Domain & DNS Security Audit Checklist

20-Point Domain Protection Audit

☐ Is registrar ownership clearly known?
☐ Is registrar MFA enabled?
☐ Is registrar password unique?
☐ Is recovery email current?
☐ Is transfer lock active?
☐ Are A/CNAME records documented?
☐ Are MX records verified?
☐ Are SPF records correct?
☐ Are DKIM records healthy?
☐ Is DMARC configured?
☐ Are obsolete DNS entries removed?
☐ Are subdomains inventoried?
☐ Is SSL dependency understood?
☐ Are certificate renewals watched?
☐ Are DNS change alerts active?
☐ Is domain reputation monitored?
☐ Are registrar notices routed properly?
☐ Is monthly DNS review scheduled?
☐ Is quarterly infrastructure audit scheduled?
☐ Would unauthorised DNS changes be noticed fast?

Scoring:

17–20 = Strong domain infrastructure maturity
12–16 = Moderate DNS exposure
0–11 = High invisible trust risk