RelianceCyber

Cyber Maturity Assessment

Service Definition

G-Cloud 15

Lot 3: Cloud Support

Contact Details

Email: tenders@reliancecyber.com

Contact Number: +44 (0) 845 519 2946

Contents

1 Overview 3

2 Methodology 5

2.1 Project Governance 6

2.2 Assumptions and Requirements 7

3 Why Reliance Cyber? 8

3.1 Core Capabilities 8

1 Overview

A maturity model is a tool for assessing an organisation's effectiveness at achieving a particular goal. In the context of cyber security, maturity models can help distinguish between organisations where security is baked in and those where it is merely bolted on.

When evaluating these models, our approach, proven over a decade with hundreds of clients, is cost- and time-effective. Our highly skilled consultants will work with you to assess your current cyber maturity. Using a structured methodology, we will assess your organisation's cyber maturity, review how it compares with recognised standards, and help you gain a clearer understanding of your current cyber maturity by identifying tactical improvements and setting long-term goals.

These engagements are designed to help support accreditation aspirations, align with specific standards or act as an enabler in achieving formal certifications against industry standards.

Key outcomes from the Cyber Maturity Assessment include:

- Workable tactical and strategic plans to address any deficiencies identified.
- Identification and prioritisation of mitigation activities.
- Provision of future budget and resource planning insights and capacity modelling.
- Identification of third-party contract requirements that can assist in overall cyber maturity controls.
- Suggestions for lower operating cost expenditure through optimisation and technical debt reduction.

This is a time and materials engagement based on the size of the organisation, the complexity of the IT estate, the maturity of the current IT controls and adherence to specific needs. All equivalent day rates will be shared, and a detailed breakdown of the proposed costs will be provided upon completion of initial scoping of the engagement.

Features	Benefits
• Cyber maturity assessed against recognised standards, such as NCSC CAF, NIST CSF, ISO 27001, NIS2 and CIS. • A tried and tested approach to assessing organisational maturity and finding areas for improvement. • Development of a cyber security strategy that aligns with possible planned change within the business. • Assessment of internal cyber security skills and capabilities. • Clear recommendations to achieve an improved cyber maturity level. • Evidence-based reporting that is accessible to all levels of technical knowledge.	• A quantifiable understanding of your maturity level that can be tracked for continued improvement. • Validation of ongoing changes or improvements that have already been made. • Expert support to help you with improving your maturity. • Aligning your organisation with the UK Government Cyber Security Strategy 2022-2030. • Enables the prioritisation of issues based on risk to the business. • Identifies vulnerabilities before they can be exploited. • Increase your resilience and response capabilities to cyber incidents. • Align budget and resources to mitigate against actual threats to your organisation.

2 Methodology

Our proven engagement methodology will help us understand your current cyber maturity, enabling us to highlight where and how you can improve going forward. The engagement will deliver prioritised recommendations which can be implemented to enhance the effectiveness of your security controls across your organisation. Our approach will:

- Identify gaps in your information security posture by aligning the current environment to threats commonly affecting the UK public sector and CNI.
- Help prioritise roadmap initiatives to close identified gaps, exposing the environment to high-risk threat vectors.
- Document existing security maturity for increased visibility to executive leadership.
- Understand your reliance on specific defences, where there are gaps in coverage or overlap, which may give an opportunity to reduce operating costs.

Our assessment methodology consists of:

1. **Documentation Review**

We will provide a documentation request list before beginning the assessment. Our consultants will review this documentation before kick-off to gain a better understanding of your environment and quickly identify any potential weaknesses.

The consultants will schedule interviews and workshops based on this information, as well as provide you with a detailed scoping questionnaire.

2. **Project Kick-Off**

A kick-off with key stakeholders relevant to the assessment will be scheduled. Our consultants will go over the assessment in detail, running through project specifications, including timings, resource commitments and constraints, to ensure all stakeholders understand what is required of them during the assessment.

3. **Workshops**

Workshops covering a range of information security domains will be scheduled with appropriate individuals in your organisation to investigate and gather evidence of current information controls. These workshops provide a deep dive into the organisation's security posture, enabling gaps and issues to be identified, as well as areas of good practice.

