360 DEFENCE (UK) LTD – SERVICE DEFINITION

B1. Umbrella Risk Management (URxM)

Service attributes	
Service type	Lot 3: Cloud Support
Service name	
Service name	B1. Umbrella Risk Management (URxM)
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.** URxM delivers defence grounded in threat informed, attacker shaped understanding of how adversaries identify, target and pressure organisations. It connects assets, threats, impacts, attack paths, risks and executive decisions into one defender cycle, keeping risk coherent and defensible from first hostile interest through governance.

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 owned management supporting modular and standalone specialist service delivery. • Threat informed, attacker shaped defence grounded in real adversary missions. • Explicit attack-path modelling using attacker logic and structured progression • Impact, appetite and tolerance aligned to real threat behaviour • Coherent risk views across clients assets, core services and enterprises • Assurance-aligned structure supporting CAF/GovAssure readiness • Executive stabilisation logic enabling Board/CISO clarity under pressure • Reputational damage protection integrated throughout Media and Crisis Communications capability • Judgement-led analysis not automated scoring or checklists • Repeatable, evolvable management adapting to changing threats and environments

Benefits	Delivers clear, defensible risk across all organisational layers Ensures decisions reflect attacker behaviour not assumptions or control-based models. Strengthens understanding of attacker progression supporting proportionate defensive action Aligns risk appetite and tolerance to real exposure, improving decisions Prevents fragmented or contradictory risk outputs across teams and services Reduces assurance friction through attacker-shaped CAF/GovAssure alignment Enables confident executive decisions during uncertainty or hostile pressure Protects organisational reputation through integrated Media and Crisis response Avoids checklist driven distortion and tick box risk models Sustains clarity as threats evolve maintaining long term risk stability
Service Implementation Planning	Delivery is modular and phased. Organisations can adopt individual components or the full URxM cycle, with services integrated progressively according to maturity, exposure and decision priorities.
Service scope	
Umbrella (URxM) Diagram Overview	

How to interpret this diagram

	This diagram shows how organisations make risk decisions in the face of sustained cyber and non-cyber threat. The storm above represents persistent, unavoidable threat pressure. The umbrella represents **Umbrella Risk Management (URxM)**— the protective governance, controls and oversight that reduce exposure without pretending threats can be eliminated. Beneath the umbrella, the **Risk Mirror** reflects both the defender's business view and the attacker-informed view, ensuring decisions are grounded in mission impact, attacker reality and control effectiveness. The outcome is not technical perfection, but informed, accountable risk decisions aligned to organisational tolerance and purpose. **Board narrative: risk, choice and assurance** Threat is constant and increasingly unpredictable, like weather, it cannot be stopped. This model shows how leadership stays protected by making deliberate, informed choices rather than reacting to incidents. The umbrella represents an organisation's risk management framework: governance, assurance and scrutiny that reduce exposure and prevent over-reaction. The Risk Mirror ensures leadership sees both sides at once: what matters most to the organisation, and what adversaries are realistically capable of doing. Decisions are then taken consciously, within tolerance, with confidence that risks are understood, owned and managed rather than hidden or deferred. **Technical narrative: threat pressure and risk decisions** The diagram models sustained threat pressure acting across multiple attack paths, some of which will penetrate controls. Umbrella Risk Management provides layered governance, assurance and control oversight, reducing blast radius rather than claiming absolute prevention. The Risk Mirror aligns defender-led impact analysis (AssetID, BIRA, mission criticality) with attacker-informed assessment (threat reality, attack paths, control pressure). This convergence supports explicit Risk Assessment and Risk Management (RxA/RxM) decisions, enabling prioritisation, acceptance, countermeasure

	enhancement or transfer based on realistic threat behaviour and control effectiveness, rather than hypothetical risk.
URxM Phases and Intent	**Defender / Business View** *Italic = phase intent, normal text = service shorthand* **Phase 0 – Mission** *Purpose & Mandate* **Phase 1 – What matters – AssetID** *Identify and prioritise defender-led assets shaped by attacker interest.* **Phase 2 – Impact & tolerance – BIRA** *Define realistic impact severity and risk appetite.* **Phase 5 – Risk decisions – RxA / RxM** *Determine defensible risk treatment and prioritisation.* ***Attacker-Informed View*** *Italic = phase intent, normal text = service shorthand* **Phase 3 – Threat reality – TxA / TxA-E** *Clarify hostile interest, capability, intent and shared behaviours.* **Phase 4 – Attack paths – RxA / RiskTree** *Model attacker pathways, dependencies and progression.* **Phase 6 – Pressure on controls – RxM** *Understand how attackers stress, bypass or exploit controls.*
What the Umbrella actually includes	

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 Trees (RiskTree)	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.
What URxM is	URxM is a defender-owned approach that uses real attacker behaviour to keep risk coherent, defensible and decision-ready across the organisation. It connects assets, threats, impacts, attack paths, risks, assurance and executive decisions into one structured, repeatable system that remains stable under pressure.		
Why URxM this is different	**Traditional risk frameworks assess controls in isolation.** URxM models the organisation as a real adversary would attack it, then connects assets, threats, impacts, attack paths, risks, assurance and executive decisions into one continuous, cyclical and repeatable structure. This is **assurance by construction**, not inspection producing risk that remains defensible and coherent from first hostile interest through to board-level decision-making.		

Service constraints	Dependent on timely provision of contextual and asset and service information
Do you hold a suitably scope ISO27001 certificate for this G-Cloud Service.	**ISO 27001 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** URxM on-boarding involves confirming scope, identifying the URxM components to be delivered, and agreeing the sequencing of workshops, interviews and validation activities. **Off-boarding** URxM includes delivery of agreed outputs, review of findings and recommendations, and confirmation of any follow-on phases or optional components.

Consumer responsibilities:	• Provide relevant asset, service and contextual information • Nominate stakeholders for validation, review and workshop attendance • Confirm intended use of outputs (operational, executive, assurance)
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 user helpdesk; support relates to engagement coordination only.* 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

	URxM pricing is based on SFIA-aligned effort. URxM components are typically delivered at senior SFIA levels due to the strategic judgement, attacker-led analysis and enterprise-level decision support required. Prices are published in the 360D G-Cloud pricing and SFIA rate-card document. Pricing (including unit prices, volume discounts, data extraction, etc.) Pricing is based on SFIA-aligned effort and does not include fixed-price deliverables unless explicitly agreed at call-off. Volume-based fee discounts may be offered where an individual resource is contracted for engagements exceeding 60 full working days, subject to agreement 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.