Ransomware Preparedness Audit Checklist

20-Point Business Ransomware Readiness Audit

☐ Are all critical devices inventoried?
☐ Is MFA enabled company-wide?
☐ Are weak passwords eliminated?
☐ Are remote access ports secured?
☐ Are operating systems patched?
☐ Are endpoint protections monitored?
☐ Are local admin rights restricted?
☐ Are backups stored offsite?
☐ Are backups immutable/disconnected?
☐ Have restore drills been tested?
☐ Is network segmentation in place?
☐ Are broad file permissions reduced?
☐ Are employees phishing trained?
☐ Is there a ransomware incident playbook?
☐ Are vendor emergency contacts documented?
☐ Are legal/insurance contacts prepared?
☐ Is executive communication planned?
☐ Are critical systems prioritized?
☐ Is alternate communication available?
☐ Are quarterly cyber drills scheduled?

Scoring:

17–20 = Strong ransomware resilience
12–16 = Moderate operational exposure
0–11 = High shutdown vulnerability