Service Definition Document

Cyber Security Assessment Service

Supplier: Sailotech UK Limited

Document Version: V1.1
Date: 14th January, 2026

+44 1296 841116
marcom@sailotech.com
G12, The Gatehouse, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 8DB, United Kingdom

1. Service Overview

Sailotech UK Limited provides a Cyber Security Assessment Service designed to support UK public sector organisations in understanding, managing, and reducing cyber security risk. The service delivers an independent, structured, and risk-based assessment of people, processes, and technology aligned with UK government guidance, recognised industry standards, and regulatory requirements. The service supports informed decision-making, improved cyber resilience, and compliance with UK public sector security expectations.

2. Scope of Service

In Scope

- Independent assessment of organisational cyber security posture
- Risk-based review of people, processes, and technology
- Security control effectiveness and maturity assessment
- Review of policies, standards, and governance arrangements
- Assessment against recognised frameworks (for example ISO/IEC 27001, NIST, and NCSC guidance)
- Identification of vulnerabilities, risks, and control gaps
- Risk prioritisation based on business impact and likelihood
- Actionable recommendations and remediation roadmap

Out of Scope

- Implementation or operation of security controls unless separately contracted
- Penetration testing unless explicitly included in scope
- Continuous monitoring, SOC, or managed security services
- Legal or regulatory sign-off activities

3. Service Delivery Model

The service is delivered primarily through secure remote engagement using approved collaboration tools. On-site delivery within the UK can be provided by prior agreement. Delivery follows a defined lifecycle including initiation, scoping, information gathering, assessment, analysis, reporting, and close-out. Delivery timelines are agreed at the outset and depend on scope, complexity, access approvals, and stakeholder availability.

4. Service Features

- Independent cyber security posture assessment aligned to recognised standards
- Risk-based analysis covering people, processes, and technology
- Security control maturity assessment and gap identification
- Policy, governance, and compliance review
- Vulnerability and threat exposure assessment
- Business impact–driven cyber risk prioritisation
- Actionable remediation roadmap
- Executive-ready reporting

5. Service Benefits

- Reduces cyber risk through early identification of weaknesses
- Improves compliance with regulatory and security standards
- Strengthens organisational cyber resilience
- Improves visibility of cyber risks
- Enables informed security investment decisions
- Supports prioritised remediation planning
- Reduces likelihood and impact of incidents
- Enhances confidence in security posture

6. Onboarding and Offboarding

Onboarding

- Scope definition and confirmation
- Stakeholder identification
- Assessment planning and scheduling

Offboarding

- Final reporting and findings walkthrough
- Secure handover of deliverables
- Formal service closure

7. Support Arrangements

Standard support is provided via email and online ticketing during UK business hours (Monday to Friday, excluding public holidays). Queries are acknowledged within one business day. Enhanced and Premium support options are available at additional cost and may include priority response times, access to named technical specialists, and service review meetings. All support arrangements and associated costs are clearly defined in the order form prior to service commencement.

8. Security and Compliance

Personnel Security

All staff involved in service delivery are screened in accordance with BS7858:2019 and the UK government's Cloud Security Principle on Personnel Security.

Government Security Clearance

As a minimum, staff meet Baseline Personnel Security Standard (BPSS) requirements. Where required, staff with Security Clearance (SC) can be provided subject to role requirements, buyer approval, and agreed lead times.

Data Protection and Privacy

The service is delivered in compliance with UK GDPR and the Data Protection Act 2018. Personal data is processed only where necessary for service delivery, handled securely, and retained in accordance with contractual and legal requirements.

Information Security

Sailotech UK Limited applies appropriate technical and organisational measures to protect information accessed during service delivery, including access controls, secure storage, and data minimisation principles.

9. Service Constraints

The service is delivered within the agreed scope, timeframe, and assumptions defined at engagement start. Findings represent a point-in-time assessment and may not reflect future changes to systems or threats. Delivery is dependent on timely access to systems, documentation, and stakeholders. The service does not include out-of-hours or weekend support unless agreed separately.

10. Pricing

Pricing is defined in the Sailotech UK Limited g-Cloud 15 pricing document available on the Digital Marketplace.

11. Accessibility Statement

This document has been produced in line with GOV.UK guidance on publishing accessible formats. It is intended to meet WCAG 2.2 AA accessibility standards and has been structured to support assistive technologies, including screen readers. The document uses clear headings, logical reading order, plain English, and accessible formatting. An alternative accessible format can be provided on request.