Website Recovery Readiness Audit Checklist

20-Point Backup & Continuity Audit

☐ Are full website files backed up?
☐ Is the database backed up?
☐ Are media/uploads included?
☐ Are backups automated?
☐ Are backups offsite?
☐ Are multiple restore points kept?
☐ Is dynamic customer/order data protected?
☐ Is backup storage secured?
☐ Is MFA enabled on backup accounts?
☐ Is restore ownership clear?
☐ Has a restore ever been tested?
☐ Is restore timing understood?
☐ Are emergency contacts documented?
☐ Are failed backup notices reviewed?
☐ Are backups checked monthly?
☐ Is quarterly restore simulation scheduled?
☐ Are WooCommerce/customer systems considered?
☐ Could malware-infected backups be bypassed?
☐ Is continuity documentation current?
☐ Would the team know what to do today?

Scoring:

17–20 = Strong recovery resilience
12–16 = Moderate continuity gaps
0–11 = High disaster vulnerability