Website Security Compliance Audit Checklist

20-Point Business Due Diligence Audit

☐ Are all privileged users inventoried?
☐ Are dormant accounts removed?
☐ Is MFA enabled on sensitive systems?
☐ Is customer data collection understood?
☐ Are forms securely handled?
☐ Is checkout trust professionally maintained?
☐ Is HTTPS healthy across the site?
☐ Are SSL renewals monitored?
☐ Are backups automated?
☐ Has restore been tested?
☐ Are security alerts monitored?
☐ Are suspicious logins watched?
☐ Are malware/file changes monitored?
☐ Are plugins/vendors reviewed?
☐ Is vendor access documented?
☐ Is registrar ownership clear?
☐ Are customer account protections active?
☐ Is monthly website review assigned?
☐ Is internal website oversight documented?
☐ Would the business appear reasonably careful?

Scoring:

17–20 = Strong digital responsibility maturity
12–16 = Moderate compliance gaps
0–11 = High negligence exposure