



360 DEFENCE (UK) LTD – SERVICE DEFINITION

E3. Media Assessment/Review, Training, Crisis Communications, Reputation Protection (MxM)

Service attributes	
Service type	Lot 3: Cloud Support
Service name	
Service name	E3. Media Assessment/Review (MxM), Training, Crisis Communications, Reputation Damage Protection
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	360D provides reputational damage protection for public bodies, combining Media Assessment/Review(MxM), crisis communications and management with real-world crisis media training. The service draws on practitioners with frontline 4th/5th Estate experience to develop playbooks, templates and spokesperson capability, including live incident support, enabling calm, appropriate responses across mainstream and social media.



Service categories	• Cloud Support Services ○ Security Services ▪ Security strategy ▪ Security risk management ▪ Security incident management ▪ Security audit services ▪ Security quality assurance (QA) and testing ▪ Other • Reputation Damage (RepDam) Protection. Media and Crisis Management and Crisis incident response <i>This service is delivered as a cloud support consultancy and does not include hosted platforms or managed services.</i>
Service features and benefits	
Features	• Tailored crisis communications playbook aligned to organisational risks • Crisis communications team mapping and escalation approvals • Time-phased reactive and proactive response planning (0–72 hours) • Pre-prepared message templates: holding statements, scripts, Q&A • Channel-specific messaging for social, web and print media • Misinformation response pack: rapid, factual and lawful correction templates • Media and platform prioritisation by influence and risk • Spokesperson training from recorded practice to live interviews



	• Delivery and body-language coaching for calm messaging • Optional live incident communications support (remote)
Benefits	• Reduces reputational harm through faster, accurate public communications • Maintains organisational control of key messages during incidents • Enables calm, appropriate responses under media and public pressure • Integrates communications into cyber and technology incident response • Provides clear rationale, scripts and escalation routes under stress • Reduces risk of reactive or improvised public statements • Supports de-escalation by preventing misinformation and message drift • Improves readiness through realistic rehearsal and pressure testing • Reduces distraction for operational and technical teams • Optional live incident call-out support out of hours
Service Delivery benefit	You are a target. • Public bodies operate under constant scrutiny, and incidents will attract media attention at speed. By assuming this early, rehearsing communications under pressure, and applying disciplined crisis response, organisations reduce reputational harm and avoid reactive, misdirected spend when scrutiny escalates.
Service Implementation Planning	• Discovery: objectives, likely scenarios, stakeholders, constraints, comms approval routes



	• Information gathering; incident response interfaces (including cyber), existing playbooks and gaps • Design: playbook structure, templates, escalation/approval flow, training plan and timetable • Delivery: workshops, drafting, scenario rehearsal and spokesperson coaching • Review: lessons learned, updates to templates and playbook, handover and next-step plan
Service scope	
MxM	MxM provides structured media assessment, crisis communications planning, spokesperson development and reputational damage protection for organisations. It focuses on preparing teams to communicate clearly under pressure, counter misinformation, and maintain control of public messaging during incidents. MxM does not replace incident response, legal counsel, or organisational communications functions. It strengthens them by providing structured playbooks, trained spokespersons, and disciplined crisis-ready messaging aligned to organisational risk. MxM covers: • Assessment of media exposure and reputational risk drivers • Design of crisis communications playbooks and approval flows • Preparation of message templates, holding statements and Q&A • Scenario-based rehearsal and spokesperson coaching • Optional live incident communications support (remote)



	MxM does not provide: • Hosting or management of communications platforms • Public relations services unrelated to incident or crisis scenarios • Long-term outsourced communications staffing • Technical incident response or forensic investigation
Service constraints	Dependent on timely access to stakeholders for interview/rehearsal, and timely approvals for final messaging templates/playbooks. Work is typically delivered remotely; on-site delivery by agreement.
Do you hold a suitably scope ISO27001 certificate for this G-Cloud Service.	ISO27001 is not applicable to this service. MxM is a skills-based training and optional incident support capability and does not involve the operation of client production systems, hosted platforms or managed information services.
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 operations or data custody.)



	Service consist of documents, templates and training outputs; copies can be provided to the client on request.
On-boarding and Off-boarding processes/scope etc.;	On-boarding: Confirm of scope, stakeholders, and organisational communications context. Agreement of information handling expectations and delivery schedule. Access to any required client-side cloud services, tools or collaboration platforms. Off-boarding: Handover of playbooks and templates and supporting materials. Guidance on closure of communications activities. Support for client off-boarding from any platforms used during delivery. Training: Spokesperson and communications team training (recorded practice through to live interview simulation). Playbook walk-through and scenario rehearsal.
Consumer responsibilities:	Provide timely access to relevant stakeholders, existing comms/IR materials. Supply required approvals, and any client-side tool or channel access. Provide a suitable video-conferencing (VC) platform or remote workshop (e.g., Microsoft teams or equivalent) 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	Yes Phone support availability 9 to 5 (UK time), Monday to Friday
Web chat support	No
Support levels	<i>This service does not include a standing user helpdesk; support relates solely to engagement coordination and any explicitly agreed incident call-out.</i> <i>Support hours and response times are agreed per engagement.</i> <i>A named service lead provides coordination throughout delivery, including:</i> • <i>agreed cadence (e.g., weekly check-ins during delivery)</i> • <i>progress reporting against plan</i> • <i>issue and decision logging for approvals and sign-off</i> • <i>final read-out and handover</i>



	<i>Optional incident call-out can be agreed with defined availability, contact route and response expectations.</i>
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, where applicable to the specific engagement.
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.