CAMBRIDGE
CYBER ADVISERS

Zero Trust Advisory

Service Definition Document. Version 1.0

19 January 2026

Zero Trust Architecture & Implementation Advisory

1. Introduction

This Service Definition Document describes the Zero Trust Architecture & Implementation Advisory service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides a structured, comprehensive approach to designing, assessing, and implementing Zero Trust principles across an organisation's digital estate.

Modern organisations operate in a boundaryless environment where identity, devices, applications, and data are distributed across cloud and on-premise platforms. Traditional perimeter-based security models are no longer sufficient to defend against sophisticated adversaries, insider threats, and supply-chain compromise. Zero Trust provides a modern security paradigm built on continuous verification, least-privilege access, and strong policy enforcement.

CCA's Zero Trust service delivers an independent, expert-led assessment of an organisation's current state, a tailored Zero Trust strategy, and a practical roadmap for implementation. Using recognised frameworks such as NIST SP 800-207 and NCSC Zero Trust principles, the service helps organisations adopt a secure-by-design model that reduces risk, strengthens resilience, and enables secure digital transformation.

2. Service Overview

The Zero Trust Architecture & Implementation Advisory service provides a holistic review of an organisation's identity, access, device, network, application, and data security controls. It evaluates the maturity of existing capabilities and defines a structured path toward a fully integrated Zero Trust model.

This service delivers an end-to-end assessment and design engagement covering governance, architecture, technology, and operational processes. It identifies gaps, risks, and opportunities for improvement across all major Zero Trust pillars, including identity, endpoints, networks, applications, data, and monitoring.

Activities include:

- Review of current security architecture and operating model
- Assessment of identity, access, and authentication controls
- Evaluation of device and endpoint trust signals
- Analysis of network segmentation and access pathways
- Review of application access, API security, and workload protections
- Data classification, protection, and access governance review
- Mapping of current state to NIST 800-207 and NCSC Zero Trust principles
- Development of a tailored Zero Trust strategy and implementation roadmap
- Executive and technical debrief sessions

Service Features

- Comprehensive assessment across all Zero Trust pillars
- Alignment to NIST 800-207, NCSC Zero Trust, and industry best practice
- Identity and access management (IAM) maturity evaluation
- Endpoint trust, compliance, and device-health assessment
- Network segmentation and micro-segmentation review
- Application and workload access analysis
- Data protection and governance evaluation
- Monitoring, analytics, and continuous-verification capability review
- Detailed strategy, architecture blueprint, and implementation roadmap
- Optional hands-on advisory and implementation support

Service Benefits

- Provides a clear, evidence-based view of Zero Trust readiness
- Reduces risk by identifying weaknesses in identity, access, and segmentation
- Supports compliance with NCSC guidance, Cyber Essentials Plus, and ISO 27001
- Enables secure cloud adoption and digital transformation
- Strengthens governance, operational capability, and architectural resilience
- Improves alignment between security and business objectives
- Enables informed investment decisions based on risk and maturity
- Supports continuous improvement and long-term Zero Trust adoption

3. Service Scope

The service includes, but is not limited to, Zero Trust strategy development, architectural assessment, technical evaluation, and maturity scoring. Activities may include IAM review, device trust assessment, network segmentation analysis, application access evaluation, data governance review, and monitoring capability assessment.

4. Delivery Methodology

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

- Scoping and Planning
- Documentation Review and Stakeholder Interviews
- Technical and Process Assessment
- Zero Trust Strategy and Architecture Development
- Analysis and Reporting
- Executive and Technical Debrief

5. Deliverables

- Executive Summary Report
- Technical Findings Report
- Zero Trust Maturity Assessment
- Risk Register and Impact Analysis
- Zero Trust Strategy and Architecture Blueprint
- Prioritised Implementation Roadmap
- Optional Advisory and Implementation Support Outputs

6. Service Levels

- Engagement commences within 10 working days of contract award
- Draft report within 10 working days of assessment completion
- Final report within 15 working days
- Weekly progress updates for longer engagements

7. Governance and Assurance

Activities align with NCSC Zero Trust principles, ISO 27001, and NIST SP 800-207. Where required, engagements will be managed by a CCA Project Manager.

Backup and Restore

Not applicable.

Reporting & Analytics

Outputs include findings report, maturity scoring, risk register, impact assessment, executive summary, Zero Trust strategy, architecture blueprint, and implementation roadmap.

Incident Management

The service evaluates incident response and monitoring capability 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 assessment 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

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, stakeholder access, and support for implementation planning.

Technical Requirements

- Scoping information
- Documentation access
- Contact details for key personnel

Supported Browsers/Devices

Not applicable.

Access Restrictions

Customer must designate authorised individuals for scope approval, change requests, access to customer systems and/or services, and receipt of outputs.

10. Service Constraints

Activities are limited to agreed scope and timeframes; some may require controlled windows.

11. Pricing

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

- Number of Zero Trust pillars in scope
- Complexity of environments
- Duration of engagement
- Required depth of architectural design

Typical engagements range from 2–8 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 purchase. CCA will invoice at the end of every calendar month, providing a breakdown of services purchased, including VAT/expenses. Consolidated invoices available on request. Invoices can 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
- Communication validation

Offboarding

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

Training Provided

- Zero Trust awareness session
- Identity and access security briefing
- Optional tabletop exercises

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 Zero Trust transformation programmes.