Cybersecurity Scorecard - Scoring Guide

Score	Description
0	Not implemented
1	Initial / Ad hoc - some elements exist but are unstructured
2	Developing - processes are starting to be formalised
3	Defined and repeatable - controls are documented and repeatable
4	Managed and measurable - effectiveness is tracked and improved
5	Optimised and embedded - continuous improvement is built-in

Cybersecurity Scorecard Questionnaire

Governance

- Do you have a documented cybersecurity policy that is reviewed annually?
- Who is responsible for cybersecurity at board/executive level?
- Are roles and responsibilities for cyber risk clearly defined?

Risk Management

- When was your last formal cyber risk assessment completed?
- Do you assess vendors and partners for cyber risk before engagement?
- Are third-party risks tracked and remediated?

Access Management

- Is Multi-Factor Authentication (MFA) enforced for all remote and admin access?
- Are privileged accounts regularly reviewed and limited by role?
- Are access rights removed immediately when staff leave?

Asset Management

- Do you maintain a regularly updated inventory of all devices, servers, and software?
- Are data assets classified based on sensitivity or regulatory requirements?
- Is there a process to track and decommission legacy assets?

Vulnerability Management

- How often do you perform internal and external vulnerability scans?
- What is your typical patch deployment timeline for critical updates?
- Are unsupported systems or software still in use?

Security Monitoring

- Do you have centralised log management and alerting in place?
- Are logs reviewed regularly for suspicious activity?
- Do you use a SIEM or MDR/XDR platform to detect threats?

Incident Response

- Is there a documented incident response plan in place?

Cybersecurity Scorecard Questionnaire

- Has the IR plan been tested (e.g., tabletop exercise) in the last 12 months?

- Are key contacts and escalation paths clearly defined?

Backup & Recovery

- Are backups encrypted and stored offline or in immutable storage?

- Are backups tested for restoration at least quarterly?

- Is your recovery time objective (RTO) documented and achievable?

User Awareness & Training

- Do employees receive annual cybersecurity awareness training?

- Are phishing simulations conducted, and are results tracked?

- Is training tailored by role (e.g., finance, execs, tech teams)?

Compliance & Standards

- Are you compliant with GDPR or other applicable regulations?

- Are you aligned with or certified against standards like ISO 27001 or Cyber Essentials?

- Do you regularly audit or assess compliance posture?