



360 DEFENCE (UK) LTD – SERVICE DEFINITION

A1. 360D Specialist Cyber Security & Risk Service

(Defender-Led, Attacker-Informed,)

Service attributes	
Service type	Lot 3: Cloud Support
Service name	
Service name	A1. 360D Specialist Cyber Security & Risk Service <i>(Defender-Led , Attacker-Informed)</i>
About 360D Service	
Service description	360D delivers defence grounded in threat-informed, attacker-shaped understanding of cyber, security and risk. We provide 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. Real defence for the real world.



What the 360D Service is	360D provides defender-led, threat and attacker-informed cyber security and risk support for organisations facing routine, complex or uncertain security challenges. 360D does not deliver tools, audits or generic frameworks. We apply structured attacker logic and professional judgement to clarify what matters, what is credible and what decisions remain defensible across all levels of exposure.								
How 360D Specialist Service Family is Structure	The 360D Specialist Cyber Security & Risk Service is organised into four levels: • A-Level – Parent Service: The overarching defender-led, attacker-informed service that defines the full 360D approach. • B-Level – Method (URxM): The integrated risk-governance cycle that connects all components into one coherent structure. • C-Level – Core Services: The foundational attacker-informed components that shape credible risk decisions, including AssetID, BIRA, TxA, TxA-E, TxM, Attack Trees (RiskTree) and RxA/RxM. • E-Level – Enterprise Services: Organisation-wide stabilisation and assurance services, including CAF-RA, Board/CISO and MxM. The table below defines each component and its purpose.								
360D Service Components and Definitions	<table><tr><th>Layer</th><th>360D Service</th><th>Description</th></tr><tr><td>Target definition</td><td>AssetID</td><td>Prioritising defender-led assets shaped by real attacker interest and business impact, forming a defensible foundation for BIRA and all subsequent risk decisions.</td></tr></table>	Layer	360D Service	Description	Target definition	AssetID	Prioritising defender-led assets shaped by real attacker interest and business impact, forming a defensible foundation for BIRA and all subsequent risk decisions.		
Layer	360D Service	Description							
Target definition	AssetID	Prioritising defender-led assets shaped by real attacker interest and business impact, forming a defensible foundation for BIRA and all subsequent risk decisions.							



	Impact & tolerance	BIRA	Impact severity and risk appetite are realistic, decision-grade and aligned to confidentiality, integrity, availability, financial loss and reputational damage.
	Threat reality	TxA / TxA-E	TxA clarifies hostile interest, their capabilities and intent/motivations using attacker-led analysis and PHIA probability language. TxA-E collapses the threat space including mapping shared group (threat) behaviours , enabling proportionate defensive action.
	Attack logic	TxM	Attacker pathways, dependencies and decision points are explicitly understood, grounding risk and control/countermeasures decisions in realistic attack progression rather than abstract scenarios.
	Risk mechanics	Attack (RiskTree) Trees	Risk is modelled as dynamic attackers process, enabling defensible scoring, comparison and prioritisation across assets and services.
	Risk decisions	RxA / RxM	Individual risks are assessed, prioritised and treated using consistent attacker-led logic across the asset/service or whole organisation.



	Risk governance	URxM	URxM provides a coherent structure for assessing exposure and assuring risks and issues are prioritised and treated accurately
	Assurance scrutiny	CAF-RA	Attacker-led GovAssure and CAF readiness, grounded in first-hand delivery experience, producing, assessor-grade evidence, and aligning CAF outcomes to real attacker behaviour.
	Executive stabilisation	Board/CISO	Executive decisions remain defensible during uncertainty or active exposure, providing stabilisation and clarity.
	Reputation Response &	MxM	Protects organisational reputation through pre-built, media-grade crisis communications and executive preparation for real-world pressure, reinforced through regular rehearsal and specialist support if required.
Service Selection and Modularity	Each 360D service is available individually or as part of a coherent, attacker-informed, defender-led risk structure. Buyers may select one, several or all components depending on organisational context, priorities and exposure. Services are designed to operate standalone or in combination, with URxM providing the integrated method for full-cycle risk governance.		
Why this is different	Traditional cyber companies starts with controls / countermeasures and ask whether they are present. 360D starts with hostile reality and asks whether a real adversary would succeed.		



