**360 DEFENCE (UK) LTD – SERVICE DEFINITION**

**E1. CAF-RA: NCSC CAF & GovAssure Readiness & Assurance**

| | |
|---|---|
| **Service attributes** | |
| Service type | Lot 3: Cloud Support |
| **Service name** | |
| Service name | E1. CAF-RA: NCSC CAF & GovAssure Assurance Support |
| **About 360D Service**<br><br>360 Defence (UK) Limited (360D) delivers defence grounded in threat-informed, attacker-shaped understanding of cyber, security and risk. We are specialists in adversary-centric analysis, decision-grade risk clarity and assurance-aligned outcomes, built on the principle that context, definitions and situational understanding are essential to defensible security.<br><br>360D applies defender-led, attacker-informed thinking to assurance so outcomes stand up to real threats, not paperwork. | |
| Service description | **You are a target.**<br><br>360D delivers defender led, attacker informed GovAssure and NCSC CAF readiness grounded in experience supporting departmental and ALB submissions. We build assessor grade evidence, calibrate claims to credible maturity, and align CAF outcomes to attacker behaviours, reducing friction across Stages 2–4 and accelerating defensible improvement planning. |

| | |
|---|---|
| What this service does (Clarity statement) | This service **does not** perform a formal GovAssure Stage 4 Independent assessment or act as an independent assessor.<br><br>It **does**:<br><br>• prepare organisations for GovAssure and WebCAF submissions,<br>• strengthen CAF evidence quality and coherence,<br>• reduce assessment friction, rework and escalation risk.<br><br>360D provides **attacker-led GovAssure / NCSC CAF readiness** grounded in **first-hand experience operating inside the GovAssure/CAF delivery environment** and supporting departments and ALBs through Stages 2–4. This is not generic "compliance consulting": it strengthens the evidence narrative, calibrates claims to what assessors recognise as credible, and translates real attacker pathways into defensible CAF outcomes and improvement priorities. |
| Service categories | • Cloud Support Services<br>  ○ Security Services<br>  ○ Security Strategy<br>  ○ Security Risk Management<br><br>***This service is delivered under Cloud Support and does not include hosted platforms or managed services.*** |
| **Service features and benefits** | |

| | |
|---|---|
| Features | • Attacker-led CAF readiness aligned to assessor expectations<br>• Stage 2 scoping and CAF profile selection support<br>• Stage 3 self-assessment strengthening and claim calibration<br>• Assessor-grade evidence pack structuring and readability<br>• Outcome and IGP mapping with evidence traceability<br>• Identify weak evidence and likely assessor challenge<br>• Translate attacker pathways into defensible CAF narratives<br>• Senior practitioner-led delivery informed by deep GovAssure and CAF practice.<br>• Prioritise improvements aligned to Stage 5 planning<br>• Optional support for assessor queries and clarifications |
| Benefits | • Ensures WebCAF and GovAssure positions defensible before independent assessment<br>• Makes CAF submissions defensible against real threats<br>• Delivered by practitioners shaping GovAssure and CAF across central government<br>• Aligns assurance outcomes to attacker reality<br>• Reduces assessor challenge and rework risk<br>• Prevents evidence over-claiming that undermines credibility<br>• Converts documentation into usable evidence<br>• Improves confidence before independent assessment<br>• Enables leaders to approve claims confidently<br>• Accelerates targeted improvement planning |
| Service Delivery benefit | • This service helps organisations **enter GovAssure prepared**, with evidence that reflects reality, maturity and intent — not optimism or box-ticking. |

| | |
|---|---|
| | • Moves Organisations from “we think we meet WebCaf” to “we can evidence it credibly“ with claims calibrated to what assessors expect to see, **based on** the WebCAF guidance provided by the Government Security Group (GSG) in support of the Government Cyber Unit, and evidence aligned to how real attackers compromise systems and services.” |
| Service Implementation Planning | • Scoping: stage, services, boundaries, profile, stakeholders<br>• Evidence intake: artefacts, policies, configs, tickets, metrics, logs<br>• Attacker-led validation: confirm realistic compromise pathways<br>• CAF mapping: outcomes/IGPs, claim calibration, strength scoring<br>• Evidence engineering: restructure pack, traceability, readability<br>• Readout: SRO brief + Stage 5-oriented improvement priorities<br>• Delivery is remote by default (e.g. Microsoft Teams); in-person by agreement. |
| **Service scope** | |
| NCSC CAF | This service supports **pre-assessment readiness only**. It aligns to the **current NCSC Cyber Assessment Framework (CAF)** version in use at the time of delivery. For example:<br><br>• **CAF v3.2** applies to GovAssure cycles up to **Spring 2026**<br>• **CAF v4.0** and the updated WebCAF apply from **Autumn 2026** onward<br><br>**It includes:**<br><br>• alignment with the current NCSC CAF version<br>• support for GovAssure Stages 1–4<br>• required advice and guidance for Stage 5 planning |

