360 DEFENCE (UK) LTD – SERVICE DEFINITION

C4. Defender Led, Attacker Informed Risk Assessment & Management (RxA/RxM)
(Methodology-Agnostic)

Service attributes	
Service type	Lot 3: Cloud Support
Service name	
Service name	C4. Defender Led, Attacker Informed Risk Assessment & Management (RxA/RxM) (Methodology-Agnostic)
About 360D Service 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.	
Service description	**You are a target.** 360D's defender-led, attacker-informed risk service works across appropriate qualitative, quantitative and hybrid methods. We show how real adversaries pursue objectives, enabling leaders to prioritise action, align governance and maintain defensible risk decisions without relying on outdated

	frameworks, automated scoring or tool-driven assumptions.

Service categories	• Cloud Support Services
	  ○ Security Services
	  ○ Security Strategy
	  ○ Security Risk Management
	
	This service is delivered under Cloud Support and does not include hosted platforms or managed s ervices.

Service features and benefits	
Features	• Defender-led analysis grounded in real adversary behaviour and intent • Attacker-informed modelling across appropriate qualitative, quantitative and hybrid methods • Structured logic revealing credible pathways to organisational harm • Consistent risk framing across assets, services and programmes • Decision-grade outputs suitable for executives and governance bodies • Analyst-led judgement, not automated scoring or tool dependence • Integration with threat, asset and impact understanding where relevant • Clear articulation of assumptions, constraints and exposure boundaries • Repeatable logic enabling coherent risk comparison across contexts • Modular delivery aligned to organisational maturity and decision needs

Benefits	• Provides defensible risk clarity grounded in real adversary behaviour • Supports confident executive decisions under uncertainty or pressure • Enables proportionate, prioritised investment and action • Avoids fragmented or contradictory risk assessments across teams • Reduces reliance on outdated frameworks or automated scoring • Improves governance alignment and assurance readiness • Strengthens organisational understanding of credible exposure • Maintains coherent risk logic across programmes and services • Prevents false confidence from tool-driven or checklist approaches • Enhances leadership confidence in risk posture and decisions
Service Implementation Planning	Delivery is modular and phased. Planning begins with understanding organisational context, existing risk approaches and decision needs. 360D then sequences appropriate activities such as discovery, modelling and validation based on credible exposure and maturity. This ensures coherent progression without assuming specific methods, legacy frameworks or predefined client practices.
Service scope	
RxA/RxM/MA	RxA/RxM/MA provides defender-led, attacker-informed risk assessment and management across appropriate qualitative, quantitative and hybrid methods. Delivery is modular and phased, beginning with understanding organisational context, existing risk approaches and decision needs. 360D

	sequences appropriate activities based on credible exposure and maturity, ensuring coherent progression without assuming specific methods, legacy frameworks or predefined client practices.
Why this service is needed	Organisations face complex, evolving threats, inconsistent risk practices and pressure to justify decisions. RxA/RxM/MA provides decision-grade clarity grounded in hostile-reality, not automated scoring or outdated frameworks. It enables leaders to prioritise action, align governance and maintain coherent, defensible risk positions across programmes, services and organisational change.
Why this service is different	RxA/RxM/MA is attacker-informed, not threat-report-driven; defender-led, not tool-led; and methodology-agnostic within reason, avoiding legacy frameworks that distort risk. It delivers consistent, auditable logic across assets and services, ensuring risk decisions remain coherent, proportionate and aligned to real adversary behaviour rather than assumptions, checklists or inherited practices.
Service constraints	Dependent on timely provision of contextual and asset information. Requires access to relevant stakeholders for clarification and validation. Progression may be affected by incomplete or outdated risk materials. Activities rely on agreed availability for workshops and reviews. Outputs depend on accuracy of client-supplied information

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;	**Not applicable.** This service involves no hosting, platforms operations or data custody, operational systems or managed services. No backup, restore or disaster recovery capabilities are required or provided.
On-boarding and Off-boarding processes/scope etc.;	**On-boarding** On-boarding establishes context, confirms decision needs and identifies relevant stakeholders. Activities typically include: • Initial scoping discussion to confirm objectives, constraints and intended use of outputs • Agreement of information requirements such as asset, service and contextual materials • Scheduling of discovery and validation sessions with nominated stakeholders

	Off-boarding Off-boarding ensures clarity, handover and closure without ongoing operational commitments: • Review of delivered outputs to confirm alignment with intended decision use • Optional executive or assurance briefings to support governance or programme needs • Confirmation of closure with no retained access, data or system dependencies
Consumer responsibilities:	• Provide relevant asset, service and contextual information • Nominate stakeholders for validation, review and workshops • Confirm intended use of outputs (operational, executive, assurance) • Ensure timely availability for discovery and review sessions • Validate assumptions and clarify organisational constraints
Reselling	
Supplier Type	360D is not a reseller
User Support	

Email or ticketing support	No
Phone support	No 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 helpdesk. Support relates solely to engagement coordination and delivery of agreed outputs.* 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 Pricing (including unit prices, volume discounts (if any), data extraction etc.) 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.

	This service is primarily delivered at SFIA Level 6, reflecting the judgement-led, attacker-informed analysis required. Where engagements involve enterprise-wide scope, Board/CXO decision support or strategic risk posture definition, SFIA Level 7 leadership may be applied.