	We view the organisation as an attacker would, then apply a defender-led mirror to remove attacker line-of-sight, stabilise exposure, and ensure risk, assurance and executive decisions remain coherent. This is assurance by construction, not inspection.
Service categories	• Cloud Support Services ○ Security Services ○ Security Strategy ○ Security Risk Management <i>This service is delivered under Cloud Support and does not include hosted platforms or managed services.</i>
Service features and benefits	
Features	• Defender-led, attacker-informed analysis grounded in real adversary behaviour • Integrated view across cyber, physical, personnel and reputational risk • Decision-grade outputs for executives, SROs and assurance functions • Consistent logic across all 360D specialist services • Judgement-led methods over automated or checklist-driven approaches • Modular delivery aligned to organisational maturity and exposure • Suitable for routine, complex, uncertain or crisis-driven situations • Coherent risk logic across assets, threats, impacts, paths and assurance • Board Toolkit materials available to support executive-level decision-making
Benefits	• Clarifies what genuinely matters to attackers and therefore decision-makers



	• Prevents false confidence from tool or framework-driven outputs • Keeps risk coherent across assessment, governance and assurance • Reduces friction with assessors and regulators • Enables proportionate, defensible investment decisions • Supports leadership confidence under uncertainty or pressure • Avoids fragmented or contradictory security advice • Protects mission, reputation and executive credibility
Service Delivery benefit	• Provides rapid, decision-grade clarity for leaders facing complex, high-impact or high-uncertainty cyber risk • Ensures decisions are grounded in credible attacker behaviour • Enables proportionate, defensible action aligned to operational security, assurance and executive governance
Service Implementation Planning	• Initial scoping discussion to confirm objectives, priorities, constraints and organisational context • Agreement of engagement focus and interfaces with existing risk, assurance or operational activity • Analyst-led delivery conducted primarily offline, with targeted stakeholder engagement • Iterative validation of findings with nominated client contacts • Delivery of agreed outputs with optional executive or assurance briefings
Service scope	



360D Specialist Cyber Security & Risk Services <i>(Attacker-Informed, Defender-Led)</i>	This service covers advisory, analytical and decision-support activity only. It does not include: • Managed security services • Hosting or operation of platforms • Automated scanning or tooling • Compliance auditing
Service constraints	Dependent on access to appropriate organisational context (unless working 100% offline). Requires availability of knowledgeable stakeholders. Judgement-led outcomes cannot be fully automated Effectiveness depends on clarity of decision intent
Do you hold a suitably scope ISO27001 certificate for this G-Cloud Service.	ISO27001 is not applicable to this service. This is a skills-based advisory service and does not involve the operation of hosted platforms or client production systems.



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 Not applicable (The service involves no hosting, platform operation or data custody)
On-boarding and Off-boarding processes/scope etc.;	On-boarding • Confirmation of scope, objectives and decision context • Identification of assets, services and stakeholders • Agreement on intended use of outputs Off-boarding • Formal handover of outputs and decision logic • Optional executive or assurance briefings • Clear articulation of assumptions and limitations
Consumer responsibilities:	• Provide timely access to relevant contextual information, documentation and stakeholders • Nominate an appropriate point of contact for coordination and clarification.



	Engage senior stakeholders where decisions, validation or prioritisation input is required. Details of any trial service available: Not applicable (skills-based service).
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	<i>This service does not include a standing user helpdesk; support relates to engagement coordination only.</i> 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 is based on SFIA 6 (default) : complex analytical judgement, autonomy, cross-domain influence and SFIA 7 : where work directly shapes enterprise risk posture, executive decisions or national-level exposure
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.