CODA
Bespoke Cyber Security

Service Definitions
REFERENCE DOCUMENT

Prepared for:	Crown Commercial Services
In relation to:	G-Cloud 15 Lot 3 - Cloud Support Services
Date issued:	06/11/2025

CONTENTS

1. INTRODUCTION

This document provides an overview of the service offerings provided by CODA Security through the G-Cloud 15 framework, as part of Lot 3 - Cloud Support.

More information on our 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.

3. COMMON SERVICE ELEMENTS

The following activities are performed across all service particulars, with specific tailoring according to the applicable threat models simulated.

3.1. Full Port and Service Detection Scanning

Utilising automated scanning tools which are freely available to potential attackers, CODA attempt to discover and identify any services exposed by the system(s) hosting the services above.

3.2. Automated Vulnerability Scanning

All services and systems include automated scanning for technical vulnerabilities where appropriate, using industry standard tools and approaches typically taken by attackers. The output of this is analysed and verified as far as practical, in order to minimise the potential for false positives.

3.3. Manual Service Inspection and Exploitation

Any services identified are manually inspected for exploitable vulnerabilities, or for unnecessary leakage of system information. Where exploitation is likely, manual attempts to verify the nature of the vulnerability are made, provided that the integrity or availability of the target systems is not likely to be impacted and that exploitation is included within the scope of testing.

3.4. Report Writing and Knowledge Transfer

All findings are reported in sufficient detail to permit full technical knowledge transfer, proof-of-concept replication, vulnerability remediation, and incorporation into internal risk management processes. Generally, a final report will be issued which consists of three sections:

- The scope of testing, and any applicable limitations.
- An executive summary with tailored risk management guidance and strategic recommendations.
- A detailed technical breakdown, explaining and demonstrating any vulnerabilities identified, with remediation advice and technical evidence where appropriate.
- Remediation Action Plan (RAP) appendix for internal assignment and tracking of remediation activities

The reports are entirely written by CODA consultants. Generative AI tools such are large language models (LLMs) are not used at any point in the reporting process.

Additionally, CODA provides post-report follow-up discussions and workshops to ensure key findings are adequately transferred. These can be held at any UK, Five Eyes, or NATO classification, subject to suitable communications and facilities being available.

Alternatively, if preferred, CODA can report directly into internal issue tracking systems such as Jira or Gitlab, enabling rapid triage of assessment findings.

APPENDICES

Appendix A - About CODA Security Limited

CODA Security Limited ("CODA") currently holds the following company accreditations. These are intended to reflect our dedication to professional delivery and quality of service. Please note that this is not an exhaustive list.

CODA are an Assured Service Provider under the National Cyber Security Centre's (NCSC) CHECK scheme.

This demonstrates that our penetration testing methodology has been approved by the NCSC as being suitable for delivering penetration testing and vulnerability assessment services to central and local departments of His Majesty's Government.

CODA are a silver sponsor of The Cyber Scheme.

This demonstrates our commitment to improving certifications standards in the field of technical assurance and penetration testing across Government systems within the UK.

CODA are certified against ISO 27001:2013, the international standard for Information Security Management Systems.

This demonstrates our commitment to the security of any data we process for our customers, and the maturity of our internal information security knowledge and experience.

CODA are certified against ISO 9001:2015, the international standard for Quality Management Systems.

This demonstrates our commitment to the delivery of high quality services, and continual improvement.

CODA are an approved Crown Commercial Services (CCS) supplier.

This demonstrates that our services and business processes have been approved by CCS as being suitable for delivering specialist bespoke Cyber Security services to His Majesty's Government.

CODA are certified against Cyber Essentials Plus under the National Cyber Security Centre's (NCSC) Scheme.

This demonstrates that our internal information security policies and procedures exceed with those required to deliver services to His Majesty's Government.

CODA are a Gold Award signatory of the Armed Forces Covenant.

This demonstrates our ongoing commitment to support those who serve, and have served, in His Majesty's armed forces, and their families.

CODA are a registered supplier on the JOSCAR framework.

This demonstrates that our capabilities have been assessed as suitable for buyers operating in the defence, critical national infrastructure, and national security sectors.

CODA have supported the work of the UKCSC since inception, with several of our consultants holding Chartered level professional registration.

This demonstrates our desire to support and influence the future of cyber security as a discipline.

Individual Certifications

In addition to the above company accreditations, our consultants hold certifications from multiple professional and industry bodies. Examples include the following:

Appendix B - Applicable Legislation 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. Note that this is not an exhaustive list.

- Computer Misuse Act 1990
- Copyright and Intellectual Property Rights
- Data Protection Act 2018 and both UK and EU GDPR implementations.
- Freedom of Information Act 2000
- Human Rights Act 1998
- National Security Act 2023
- NCSC CHECK Standard
- Official Secrets Act 1989
- Payment Card Industry Data Security Standard
- Privacy and Electronic Communications (EC Directive) Regulations 2003

We use best practice cryptography wherever supported and enforce strict data-at-rest protection for all internal and client data we hold and process.

All CODA staff are subject to high-level pre-employment checks, including Enhanced Disclosure and Barring Service (eDBS) assessments, and appropriate levels of vetting.

Appendix C - Leadership Team

All services delivered by our consultants are overseen by a senior leadership team consisting of the Directors and Principal Consultant staff.

All members of the senior leadership have many years of individual experience delivering cyber security services such as penetration testing and IT Health Check assessments across Government, Defence, National Security, Academia, and the Private Sector.

They all hold CISSP and Chartered Cyber Security Professional (ChCSP) certifications, as well as providing representation on multiple industry and professional standards boards, and technical guidance to organisations such as the UK Cyber Security Council (UKCSC).

Appendix D - Corporate and Social Responsibility

CODA have a robust internal ethical policy, and all staff sign up to various codes of conduct appropriate to their roles. This includes active support to those staff members with disabilities or complex personal life situations, and reduction in our overall environmental footprint.

CODA actively recruit new staff members at the start of their cyber security career, particularly those transitioning from fields such as the Armed Forces - with whom we maintain strong cultural links. These staff are supported through their professional development with targeted training and support, which includes generous leave allowances and flexible working.