SERVICE DEFINITION

CISO-AS-A-SERVICE

BARRIER

ABOUT US

At Barrier, our mission is to help our customers build cyber resilience and develop strategies to defend against cyber-attacks. We have developed a portfolio of services and solutions that suit customers small and large, in both the private and public sector. Our portfolio encompasses security consultancy, solutions from innovative vendors to mitigate attacks, through to managed services that proactively detect attacks and provide swift incident response measures.

We have built a practice dedicated to providing assurance that systems are resilient to attack. We provide penetration testing services to check the effectiveness of the deployed controls against real-world attacks, and we can implement a vulnerability management system to maintain levels of operational resilience.

Our aim is to build trust and understanding of how our customers' organisation functions. Our work takes us across all sectors, with strong references in the Finance Sector, Data Hosting, Legal, Local Government, MOD, and the wider Public Sector.

Established in 2006, we are a cybersecurity-focused solutions and service provider. Our customers trust Barrier as a strategic part of their cybersecurity team and here's why:

- Our knowledge of the cybersecurity industry helps select the right solutions
- Our experience helps organisations build cohesive cyber resilience strategies
- Our people are empowered to work closely with our customers to forge strong partnerships
- Our services become an intrinsic part of our customer's security operations

Barrier Networks Limited
272 Bath Street, Glasgow, G2 4JR
Tel: 0141 356 0101

SERVICE OVERVIEW

Barrier's CISO-as-a-Service (CISOaaS) offering provides organisations with access to experienced security leadership to define, implement, and mature their information security strategy, governance, and compliance posture.

SERVICE FEATURES

CISOaaS delivers strategic, operational, and advisory capabilities across the following areas:

- **Governance, Risk, and Compliance:** Development or refinement of cybersecurity governance frameworks, risk assessment and management processes (including risk registers and mitigation plans), support for regulatory compliance, and cyber and information security policy development.
- **Cyber Strategy and Roadmap:** Creation of a cyber and information security strategy aligned with business objectives, definition of a multi-year roadmap with prioritised initiatives, metrics and KPIs to track maturity and performance, budget planning and justification for cyber investments.
- **Security Architecture and Design Oversight:** Oversight of secure design principles in IT and digital initiatives ('Secure by Design'), review and approval of solution architectures from a security standpoint, security input to vendor selection and third-party assurance.
- **Operational Security Management:** Oversight of day-to-day operations (in liaison with SOC/MSSP), incident response leadership or coordination, vulnerability and patch management oversight.
- **Awareness, Culture, and Training:** Development of a cyber awareness and training programme and creation of communication plans for staff engagement.
- **Board and Executive Engagement:** Regular board reporting, e.g. creation and dissemination of dashboards, risk summaries, heat maps, etc.

SERVICE DELIVERABLES

Each CISOaaS engagement is individually scoped using Barrier's structured Deliverables Framework. Typical deliverables in alignment with the core service features are listed below.

ACTVITY	TYPICAL DELIVERABLES	FREQUENCY
Governance, Risk, and Compliance (GRC)		
Development or Refinement of Cybersecurity Governance Frameworks	Current State Assessment Report; Target-State Definition; Framework Implementation or Refresh Plan; Framework Documentation and Integration	Annual
Risk Assessment and Management Processes	Risk Management Framework Definition; Risk Evaluation and Prioritisation; Mitigation Planning and Treatment; Governance, Reporting and Integration; Continuous Improvement and Annual Refresh	Quarterly
Support for Regulatory Compliance (e.g. GDPR/DPA18, PCI DSS, CE, DORA, SOC2, etc.)	Compliance Framework Definition and Scoping; Baseline Assessment and Gap Analysis; Remediation Planning and Control Implementation Support; Evidence Management and Audit Readiness	Annual
Cyber and Information Security Policy and Procedure Development	Policy Framework Definition and Alignment; Current-State Policy and Procedure Review; Policy and Procedure Development; Stakeholder Engagement and Communication; Assurance and Integration	Annual
Cyber Strategy and Roadmap		
Oversight of Secure Design Principles in IT and Digital Initiatives ('Secure by Design')	Secure by Design Framework and Governance; Design Review Process Establishment; Design Engagement and Oversight Activities; Secure Architecture Integration and Alignment	Annual
Review and Approval of Solution Architectures from a Security Standpoint	Architecture Review Framework and Governance; Architecture Intake and Scoping; Detailed Architecture Review; Approval and Assurance Outcomes; Integration with Enterprise and Project Governance	Annual
Security Input to Vendor Selection and Third-Party Assurance	Third-Party Risk and Assurance Framework; Procurement and Vendor Selection Support; Supplier Onboarding and Due Diligence	Annual

