Cybersecurity Risk Assessment Master Checklist

25-Point Business Exposure Review

☐ Are critical digital assets listed?
☐ Are business-critical dependencies identified?
☐ Are privileged users inventoried?
☐ Is MFA enabled on key systems?
☐ Are former staff/vendor accounts removed?
☐ Is website software reviewed?
☐ Is hosting access reviewed?
☐ Is business email MFA enabled?
☐ Are suspicious inbox rules reviewed?
☐ Is domain registrar secured?
☐ Are employee devices inventoried?
☐ Are software updates enforced?
☐ Are staff phishing risks reviewed?
☐ Are payment scam controls documented?
☐ Are customer data exposure points understood?
☐ Are backups automated?
☐ Has restore been tested?
☐ Are backups isolated?
☐ Are suspicious login alerts enabled?
☐ Are website uptime/SSL alerts active?
☐ Are malware alerts routed actively?
☐ Are risks labelled high/medium/low?
☐ Are owners assigned to fixes?
☐ Is monthly reassessment scheduled?
☐ Would the business know its top 5 cyber risks today?

Scoring:

21–25 = Strong cyber visibility maturity
15–20 = Moderate unmanaged exposure
0–14 = High uncertainty and hidden vulnerability