Cyber Consultancy Service Definition

Document title	Cyber Consultancy Service Definition		
Reference No.	IF-SER-010	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Holly Jackson, Cyber Manager		
Issue date	23/01/2026		

Cyber Consultancy Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Holly Jackson	Review and amendments	12/01/2026
1.0	Lisa Washer	Final review and publish	23/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Cyber Consultancy Service Definition

Contents

Cyber Consultancy Service Definition

1. Cyber Consultancy Services

1.1 Service Overview

1.1.1 Cyber Consultancy Services provide organisations with expert guidance to understand and manage cybersecurity risks effectively. The purpose of these services is to provide expert advice and practical solutions that strengthen security posture, ensure compliance, and support long-term resilience. These services address common needs such as improving risk management, reaching compliance, creating clear security policies, and supporting informed decision-making around cyber resilience.

1.2 Service Features

1.2.1 The following lists the core capabilities and characteristics of the service:

- **Security Posture & Maturity Assessments -** Independent evaluation of current controls against recognised frameworks (e.g., NIST CSF, ISO/IEC 27001), with a maturity score and prioritized improvement plan.
- **Risk Assessment & Treatment Planning -** Structured identification of risks (threats, vulnerabilities, impacts), risk rating, and a pragmatic treatment plan with owners, timelines, and success criteria.
- **Policy, Standards, and Procedure Development -** Creation or refresh of security policies, control standards, and operational procedures tailored to the organization's size, culture, and regulatory context.
- **Governance & Operating Model Design -** Definition of roles, responsibilities, decision forums, RACI matrices, and reporting rhythms to embed effective security governance.
- **Roadmaps -** 6–24 month security roadmaps, dependency mapping, costed options, and business cases that link actions to risk reduction and measurable outcomes.
- **Risk-Based Prioritisation -** Focuses on highest-impact, feasible actions first, balancing risk reduction, cost, complexity, and time-to-value.
- **Technical and Executive Reporting -** Clear, evidence-based reports suitable for technical teams, management, and regulators.

2. Service Benefits

2.1.1 The following lists the benefits of the service:

- **Improved Risk Visibility -** Organisations gain a clear understanding of their current security posture, vulnerabilities, and areas of exposure.
- **Informed Decision-Making -** Provides actionable insights and prioritisation, enabling leadership to allocate resources effectively and focus on high-impact areas.
- **Regulatory Compliance Support -** Helps meet industry and legal requirements (e.g., PCI DSS, GDPR, ISO 27001) through structured frameworks and guidance.
- **Enhanced Governance and Accountability -** Establishes clear roles, responsibilities, and processes for managing cybersecurity across the organization.
- **Operational Resilience -** Reduces the likelihood and impact of security incidents by embedding robust controls and proactive measures.
- **Cost Efficiency -** Avoids unnecessary investments by aligning security improvements with business priorities and risk appetite.
- **Knowledge Transfer and Capability Building -** Equips internal teams with the skills, processes, and documentation needed to maintain and evolve security practices independently.

3. Scope of Service

3.1 In-Scope Activities:

3.1.1 The scope of what is included within the cyber consultancy service is outlined here:

- Cyber risk assessments and maturity evaluations.
- Policy and governance framework development.
- Strategic security roadmap creation.
- Advisory on compliance and regulatory alignment.

3.2 Out-of-Scope Activities:

3.2.1 The following activities are not included as part of the standard cyber consultancy service scope:

- Direct implementation of technical controls.
- Managed security services or 24/7 monitoring.
- Incident response beyond advisory role.

3.3 Assumptions and dependencies

3.3.1 Delivery of the Service is subject to the following assumptions, constraints, and dependencies, which influence scope, timelines, and outcomes:

- **Timely Client Engagement** - Progress and timelines depend on timely engagement from nominated client contacts, including system owners, subject matter experts, and decision-makers.
- **Resource Availability** - Delivery is subject to specialist availability and agreed engagement terms, including scheduling and priority requirements.
- **Regulatory Change Impact** - Any changes to external regulations may affect the scope of work or the agreed project timelines.
- **Designated Point of Contact -** The client will provide an internal point of contact to coordinate activities and facilitate communication.

4. Onboarding

4.1.1 The onboarding process begins with a kick-off meeting where we align all stakeholders and confirm the objectives of the engagement. This meeting ensures clarity on scope, expectations, and key milestones.

4.1.2 Following this, we arrange access to the necessary documentation and systems required to perform assessments and deliver the agreed services. Secure access protocols are followed to maintain confidentiality and compliance.

4.1.3 Communication frequency and methods, including regular status updates, escalation notifications, and reporting cadence, are defined and agreed at the outset to ensure clear, consistent engagement throughout the investigation. Access requirements, constraints, and dependencies are documented, and coordination with legal, compliance, or third-party providers is initiated where required. Onboarding ensures clarity of roles, responsibilities, and next steps, enabling effective and timely activities.