Operational Security Management		
Oversight of Day-to-Day Security Operations	Operational Security Governance and Oversight Framework; SOC/MSSP Performance and Service Management; Operational Threat and Incident Monitoring Oversight; Vulnerability and Exposure Management and Risk Capture; Define Internal Audit, Security Testing, and Assurance Requirements; Operational Reporting and Metrics	Quarterly
Incident Response (IR) Leadership or Coordination	IR Framework and Governance; IR Preparedness and Readiness; Active Incident Coordination and Leadership; Investigation and Forensic Oversight; Post-Incident Review and Reporting; Training, Exercises, and Continuous Improvement	Biannual
Vulnerability and Patch Management Oversight	Framework and Governance Definition; Current-State Assessment and Baseline Establishment; Vulnerability Identification and Prioritisation Oversight; Patch Management Oversight; Reporting and Performance Management	Quarterly
Awareness, Culture, and Training		
Development of a Cyber Awareness and Training Programme	Awareness and Training Strategy Definition; Current-State and Needs Assessment; Programme Design and Content Development; Implementation and Delivery Support; Measurement, Metrics, and Reporting	Annual
Creation of Communication Plans for Staff Engagement	Communication Strategy and Governance; Current-State Review and Needs Analysis; Communication Plan Development; Content Creation and Collateral Development	Annual
Board and Executive Engagement		
Regular Board Reporting	Governance and Reporting Framework; Reporting Template and Visualisation Design; Core Board Reporting Deliverables; Strategic and Thematic Reporting; Executive and Board-Level Briefings on Security Posture and Threats	Quarterly

ADDITIONAL DELIVERABLES

Quarterly service reports tracking progress and key service metrics are provided. Additional activities are available as additional professional services engagements (subject to scoping):

- Vendor/Product Research and Guidance
- Security Awareness to Technical and Non-Technical Audiences
- Threat Landscape Assessment and Presentations
- Supplier Security Risk Evaluation
- Internal Security Auditing
- Routine Security Management

SERVICE OUTCOMES

- **Strategic Cybersecurity Direction:** Clearly defined cybersecurity strategy and delivery roadmap aligned to business context and objectives.
- **Enhanced Risk Visibility and Management:** Clear, ongoing insight into the organisation's cyber risks through documented mitigation plans, progress tracking, and risk ownership.
- **Informed Decision-Making:** Translate technical security risk into clear, business-focused insight to improve board understanding and support confident, timely decisions.
- **Strengthened Security Governance:** Establish structured governance through regular security steering or risk committees for accountability and oversight.
- **Improved Compliance Readiness:** Align organisational policy and controls with relevant standards and regulations, providing evidence-based assurance.
- **Operational Resilience and Incident Preparedness:** Improve readiness with tested response processes, escalation paths, and continuous maturity improvement.

SUPPORT LEVELS

Support Level	Operational Hours	Operational Days	Targeted Response
8x5xNBD	08:30 – 17:30	Monday - Friday	Next Business Day

CUSTOMER REQUIREMENTS

For the service to operate, the customer will be required to provide the following:

- Any available reports, policies, procedures, incident playbooks, risk registers, and other documentation.
- Access to key stakeholder for interviews and meetings for each deliverable.
- A schedule of regular meetings with key stakeholders.
- A single point of contact for the Service to facilitate communications.
- A named Risk Owner for organisational risks.

EXCLUSIONS

Services that Barrier will not provide as a part of CISOaaS are set forth below.

- **Incident Response**: Best efforts will be made to provide strategic support to the customer during incidents. An incident response retainer is purchased separately to support response to cybersecurity incidents.

- **Internal Security Audit**: Barrier will support or collaborate with internal or external auditors as required, but CISOaaS does not constitute or replace an independent internal audit function.

- **Cyber Risk**: The customer's organisational cyber risks are not owned by Barrier Networks.

- **Cyber Risk Remediations**: The customer retains ultimate responsibility for all risks and remediation of identified issues. Barrier can support agreed remediations through additional professional services engagement and procure technology where required. Barrier cannot make assurances or guarantees concerning audit outcomes, regulatory compliance, or risks of compromise.

BARRIER NETWORKS

272 Bath Street
Glasgow, United Kingdom
G2 4JR

info@barriernetworks.com
+44 (0)141 356 0101

BARRIER