Login Security Audit Checklist

20-Point Authentication Hardening Audit

☐ Are all privileged accounts inventoried?
☐ Are dormant accounts removed?
☐ Are critical passwords unique?
☐ Are shared team logins eliminated?
☐ Is MFA enabled on sensitive systems?
☐ Are authenticator methods strong?
☐ Are login attempts rate-limited?
☐ Are bot challenges active?
☐ Is username enumeration reduced?
☐ Are session cookies secure?
☐ Are remembered sessions controlled?
☐ Are password reset flows reviewed?
☐ Is business email protected?
☐ Are admin roles minimized?
☐ Are customer accounts monitored?
☐ Are SSO permissions understood?
☐ Are failed logins logged?
☐ Are suspicious access alerts enabled?
☐ Is monthly credential review scheduled?
☐ Is team credential training active?

Scoring:

17–20 = Strong authentication maturity
12–16 = Moderate unauthorised access exposure
0–11 = High credential vulnerability