SERVICE DEFINITION

CRTA & RISK OPERATIONS CENTRE (ROC)

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 Cyber Risk Technical Assessment (CRTA) provides a structured, expert-led evaluation of technical risks in a business context – delivering actionable, prioritised guidance and ongoing tracking to strengthen cyber resilience in a sustainable way.

SERVICE FEATURES

- **Technical Risk Discovery:** Technical controls protecting and monitoring information systems, data assets, and business processes will be systemically examined and assessed in alignment with industry best practices and established security standards (e.g. NIST CSF, CIS Top 18, Cyber Essentials, IEC 62443, etc.).

- **Risk Profile Building:** A selection of stakeholders within the customer's management team are interviewed in order to understand the key areas of risk to the organisation and enrich the technical findings with valuable organisational context as a result.

- **Risk Rating:** Technical findings are evaluated within the context of their relative risk in light of the current and emerging threat landscape, inclusive of considerations such as: (i) how the finding could be exploited in an attack, (ii) the potential impact on critical systems and processes, and (iii) its relevance to the organisation's strategic objectives and near-term goals.

- **Remediation and Risk Reduction Advisory:** Clear, prioritised guidance is delivered to address identified risks. Recommendations – considering both immediate mitigations and long-term security improvements – are tailored to the organisation's infrastructure, security maturity and operational constraints to ensure practical implementation.

- **Risk Operation Centre (ROC) Deployment:** A self-hosted web application, managed by Barrier and delivered through the Azure Marketplace, is deployed within the client's Azure infrastructure to provide a centralised interface for assessment results, risk tracking, and reporting.

SERVICE DELIVERABLES

- **CRTA Findings Workshop:** Following completion of the assessment, Barrier will host a workshop with the project sponsor in order to review the report and ensure that the findings are relevant and actionable.
- **CRTA Report:** Final report inclusive of an Executive Summary and detailed findings, risks, and remediations.
- **Remediation Roadmap:** A proposed roadmap of prioritised remediations grouped into logical collections of initiatives to guide swift and efficient risk reduction.
- **Risk Operations Centre (ROC) Platform:** An Azure web application, hosted in the customer's environment, to provide reporting, visualisations, and details of findings and recommendations. Deliverable inclusive of:
    - Initial deployment package and documentation
    - Provision of access and role-based permissions to required stakeholders
    - Updates to the platform software as required
    - Changes to user account access (e.g. adding or removing existing users)

SERVICE OUTCOMES

- **Real-Time Risk Awareness:** Executives and stakeholders have continuous, consolidated visibility of cyber risk through access to dynamic dashboards and periodic expert reviews.
- **Prioritised Remediation Planning:** Actionable, costed risk reduction initiatives allowing organisations to efficiently focus resource on the most critical remediations.
- **Simplified Compliance Management:** Alignment of risk findings to relevant standards and frameworks, reducing audit effort and improving regulatory confidence.
- **Contextual Risk Insight:** Translation of technical risk into business-relevant guidance, enhancing understanding of potential impact and organisational exposure.
- **Secure Data Ownership:** Full control and privacy over risk data within the customer's environment, reinforcing governance and trust in reporting.
- **Informed Decision-Making:** Integration of technical assessment findings with organisational context provides a complete view of cyber risk and prioritised risk reduction to support timely, confident business decisions.

SUPPORT LEVELS

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

SERVICE CHANGES

Barrier can carry out changes to the services following a customer request. These changes can range from simple to complex and will be determined by the Service Manager upon receipt of the change request.

Simple changes include actions such as adding or removing user accounts to maintain appropriate access to the ROC. Complex changes may involve configuration or customisation beyond standard access management and may require additional consultancy time and cost accordingly. This will be fully discussed and agreed with the customer prior to any change being carried out.

Customers are allocated 3 change requests per month across the lifetime of the service.

BARRIER NETWORKS

272 Bath Street
Glasgow, United Kingdom
G2 4JR

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

BARRIER