| | |
|---|---|
| | • preparation for WebCAF submissions<br><br>**It can be extended to:**<br><br>• support mediation where departments and independent assessors disagree on evidence or maturity, providing assessor-aware clarification without acting as an independent assessor<br><br>**It does not:**<br><br>• act as an independent GovAssure assessor<br>• provide certification, audit or regulatory approval<br>• score controls as part of a formal Risk Assessment<br><br>**Outputs are designed to inform:**<br><br>• Threat Assessment (TxA / TxA-E)<br>• Business Impact & Risk Appetite (BIRA)<br>• Threat Modelling (TxM)<br>• Risk Assessment (RxA)<br>• assurance planning and remediation activity |
| Service constraints | This service **does not act as the independent GovAssure assessor**.<br><br>Delivery provides readiness, evidence strengthening, and advisory support aligned to assessor expectations. |

| | |
|---|---|
| Do you hold a suitably scope ISO27001 certificate for this G-Cloud Service. | ISO27001 is not applicable to this service. It is a skills-based service with no hosted platforms, operational systems or data custody. |
| Relevant information surrounding our service in relation to Government Classification Scheme | 360D security specialists include NCSC Lead Certified Cyber Practitioner (and equivalent) professionals with information assurance and cyber security expertise to support the design, development and operation of systems handling information up to **SECRET**, in accordance with applicable HMG policies and client requirements. |
| **Details of the level of backup/restore and disaster recovery that will be provided;** | **This does not apply to this risk management service provision**<br><br>Not applicable (The service involves no hosting, platform operations or data custody.) |
| **On-boarding and Off-boarding processes/scope etc.;** | **On-boarding**<br>Confirmation of scope, GovAssure stage and applicable CAF profile. Agreement on information handling and delivery timelines. Identification of stakeholders required for evidence review and validation |

| | |
|---|---|
| | **Off-boarding**<br>Formal delivery of findings, evidence guidance and improvement recommendations. No client data is retained by 360D. Optional briefing for senior leadership or assurance teams. |
| **Consumer responsibilities:** | Provide access to relevant business owners, contextual information, and senior decision-makers to agree impacts and risk appetite.<br><br>**Details of any trial service available:** Not applicable (this is a skills-based service). |
| **Reselling** | |
| Supplier Type | 360D is not a reseller |
| **User Support** | |
| Email or ticketing support | No |
| Phone support | No<br><br>This service does not include a standing helpdesk or call-out capability. Support relates solely to engagement coordination and delivery of agreed outputs. |

| | |
|---|---|
| Web chat support | No |
| Support levels | *This service does not include a standing user helpdesk; support relates to engagement coordination only.*<br><br>Named service lead responsible for delivery and quality assurance. Single-point coordination for scope clarification, report delivery, and optional briefing. |
| **Financial Recompense** | |
| Financial recompense model for not meeting service levels: | Any recompense for not meeting agreed service levels is defined in the contract and confirmed at call-off. Termination terms are defined in **360 Defence Terms and Conditions**. |
| **Termination terms: By consumers (i.e. consumption); and By the Supplier (removal of the G-Cloud Service):** | See 360 Defence Terms and conditions |
| **Data restoration / service migration** | Not applicable (no data hosting or migration deliverable). |
| **Staff Security** | |
| Staff Security Clearance | Staff screening performed which conforms to BS7858:2019 |
| Government security clearance | Up to Developed Vetting (DV) |
| **Pricing** | |

| | |
|---|---|
| Discount for educational organisations | Yes<br><br>Pricing (including unit prices, volume discounts (if any), data extraction etc.)<br><br>Pricing is based on SFIA-aligned effort and does not include fixed-price deliverables unless explicitly agreed at call-off. |
| **Documents** | |
| Service definition document | This document |
| Terms and Conditions | See 360D terms and conditions separate document |
| Pricing document | Our prices are published in the 360D G-Cloud pricing and SFIA rate card document/matrix. Pricing is based on role and effort. We may offer fee discounts where an individual resource is contracted for engagements exceeding 60 full working days, subject to agreement at call-off. |