IT Outsourcing Readiness Assessment Checklist

Score each item:

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

Vendor Selection and Clarity

☐ We understand exactly what outsourced IT services are included.
☐ We understand what services are billed separately.
☐ We asked cybersecurity-specific questions before signing.
☐ We did not choose the provider solely on lowest price.

Business Control

☐ Critical admin/vendor accounts remain retrievable by the business.
☐ Leadership knows where privileged credentials are stored.
☐ We possess or can request technical documentation.
☐ We could transition providers if necessary without complete chaos.

Cybersecurity Visibility

☐ We know what endpoint/security tools are actually deployed.
☐ MFA is enforced on critical business systems.
☐ Backup oversight is visible rather than assumed.
☐ Leadership understands cybersecurity is shared responsibility.

Vendor Accountability

☐ We receive recurring reporting or review meetings.
☐ Support responsiveness is consistent.
☐ Cyber recommendations are proactive, not only reactive.
☐ Costs are explained in relation to visible business value.

Financial and Contract Awareness

☐ We understand long-term contract implications.
☐ Licensing/tool invoices are not opaque bundles we never review.
☐ We periodically reassess provider fit rather than auto-renewing passively.

Executive Digital Confidence

☐ Leadership can ask practical oversight questions without hesitation.
☐ We do not feel technically captive.
☐ We know who handles what during outages or cyber incidents.
☐ Outsourcing has reduced confusion rather than deepened it.

SCORING RESULTS

38–46 Points → Strong Maturity

Your organisation demonstrates healthy outsourced IT governance, preserved business control, and strong vendor visibility.

22–37 Points → Moderate Exposure

You have outsourced support in place, but several assumptions or control gaps may still create avoidable dependence or cyber uncertainty.

0–21 Points → High Vulnerability

Your business is likely highly dependent on outsourced IT without sufficient visibility, accountability, or technical ownership protection.