CAMBRIDGE
CYBER ADVISERS

Vulnerability Management

Service Definition Document. Version 1.0

30 January 2026

Vulnerability Management

1. Introduction

This Service Definition Document describes the Vulnerability Management service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides continuous, intelligence-informed identification, assessment, prioritisation, and tracking of vulnerabilities across cloud and on-premise environments.

Modern organisations operate in complex hybrid infrastructures where new vulnerabilities emerge daily. Effective vulnerability management requires more than periodic scanning—it demands continuous visibility, rapid triage, and coordinated remediation. CCA's Vulnerability Management service delivers structured, repeatable, and proactive oversight of security weaknesses across infrastructure, applications, and cloud platforms.

Using industry-leading tooling, expert analysis, and a proven methodology, CCA ensures that vulnerabilities are identified quickly, assessed accurately, and remediated efficiently. The service supports compliance with regulatory frameworks and strengthens organisational resilience by reducing exposure to cyber risk.

2. Service Overview

CCA's Vulnerability Management service provides scheduled and ad-hoc scanning, vulnerability assessment, prioritisation, and remediation support across on-premise, Azure, AWS, and GCP environments. The service delivers continuous visibility of security weaknesses and ensures rapid notification of critical and zero-day vulnerabilities.

Activities include:

- Scheduled daily, weekly, monthly, or ad-hoc vulnerability scans
- Hardware and software vulnerability assessments
- Compliance scanning aligned to frameworks such as PCI-DSS
- Web application scanning
- Identification and prioritisation of critical and zero-day vulnerabilities
- Customisable dashboards for technical and non-technical stakeholders
- Automated and bespoke reporting
- Collaboration with resolver teams and suppliers to drive remediation

The service is conducted using formally agreed Rules of Engagement and ensures safe, controlled, compliant execution throughout.

Service Features

- Scheduled and ad-hoc vulnerability scanning
- Infrastructure, application, and cloud vulnerability assessments
- Compliance scanning (e.g., PCI-DSS)
- Web application vulnerability scanning
- Zero-day and critical vulnerability identification
- Customisable dashboards
- Automated and bespoke reporting
- Integration with resolver teams
- CREST-aligned testing practices
- Optional continuous monitoring uplift

Service Benefits

- Improved visibility of vulnerabilities across hybrid environments
- Faster remediation through immediate notification of critical issues
- Enhanced governance and compliance posture
- Reduced operational overhead
- Evidence-based prioritisation of remediation
- Increased stakeholder confidence
- Cost efficiencies through streamlined workflows
- Strengthened overall security posture

3. Service Scope

The service includes vulnerability scanning, assessment, prioritisation, reporting, and remediation support across cloud and on-premise environments. Activities may include infrastructure scanning, cloud platform scanning, web application scanning, compliance-aligned assessments, vulnerability triage, and remediation guidance.

4. Delivery Methodology

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

- Scoping and Requirements Definition
- Discovery and Configuration
- Vulnerability Scanning and Assessment
- Analysis and Prioritisation
- Reporting and Remediation Support
- Review and Continuous Improvement

5. Deliverables

As part of the CCA Cyber Red Teaming & Adversary Simulation service, the following standard deliverables are provided:

- Executive Summary Report
- Technical Vulnerability Findings Report
- Prioritised Remediation Roadmap
- Compliance Scan Outputs (e.g., PCI-DSS)
- Web Application Vulnerability Report
- Custom dashboards
- Optional continuous monitoring outputs

Additional deliverables can be agreed depending on requirements.

6. Service Levels

The standard CCA delivery SLAs are:

- Service onboarding within 10 working days of contract award
- Critical vulnerability notifications issued immediately
- Monthly or weekly reporting (as scoped)
- Quarterly service review meetings

Optional enhanced SLAs are available for accelerated engagements or continuous testing.

7. Governance and Assurance

All testing is conducted under agreed Rules of Engagement. Activities comply with legal, ethical, and safety requirements, and align with CREST and NCSC best practices.

Backup and Restore

Not applicable — this service does not handle customer production data or operate within customer systems in a way that requires backup/restore functionality.

Reporting & Analytics

Outputs include:

- Full vulnerability register
- Severity analysis
- Compliance mapping
- Trend analysis

- Executive summaries
- Remediation guidance

Incident Management

Controlled escalation paths defined in Rules of Engagement

- Clear escalation paths
- Immediate notification of critical vulnerabilities
- Recommendations for incident response

Disaster Recovery

Not applicable — service is not hosted and does not rely on persistent operational infrastructure.

Availability

Service availability applies only to consultant scheduling. CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time with out-of-hours engagements available on request.

8. Security and Data Protection

Customer data is handled confidentially and securely. Data is retained only for the duration necessary to deliver the service and securely destroyed within 30 days of engagement completion. GDPR principles are applied throughout.

- All customer data handled under strict confidentiality
- UK-based testing team available
- Data stored and processed in secure environments
- Data retained for 30 days post-engagement then securely destroyed
- Compliance with GDPR, NCSC guidance, and ISO 27001-aligned practices
- No customer data transferred outside approved jurisdictions

GDPR & Data Privacy

- Personal data used only where strictly required (e.g., targeted phishing scenarios)
- Data minimisation applied
- DPIA support available where necessary
- All findings anonymised unless otherwise requested by customer

Accreditations

- CREST-aligned
- ISO 27001-aligned internal management practices
- Cyber Essentials-aligned

Staff Security Clearance

SC cleared staff available on request. Baseline Personnel Security Standard (BPSS) checks conducted for all consultants.

9. Customer Responsibilities

Customers are responsible for providing accurate scoping information, nominating escalation contacts, supporting internal approvals, and implementing remediation actions.

Technical Requirements

- Provide accurate asset information
- Enable scanning access
- Support approvals
- Implement remediation actions

No agent installation is required unless explicitly scoped.

Supported Browsers/Devices

Not applicable — this is a consultancy service, not a hosted software product.

Access Restrictions

Customer must designate authorised individuals for:

- Scope approval
- Rules of Engagement
- Emergency halt
- Receipt of confidential outputs

10. Service Constraints

Testing activities are limited to agreed scope and timeframes. Physical testing requires prior authorisation. Change freezes or restricted windows may apply.

- Activities limited to agreed scope and timeframe
- Scanning windows may require coordination with change freezes
- Cloud scanning may require permissions
- Web application scanning requires authorisation
- All activities must comply with legal and ethical constraints

11. Pricing

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

- Scope, frequency, and environment complexity
- Number of assets
- Scanning frequency
- Compliance requirements
- Web application scanning volume
- Optional continuous monitoring

Typical engagements range from 4-12 weeks.

Day-rate pricing is available on the pricing document and compliant with G-Cloud pricing rules.

Ordering and Invoicing Process

Ordering from clients is generally done via the presentation of a Purchase Order following confirmation of the purchase of a service. CCA will invoice at the end of every calendar month, giving a precise breakdown of the services purchased, including VAT/other expenses. CCA can provide consolidated invoices if required. Invoices can be issued electronically or via post.

12. Exit and Offboarding

At engagement end, all findings are delivered, knowledge transfer sessions completed, and customer data securely destroyed. Certificates of destruction can be provided.

Onboarding:

- Requirements workshop
- Definition of scope, assets, and schedules
- Dashboard configuration
- Validation of communication protocols and escalation points

Offboarding:

- Full walkthrough of all findings
- Delivery of report, evidence and artefacts
- Remediation workshop (optional)
- Secure data destruction within 30 days post-engagement (certificate provided)

Training Provided

- Awareness session
- Dashboard walkthrough
- Resolver team workshops

- Compliance briefings

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.