Cyber Insurance Readiness Assessment Checklist

Score each item:

- Yes = 2 points
- Sometimes = 1 point
- No = 0 points

Coverage Awareness

☐ I understand in plain terms what cyber insurance is designed to do.
☐ I do not assume traditional business insurance automatically covers cyber events.
☐ I know whether our organisation currently has cyber coverage.
☐ I understand the major incident categories our policy is intended to address.

Policy Visibility

☐ I know the insurer, broker, and policy renewal details.
☐ I understand key deductibles, waiting periods, or sublimits.
☐ I have reviewed major exclusions in business language.
☐ I know what incident notification process the insurer requires.

Underwriting and Insurability

☐ MFA is active on important business systems.
☐ We maintain tested backups.
☐ Employee phishing/fraud awareness exists in some form.
☐ Underwriting disclosures accurately reflect our actual controls.

Claims Preparedness

☐ We know how to contact the insurer quickly during an event.
☐ We understand which response vendors may be insurer-appointed.
☐ We can document business interruption and recovery losses if needed.
☐ Leadership understands that insurer involvement may begin immediately.

Cybersecurity Beyond Insurance

☐ We do not treat cyber insurance as a replacement for cyber hygiene.
☐ Password and privileged account controls are supervised.

☐ Vendor/cloud access is reviewed periodically.
☐ We recognize that insurance cannot remove all operational disruption.

Financial Resilience Maturity

☐ Leadership views cyber incidents as both security and financial events.
☐ We think about both prevention and recovery economics.
☐ Cyber insurance decisions are reviewed strategically, not casually renewed.
☐ We see cyber insurability as part of modern business resilience.

SCORING RESULTS

38–48 Points → Strong Maturity

Your organisation demonstrates strong financial and operational awareness around cyber coverage, claims readiness, and insurability discipline.

22–37 Points → Moderate Exposure

You have some awareness or coverage in place, but meaningful blind spots still exist around policy understanding, controls, or claims preparedness.

0–21 Points → High Vulnerability

Your business likely remains financially underprepared for digital incidents and may be relying on assumptions rather than informed resilience planning.