedures have been developed to meet the requirements of its customers, informed by best practice and lessons learned. Their maturity and content are externally audited to ensure compliance with both ISO9001 and ISO27001 for which C3IA holds UKAS accredited certification.

C3IA delivers its consulting offering aligned to the NCSC approach to consultancy services and delivery (mandated under the NCSC Assured Consultancy Scheme (ISO 20700)). This approach implements measures to ensure that service delivery meets the highest technical and quality standards through defined Service Offering, Delivery and Service closure and feedback project steps.

Service Constraints

There are no service constraints associated with this service.

Service Levels

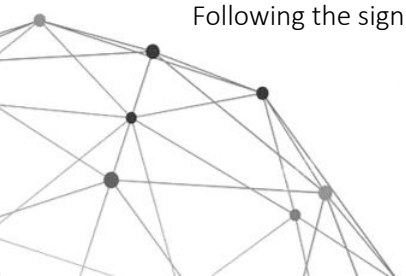
Service levels are defined and agreed with the service consumer during the On-Boarding process. During delivery service levels will be regularly reviewed per the Service Delivery and Project Management Plans to ensure progress is maintained as expected and agreed under the contract. Where Milestones have been set customer approval is sought, using a Certificate of Acceptance, to confirm satisfaction with progress and will require approval against deliverables. Should an issue be identified C3IA has defined procedures within its Quality Management System to take corrective action.

Training

Training is not provided with this service.

Ordering & Invoicing

Following the signing of the Call-Off Contract Order Form, C3IA requires a purchase



order to be raised and received 10 working days before the first invoice date to allow time to process through the system and raise any invoices due.

As per the Call-Off Contract Order Form, payment of invoices shall be made within 30 days from receipt of invoice. Payment shall be made by BACS.

Termination Terms

Termination shall be in line with the G-Cloud Call-Off Contract Order Form and per clause 18 of the Call-Off Contract.

Data Restoration Terms

This does not apply to this service.

Consumer Responsibilities

Service consumer responsibilities will vary by the specific nature of the engagement, but C3IA will typically require:

- Access to information from the service consumer
- Access to Stakeholders and relevant SMEs
- Access to work sites/office locations

Technical Requirements

Technical Requirements will be specific to the individual service consumer's requirement. As such, they will be defined by the consumer within the Call-Off Order form and/or defined within the scope of work definition during the On-boarding process.

Data Extraction / Removal

C3IA cloud support services will usually result in the delivery of documentary reports and products. All artefacts will be issued in non-repudiated document formats, although copies of any testing results and/or tools' output can be provided in an editable form to enable service consumer use.

C3IA will retain a copy of the report in a secure format for 6 years, however, all other data will be securely deleted from any computers, storage devices and storage media once the service delivery has been completed. Dependent upon the information classification and service consumer requirements, secure deletion of all storage media can be carried out using Blancco Drive Eraser and Certificates of Erasure will be available if requested in advance. C3IA may require the service consumer to pay additional deletion costs if Blancco use/Certificates of Erasure are requested.

Data Storage & Processing

C3IA cloud support services will usually result in the delivery of documentary reports and products. The data collected to produce these artefacts will be processed as follows:

- Data at UNCLAS/OFFICIAL level will usually be processed with the C3IA Microsoft 365 Tenancy where all service consumer data is stored within SharePoint and OneDrive within Azure Data Centres in the UK.
- Data at OFFICIAL SENSITIVE level is processed on our segmented DCPP High compliant information systems.

Customer contact data (Names, email addresses and telephone numbers) may be held within our CRM. This data may be stored outside of the UK (i.e. EEA/US) but only in locations that have data protection agreements providing UK equivalence for data protection.

C3IA has a Data Protection Officer, who is appropriately trained and supported by other data protection practitioners to ensure compliance with GDPR and DPA 2018.

About Us

Our Company

C3IA is a defence, security, law enforcement and counter terrorism consultancy who provide specialist technical and cyber security services to the public and private sectors. A UK Government critical defence supplier, we are well recognised for our record of high quality, collaborative delivery in the UK MOD, wider UK government and public sector, and the finance and energy sectors. Our trusted and experienced team carry the highest security clearances, skills and qualifications, and provide expertise in capability acquisition, ICT systems engineering and NCSC-assured cyber security. We have Facility Security Clearance status to MOD Tier 2 and can therefore manage classified material to deliver secure and high assurance support.

Why Us?

C3IA was one of the first companies to be awarded National Cyber Security Centre (NCSC) 'Assured Cyber Security Consultancy' status after extensive assessments of our consultants and experience. Our staff hold a variety of qualifications and certifications that include the National Cyber Security Centre's Certified Professional (CCP) and the UK Cyber Security Council's Chartered Cyber Security Professional status. All our staff hold UK government security clearances and are experienced professionals ready to support you.

Security Assured

As a cyber security consultancy, C3IA takes its own security very seriously. We hold ISO 27001 accreditation, as well as certifications for Cyber Essentials, Cyber Essentials Plus and IASME Gold. We also hold ISO 9001 accreditation for quality management.

Providing Service

Throughout the contract, we will do our utmost to ensure you are totally satisfied with the service you receive. We will always take feedback in a constructive manner and look to continually improve our service to you as we aim to build a great relationship that is lasting and rewarding. If any concerns arise, we have an established escalation pathway to the NCSC Named Head Consultant in the Company, the Security Director, for resolution. We look forward to working with you.