4. **Reporting**

A finalised report will be provided upon completion of the workshops. This will give a detailed account of your current level of cyber maturity and will be accessible to readers of all technical levels. An executive summary will highlight the key findings, with further detailed technical documentation provided within the report. Recommendations to improve your maturity will be provided, highlighting the next steps required to enhance your cyber security maturity.

A presentation will also be delivered to your stakeholders and board members. The presentation will provide an executive-level view of key cyber risks across the organisation and recommendations for remediating the most serious issues, based on risk exposure and return on investment.

5. **Follow-Up Workshop (optional)**

Optionally, we can schedule a follow-up workshop with your stakeholders for our consultant to go over their recommendations and understand how your organisation is managing the implementation of change.

This further workshop may be held six months following the final presentation. This additional workshop allows you to highlight the progress you've made, raise any challenges you've found and allows our consultant to provide insight and additional recommendations to further develop your cyber maturity.

2.1 Project Governance

It is important to define how the project will be organised so that clear management direction is possible. A complex cyber programme requires individuals with experience in consultancy, risk management, business continuity, pervasive monitoring and incident response, and we will provide subject-matter experts as required for the engagement.

To track progress and provide updates to all stakeholders, we will provide:

- Weekly progress reports via email, covering key activities, progress and any issues requiring escalation.
- Checkpoint meetings every two weeks (mid-month and end-of-month) to cover progress issues in more detail, and will include planning for the next two-week period, including resource requests.

In the event of any serious findings or failures, we will immediately escalate them to your management.

2.2 Assumptions and Requirements

Our approach is structured around minimising disruption, reducing the overhead of your internal resources and maximising self-guided deliverables where possible. However, involvement from all areas of the client's business is required with the engagement. This includes:

- Documentation, agreed ahead of the engagement, covering the following key areas:
  - Organisation chart, highlighting teams and functions with responsibility for cyber security.
  - Cyber and Information Security Policy set.
  - Incident Response policies and playbooks.
  - Previous Maturity Assessments performed.
  - Any documentation supporting certification or alignment to a recognised standard.
  - Supply Chain Risk Management framework and assessments.
  - Training materials covering aspects of information and cyber security.
  - Internal or external audit reports covering information and cyber security.
  - Threat intelligence, where applicable.
  - Network diagrams and information.
  - Asset lists were available, covering infrastructure, software and endpoint devices.

- Interviews with key staff:
  - All the key identified departments should nominate key staff for interviews so that the interview process covers operations, technology, assurance and audit and review functions.

Unless otherwise requested, we will conduct this work remotely. In addition, we will work flexibly to accommodate the different time zones and different meeting requirements.

To ensure the programme does not run into delays, you should ideally provide a coordination resource to help set up meetings, provide documentation and related materials and check deliverables for completeness.

