CAMBRIDGE CYBER ADVISERS

Penetration Testing Service

Service Definition Document. Version 1.0

19 January 2026

Penetration Testing Service

1. Introduction

This Service Definition Document describes the **Penetration Testing** service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides a controlled, intelligence-led assessment of an organisation's security defences by safely simulating real-world cyber-attacks across networks, applications, cloud environments, and human factors.

Modern organisations face increasingly sophisticated adversaries who exploit vulnerabilities in systems, configurations, and user behaviour. This service provides an independent, evidence-based evaluation of an organisation's susceptibility to compromise, identifying exploitable weaknesses and demonstrating the potential business impact of successful attacks.

Using a combination of manual testing, automated tooling, threat-informed techniques, and alignment to recognised methodologies such as OWASP, NCSC CHECK principles, and CREST standards, the assessment delivers a clear, actionable understanding of security weaknesses and the steps required to reduce risk.

2. Service Overview

The Penetration Testing service provides a structured, end-to-end evaluation of an organisation's technical security posture. The assessment simulates attacker behaviour to identify vulnerabilities, misconfigurations, and weaknesses that could be exploited to gain unauthorised access, disrupt operations, or compromise sensitive data.

The service covers internal and external networks, web applications, APIs, cloud platforms, mobile applications, wireless networks, and social engineering vectors. Testing is conducted by experienced ethical hackers using industry-standard methodologies and threat-aligned techniques.

Activities include:

- Vulnerability identification and exploitation
- Manual and automated testing of applications, networks, and cloud services
- Review of authentication, authorisation, and session management controls
- Assessment of configuration weaknesses and insecure design patterns
- Privilege escalation and lateral movement testing (where in scope)
- Social engineering and phishing simulations (optional)
- Evidence capture and impact demonstration
- Detailed reporting with remediation guidance
- Executive and technical debrief sessions

Service Features

- Threat-informed penetration testing aligned to OWASP, NCSC, and CREST standards
- Manual exploitation by experienced ethical hackers

- Testing across network, application, cloud, and human attack vectors
- Realistic simulation of attacker tactics, techniques, and procedures
- Clear evidence of vulnerabilities and potential business impact
- Detailed technical reporting with step-by-step findings
- Executive summary with risk-based prioritisation
- Optional retesting to validate remediation
- Optional continuous testing programmes

Service Benefits

- Identifies exploitable vulnerabilities before malicious actors can abuse them
- Demonstrates real-world attack paths and business impact
- Supports compliance with Cyber Essentials Plus, ISO 27001, PCI DSS, and NCSC guidance
- Strengthens resilience across applications, infrastructure, and cloud environments
- Enables informed investment decisions based on risk and exploitability
- Improves security awareness and operational readiness
- Supports continuous improvement and secure development practices

3. Service Scope

The service includes, but is not limited to, penetration testing across:

- External and internal networks
- Web applications and APIs
- Mobile applications
- Cloud platforms (Azure, AWS, GCP)
- Wireless networks
- Social engineering and phishing (optional)
- Configuration and security control evaluation
- Exploitation and impact demonstration

Activities may include vulnerability discovery, exploitation, privilege escalation, lateral movement, and assessment of detection and response capability (where agreed).

4. Delivery Methodology

All CCA engagements follow a phased approach using our standard methodology:

- **Scoping and Planning** – defining targets, constraints, rules of engagement, and testing windows
- **Reconnaissance and Enumeration** – mapping attack surface and identifying potential entry points
- **Vulnerability Analysis** – identifying weaknesses through manual and automated techniques
- **Exploitation** – safely exploiting vulnerabilities to demonstrate impact

- **Post-Exploitation** – privilege escalation, persistence, and lateral movement (if in scope)
- **Analysis and Reporting** – documenting findings, evidence, and remediation guidance
- **Executive and Technical Debrief** – walkthrough of results and recommended next steps

5. Deliverables

- Executive Summary Report
- Technical Findings Report
- Vulnerability and Exploit Evidence Pack
- Risk Register and Impact Analysis
- Prioritised Remediation Roadmap
- Optional Retest Report
- Optional Advisory and Remediation Support Outputs

6. Service Levels

- Engagement commences within 10 working days of contract award
- Draft report within 10 working days of testing completion
- Final report within 15 working days
- Weekly progress updates for longer engagements
- Critical vulnerabilities disclosed immediately upon discovery

7. Governance and Assurance

Activities align with OWASP Testing Guide, NCSC CHECK principles, CREST methodologies, and ISO 27001 governance practices. Where required, engagements will be managed by a CCA Project Manager.

Backup and Restore

Not applicable.

Reporting & Analytics

Outputs include findings report, risk register, impact assessment, executive summary, remediation roadmap, and optional evidence pack.

Incident Management

The service identifies vulnerabilities but does not manage customer incidents.

Disaster Recovery

Not applicable.

Availability

CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time.

8. Security and Data Protection

- Confidential handling of customer data
- UK-based testing team
- Secure environments for data processing
- Data retained for 30 days then destroyed
- GDPR, NCSC, and ISO 27001-aligned practices

GDPR & Data Privacy

- Personal data minimisation
- DPIA support available
- Findings anonymised unless requested otherwise

Accreditations

- ISO 27001-aligned practices
- NCSC-aligned methodologies
- CREST-aligned penetration testing approaches

Staff Security Clearance

SC-cleared staff available upon request; BPSS as a minimum for all CCA consultants.

9. Customer Responsibilities

Customers must provide scoping information, documentation, access to systems, and support for testing windows.

Technical Requirements

- Scoping information
- Access to target systems
- Contact details for key personnel

Supported Browsers/Devices

Not applicable.

Access Restrictions

Customer must designate authorised individuals for scope approval, change requests, and receipt of outputs.

10. Service Constraints

Activities limited to agreed scope and timeframes; some may require controlled testing windows to avoid operational impact.

11. Pricing

Pricing is engagement-based and determined by scope, duration, and complexity. Pricing is based on:

- Number and type of targets (applications, networks, cloud assets)
- Complexity of environments
- Required depth of testing
- Duration of engagement
- Optional social engineering or red-team-style activities

Typical engagements range from 1–6 weeks.
Day-rate pricing is available on the pricing document and compliant with G-Cloud pricing rules.

Ordering and Invoicing Process

Ordering is typically completed via Purchase Order following confirmation of service. CCA invoices monthly, providing a detailed breakdown of services delivered, including VAT/expenses. Consolidated invoices available. Invoices may be issued electronically or via post.

12. Exit and Offboarding

- Findings delivered
- Knowledge transfer completed
- Data destroyed within 30 days (certificate available)

Onboarding

- Requirements workshop
- Scope definition
- Stakeholder identification
- Rules of engagement confirmation

Offboarding

- Walkthrough of findings
- Delivery of reports
- Optional remediation workshop
- Secure data destruction

Training Provided

- Awareness session
- Secure development briefing
- Optional phishing or social engineering training

13. Termination

- Standard G-Cloud termination terms apply
- Customer may terminate with notice; work completed to date will be invoiced
- Provider may terminate only under defined exceptions (e.g., breach of Rules of Engagement or safety concerns)

14. Contact and Support

A delivery manager is assigned for each engagement. Support is available via email and phone during delivery hours.

Included as standard:

- Email and phone support during the engagement
- Delivery manager assigned
- Access to reporting team for clarifications

Enhanced support packages available for continuous testing programmes.