Service Specification – Cyber Maturity Assessment and Advisory Service

1. Service Description

The Cyber Maturity Service provides consultancy-led, independent assessment and advisory support to help organisations understand and improve their cyber security maturity. The service focuses on governance, risk management, assurance, and organisational readiness, aligned to recognised public sector cyber frameworks. The service is advisory in nature and does not include managed security services or operational control.

2. Scope of Service

The service includes review of cyber governance arrangements, policies and procedures, risk management practices, assurance processes, and organisational capability. Delivery may include documentation review, stakeholder interviews or workshops, gap analysis against recognised frameworks such as CAF and DSPT, and development of a prioritised cyber improvement roadmap.

3. Service Exclusions

The service does not include system configuration, technical remediation, penetration testing, security monitoring, incident response execution, hosting, or managed cyber security services. Responsibility for implementation and operation remains with the customer.

4. Delivery Approach

The service is delivered remotely or on-site as agreed. Delivery is planned in advance and aligned to organisational priorities, scale, and risk. Timescales are confirmed at service initiation.

5. Outputs and Deliverables

Deliverables typically include a cyber maturity assessment report, identified risks and gaps, maturity ratings across defined domains, and a clear, prioritised improvement roadmap. Reports are suitable for both technical and executive audiences.

6. Service Levels and Support

Support requests are logged and triaged based on impact and urgency. Tickets are acknowledged within one business day, with high-priority issues responded to on the same working day. Service levels relate to consultancy responsiveness only.

7. Security and Confidentiality

All work is conducted in line with industry-standard information governance practices, including confidentiality, secure handling of information, and least-privilege access.

8. Dependencies and Client Responsibilities

Service delivery depends on timely access to relevant documentation, stakeholders, and information. The customer retains responsibility for cyber operations, system security, and regulatory compliance.

9. Exit and Knowledge Transfer

On completion, assessment outputs and documentation are provided to the customer. As no customer data is hosted as part of this service, all operational data remains with the customer.