3 Why Reliance Cyber?

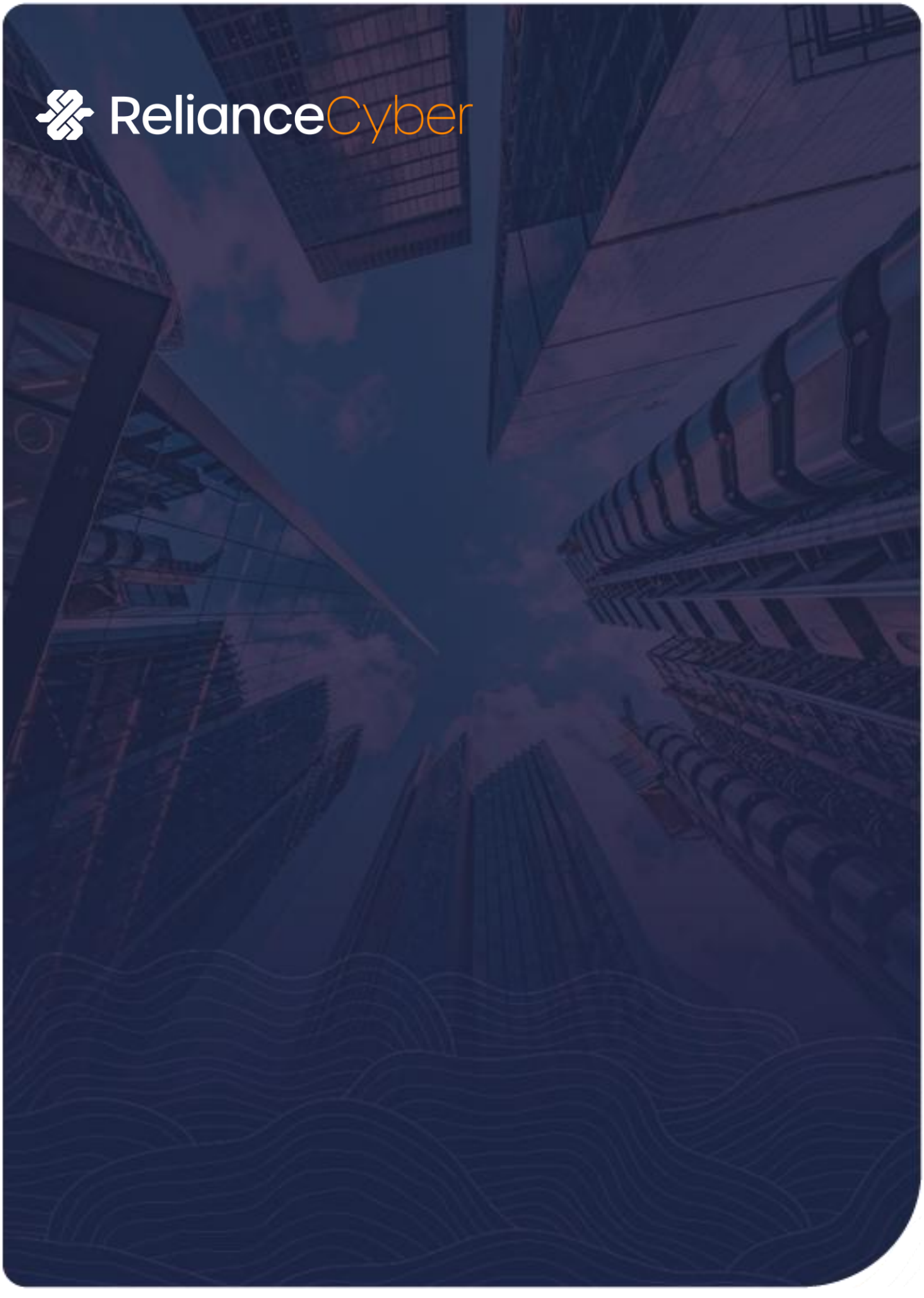
Reliance Cyber is a Managed Security Services Partner (MSSP), dedicated to fortifying our clients through cyber security. With a rich legacy spanning 20 years, Reliance Cyber has emerged as a trusted and innovative MSSP, continually reinvesting to ensure our clients receive the best security support on the market. This has enabled us to recruit the best SC specialists and develop market-leading capabilities focused solely on cyber security.

Operating 24x7x365, we prioritise collaboration, transparency and long-term trust-based relationships with clients to navigate the ever-evolving landscape of cyber threats.

3.1 Core Capabilities

Reliance Cyber's core services are structured around three strategic pillars, reflecting our holistic approach to cyber threat management across managed, proactive and reactive services.

- **Managed Services** – We deliver enhanced security operations through continuous monitoring, proactive threat detection, and rapid remediation. Operating 24x7 on our clients' behalf, our managed services include Managed Detection and Response (MDR), Managed Endpoint Detection and Response (EDR), Managed Secure Access Service Edge (SASE), Phishing Monitoring and Vulnerability Management.
- **Proactive Consulting Services** – We support clients in identifying and addressing vulnerabilities before threat actors can exploit them. Our proactive security offerings include Cyber Threat Intelligence, Crisis Simulations, Compromise Assessments and a range of bespoke solutions tailored to meet each client's unique risk landscape.
- **Reactive Consulting Services** – When incidents occur, we provide expert incident response and recovery support. Our services are delivered using methodologies certified by CREST and aligned with guidance from the National Cyber Security Centre (NCSC). Leveraging deep digital forensics expertise, we help clients contain, investigate, and recover from cyber incidents swiftly and effectively, minimising impact and enabling lessons learned to strengthen future defences.


RelianceCyber