5. Service Delivery Model

5.1 Engagement Approach

5.1.1 Our delivery model is collaborative and advisory-led, ensuring that we work closely with client stakeholders throughout the engagement. This approach promotes transparency, alignment, and shared ownership of outcomes.

5.1.2 Delivery is primarily conducted remotely to maximize efficiency and reduce costs, although on-site workshops can be arranged when face-to-face collaboration is beneficial. This flexibility ensures that the engagement meets the client's operational needs.

5.2 Delivery Phases

5.2.1 The service is typically delivered across the following phases:

- **Discovery** – This initial phase focuses on understanding the client's current environment, objectives, and challenges. We gather relevant information through documentation reviews and stakeholder interviews to establish a clear baseline.
- **Assessment** – During this phase, we analyse the client's security posture, identify risks, and evaluate existing controls against recognized frameworks. This provides a comprehensive view of strengths and weaknesses.
- **Recommendations** – Based on the assessment findings, we develop actionable recommendations that address identified gaps and align with the client's business priorities and risk appetite.
- **Roadmap Development –** In the final phase, we create a strategic roadmap that outlines prioritised initiatives, timelines, dependencies, and cost considerations to guide the client toward improved security maturity.

5.3 Typical Timelines

5.3.1 The typical timeline for delivery ranges from two to twelve weeks, depending on the scope and complexity of the engagement. This timeframe allows for thorough analysis, stakeholder input, and the development of actionable recommendations.

6. Support Model

6.1.1 We provide support during standard business hours, Monday to Friday, from 09:00 to 17:00 GMT. Clients can reach us through email or scheduled calls for any queries or assistance required during the engagement.

6.1.2 For issues that require escalation, we follow a defined escalation path managed by the dedicated engagement lead to ensure timely resolution and continuity of service.

7. Service Level Agreements

7.1.1 The following service levels describe indicative performance targets for the service. These service levels are provided for guidance only and do not constitute guaranteed commitments unless expressly agreed in writing.

7.1.2 Where a pre-existing contract or retainer agreement is in place, the service levels and SLAs defined within that agreement shall apply and take precedence over the indicative service levels outlined below.

7.2 Response time

7.2.1 We aim to respond to all client queries within two business days, ensuring timely communication and continuity throughout the engagement.

7.3 Delivery timeframe

7.3.1 Deliverables are provided in accordance with the agreed project plan, ensuring that all outputs meet the defined scope, quality standards, and timelines. Each deliverable is reviewed for accuracy and completeness before submission. Where applicable, interim updates are shared to maintain transparency.

7.4 Reporting turnaround

7.4.1 Reports are issued within ten business days following the completion of the assessment phase, ensuring that findings are documented clearly and comprehensively.

8. Technical Requirements

8.1.1 Delivery of the Service requires appropriate information, and resources to enable effective activities. The following requirements apply and are confirmed during onboarding.

- **System and Environment Information -** Provision of relevant technical documentation, such as network diagrams, asset inventories, system architecture, identity and access models, and security tooling in use, to support audits and assessments.
- **User and Stakeholder Availability -** Availability of client personnel to support access provisioning, clarify system behaviour, and validate findings.
- **Secure Communications -** Use of secure communication channels for information exchange, including file transfer and reporting, to protect sensitive information.
- **Video Conferencing Capability -** Required for remote workshops.

9. Exit and Offboarding

9.1.1 The service concludes once all agreed activities have been completed and final deliverables have been provided. Service closure is managed in a controlled manner to ensure clarity of outcomes, secure handling of information, and effective knowledge transfer.

9.2 Final Deliverables

9.2.1 At the conclusion of the engagement, all agreed deliverables are provided in the specified format, ensuring completeness and alignment with contractual obligations. This may include final reports, strategic roadmaps, governance documentation, and any supporting materials developed during the engagement.

9.3 Knowledge Transfer and Close-Out

9.3.1 A close-out meeting may be held to review findings, explain conclusions, and discuss recommended next steps. This session supports knowledge transfer to relevant stakeholders, including IT, security, legal, and management teams, and provides an opportunity to address questions and clarify outcomes.

10. Roles and Responsibilities

10.1.1 The following roles are defined to ensure effective governance, delivery, and communication throughout the engagement.

10.2 Account Manager

10.2.1 Acts as the primary commercial and engagement contact for the organisation. Responsible for contract management, service coordination, and strategic escalation. Ensures the service is delivered in line with agreed scope and expectations.

10.3 Engagement Lead

10.3.1 Oversees the engagement by managing timelines, coordinating communication between all parties, and ensuring deliverables meet the required quality standards.

10.4 Consultant

10.4.1 Delivers assessments, develops recommendations, and prepares reports in line with the agreed scope and quality expectations.

10.5 Client Lead

10.5.1 Acts as the organisation's primary point of contact for the engagement. Coordinates internal stakeholders, facilitates access to documentation and information, and supports decision-making and escalation activities.

*****END OF DOCUMENT*****