Cyber Maturity Assessment (CMA)

- Identify risks
- Map out areas for improvement
- Enhance your security framework

Triskele Labs

Are you managing a significant volume of sensitive customer information?

Or are you concerned about the performance of your outsourced IT partners?

Do you know your cyber security gaps and your plan to remediate them?

Are you trying to plan your cyber security budget but need help figuring out where to start?

Have you previously suffered a cyber security incident?

Why do you need a Cyber Maturity Assessment (CMA)?

CMA is a comprehensive evaluation of an organisation's environment using our proprietary framework, which integrates elements of ISO27001, NIST Cybersecurity Framework (CSF) V2 and Essential 8, combined with our extensive experience.

The Cyber Maturity Assessment will encompass a comprehensive review from the boardroom to the basement, focusing on both strategic and operational levels to evaluate the cybersecurity posture across 19 key domains. The aim is to identify risks, gaps, and areas for improvement to enhance your organisation's security framework.

- Security Overview
- Asset Management
- Business Environment
- Network Security
- Access Control
- Awareness and Training
- Data Security
- Host Security
- Patch Management
- Mobile Device Management
- Data Loss Prevention (DLP)
- Configuration Management
- Threat Management
- Vulnerability Management
- Security Monitoring
- Resource Planning
- Backup & Recovery
- Business Continuity
- Disaster Recovery

Project Phases

Project Initiation and Planning

Technical Review

Cyber Maturity Assessment

Project Management and Quality Assurance

Use Cases

An organisation suffered a cyber security breach. Based on the advice received during the investigation, they remediated the initial issue that resulted in the breach. Unsure of their other cyber security weaknesses, they commissioned an CMA. The CMA identified further issues and helped the organisation modernise their IT infrastructure.

An organisation relied heavily on outsourced IT management with an MSP. Management wanted independent assurance that the MSP was managing their IT infrastructure correctly and not creating any vulnerabilities that could be exploited.

An organisation's board has been hearing a lot about cybersecurity in the news after several high-profile incidents. They want to understand their current cyber security posture to ensure they do not suffer a cyber security incident.

An organisation conducted a cyber security review three years ago. They have implemented the recommendations from the review and wish to validate their work and confirm that their environment aligns with current day-best practices.

Triskele Labs

Get in touch

triskelelabs.com
1300 24 CYBER
info@triskelelabs.com

Contact Us

Exclusions

Remediation Services
The engagement does not cover the actual remediation or implementation of recommended security measures. However, we will provide guidance and support on how you can address identified issues.

Full Compliance Audits
The CMA and Technical Review will incorporate elements of industry frameworks, but this engagement does not constitute a full compliance audit against ISO27001, NIST CSF V2, or any other specific standard.

Continuous Monitoring
The engagement is a point-in-time assessment and does not include ongoing monitoring of organisations environment. Continuous monitoring services can be provided under a separate agreement if required.

Analysis of Raw Scan Results
The raw results from the vulnerability scans will be provided as-in, with ought detailed analysis. However, customers are welcomed to choose to engage us for further analysis if needed.

Terms & Conditions

- 100% payment on signing
- Fees exclude GST
- Any additional services requested beyond the scope of this proposal will be quoted separately and invoiced accordingly.