Company Email Security Audit Checklist

20-Point Business Inbox Defence Audit

☐ Are all business inboxes inventoried?
☐ Is MFA enforced on every email account?
☐ Are passwords unique?
☐ Are forwarding rules reviewed?
☐ Are fake invoice scams discussed?
☐ Is CEO fraud discussed?
☐ Are suspicious attachments treated cautiously?
☐ Are manual logins preferred over emailed links?
☐ Are payment changes voice-verified?
☐ Are executive urgent requests confirmed?
☐ Are approved file-sharing methods documented?
☐ Is SPF configured?
☐ Is DKIM configured?
☐ Is DMARC configured?
☐ Are suspicious login alerts enabled?
☐ Are odd outbound email patterns monitored?
☐ Are remote/mobile email risks discussed?
☐ Is suspicious email reporting easy?
☐ Is company email policy written?
☐ Would one compromised inbox create major business confusion?

Scoring:

17–20 = Strong company email maturity
12–16 = Moderate communication exposure
0–11 = High inbox fraud vulnerability