360 DEFENCE (UK) LTD – SERVICE DEFINITION

E2. Board/CISO Executive Leadership Support

Service attributes	
Service type	Lot 3: Cloud Support
Service name	
Service name	E2. Board/CISO - Executive Leadership Support
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	Board/CISO exists when leaders sense something is wrong, or exposure is present, but traditional indicators don't explain it. 360D delivers defence grounded in threat-informed, attacker-shaped logic to validate hostile reality, identify attacker line-of-sight, stabilise exposure, and restore defensible executive security decision-making. Not incident response: executive-level threat validation and control stabilisation.

What Board/CISO is	Board/CISO is a **specialist executive security support capability**. It is activated when organisations face uncertainty, emerging hostile pressure, suspected compromise, or strategic security failure that cannot be explained or resolved through routine indicators, reporting or tooling. Board/CISO applies 360D's defence-first, threat-informed, attacker-shaped Risk Mirror logic at executive level: assessing the organisation through hostile line-of-sight, then flipping that view to stabilise exposure and restore defensible security decision-making. This is not staffing, body-shopping or incident response. It is judgement-led executive security leadership support.
Why Board/CISO is different	**Board/CISO exists for the moment when leaders feel something is wrong or already know it is** but dashboards, reports and controls cannot explain why. Traditional models ask whether controls or countermeasures exist. **Board/CISO asks whether a real adversary would succeed.** It validates threat reality, identifies attacker line-of-sight and stabilises exposure so leadership decisions remain defensible. This is **assurance through threat reality**, not inspection.

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 services.
Service features and benefits	
Features	• Executive-level rapid response security leadership under uncertainty • Threat-informed, attacker-shaped Risk Mirror analysis for leaders • Validate or disprove suspected hostile exposure rapidly • Identify attacker line-of-sight across people, assets, and operations • Prioritise stabilisation and containment actions at executive level • Recalibrate strategic controls and countermeasures when indicators conflict or mislead • Supports Boards and CISOs with Board Toolkit decision-making materials • Integrates with full 360D defence and risk services • Short-duration, outcome-focused executive intervention delivery • Delivered by Principal/lead practitioner specialists
Benefits	• Confirms whether real hostile exposure exists • Reduces uncertainty when indicators conflict or mislead • Prevents overreaction or paralysis at executive level • Clarifies attacker visibility, leverage and organisational exposure • Restores confidence in executive security decision-making • Aligns leadership action to real adversary behaviour • Accelerates stabilisation without long engagements • Avoids defaulting to tool-driven or checklist responses • Supports decisive leadership under pressure • Protects mission, reputation and executive credibility

Service Delivery benefit	• Immediate executive-level clarity when uncertainty or exposure threatens organisational stability
Service Implementation Planning	• Initial confidential scoping to confirm concern, urgency and context • Principal/lead practitioner-led rapid assessment using threat-informed, attacker-shaped logic • Short, time-bound engagement focused on validation, stabilisation and executive clarity • Clear recommendations for follow-on activity where required
Service scope	
Board CISO	Board/CISO provides short-duration, high-intensity executive security leadership support where uncertainty, suspected hostile activity or strategic security failure cannot be resolved through routine reporting, tooling or controls. It focuses on validating threat reality, identifying attacker line-of-sight, stabilising exposure and restoring defensible executive security decision-making using 360D's defence-first, threat-informed, attacker-shaped logic. Board/CISO does not replace a permanent CISO, provide managed security services or act as incident response.
Service constraints	• Dependent on timely access to senior stakeholders and relevant organisational context • Requires availability of organisational insight needed for threat validation • Client action required where risk acceptance or mitigation decisions are necessary

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 risk management service provision** Not applicable (The service involves hosting, platform operations or data custody.)
On-boarding and Off-boarding processes/scope etc.;	**On-boarding** • Initial confidential engagement to confirm concern, urgency and organisational context • Agreement of information handling expectations and delivery timelines • Identification of senior stakeholders required for threat validation and decision support **Off-boarding** • Formal delivery of findings, stabilisation guidance and executive-level recommendations • Optional briefing for Boards, CISOs, SROs or senior leadership • No client data is retained by 360D

Consumer responsibilities:	Provide timely access to senior stakeholders and relevant organisational insight. Supply contextual information required to validate threat reality and exposure. Confirm intended use of outputs (executive decision support, assurance, stabilisation) **Details of any trial service available:** Not applicable (The service is a 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	*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 Pricing is based on SFIA-aligned effort. Board/CISO engagements are delivered at SFIA Level 7 by default, reflecting the autonomous executive judgement, adversary interpretation and strategic authority required.

	SFIA Level 6 may support analysis where appropriate. Prices are published in the 360D G-Cloud pricing and SFIA rate card. 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.