CODA
Bespoke Cyber Security

General Consultancy Services

SERVICE DEFINITION DOCUMENT

Prepared for:	Crown Commercial Services
In relation to:	G-Cloud 14 Lot 3 Cloud Support Services

CONTENTS

1. PREFACE

This document provides an overview of the service offerings provided by CODA Security through the G-Cloud 14 framework, as part of Lot 3 - Cloud Support.

More information on the services is available from our website at the following URL:

https://www.codasecurity.co.uk.

2. SERVICE DELIVERY

2.1. Introduction

CODA provide bespoke services to our clients that are tailored to their particular requirements. We do not offer a "commodity off-the-shelf service", and all service delivery teams are fully trained, qualified, and equipped to fulfil their assigned tasks.

As such, all engagements require a degree of preparation, including establishing the scope of work, any timelines or classification considerations, and key points of contact on both sides.

2.2. Preparation

CODA perform all remote testing of any infrastructure from our EU and UK datacentre-hosted systems and appliances. The public IP addresses related to these will be supplied in advance of testing beginning, and these should be whitelisted on any intrusion detection or prevention systems. It is not normally required for these to be whitelisted on firewall devices, however, suspicious events identified with these source IP address can typically be ignored. While CODA will take all reasonable precautions and are well-versed and experienced in testing against production environments, it is recommended that full backups of any systems in scope of the assessment are taken prior to testing beginning.

2.3. Nominated Point of Contact

Throughout any engagement, a client point of contact will be required to be nominated in case of technical difficulties that impede assessment, or significant findings that may require rapid remediation. This point of contact should be aware of the engagement and have sufficient decision-making authority and technical understanding to support it. CODA will also nominate a primary technical point of contact, typically the lead tester, who will liaise with the client point of contact throughout the assessment, including during any post-report discussion.

2.4. Limitations on Testing

Please note that CODA do not routinely perform denial of service testing or brute-force password guessing, unless specifically requested as part of the scoping process. This is to minimise the potential operational impact on our client’s systems, and to ensure that, wherever possible, loss of service availability as a result of the assessment process is avoided.

2.5. Requirements and Dependencies

Wherever possible, CODA will seek to reduce the operational impact of any assessment activity. This means that key requirements and dependencies will be identified and drawn-out in the initial scope-of-work, wherever this can be practically achieved.

In some cases, additional information may become apparent during the assessment that means additional requirements are identified, and so it is important that a technical contact is available throughout the assessment.

2.6. Reporting

All engagements include knowledge transfer, which in most cases means the production of a detailed technical report, including:

- An executive summary with tailored risk management guidance; and
- Detailed technical breakdown including evidence and remediation advice where appropriate.

Additionally, CODA will provide up to one hour of post-report follow-up discussion to ensure key findings are adequately transferred.

3. FRAMEWORKS AND STANDARDS

CODA complies with its responsibilities under the applicable legal frameworks, as well as operating, as far as is practical, within any information security management frameworks and governance structures that may apply to the scope of any assessment activity.

The relevant legislation and standards that typically apply are listed below; more details of CODA's compliance with these can be supplied upon request and are also provided in any published scopes of work.

- Data Protection Act 2018 and GDPR
- Computer Misuse Act 1990
- Human Rights Act 1998
- Official Secrets Act 1989
- Freedom of Information Act 2000
- Payment Card Industry Data Security Standard
- Copyright and Intellectual Property Rights
- NCSC CHECK