Business Email Compromise Readiness Assessment Checklist

Instructions

Use this checklist to evaluate your organisation's Business Email Compromise resilience and operational fraud preparedness.

Score each item:

- Yes = 2 points
- Partial/In Progress = 1 point
- No = 0 points

Email Security & Authentication

☐ MFA is enforced for email and financial systems.

☐ Strong password policies are consistently followed.

☐ Email authentication protections are implemented.

☐ Suspicious login activity is monitored.

☐ Access permissions are reviewed regularly.

Financial Controls & Verification

☐ Wire transfers require multi-person approval.

☐ Payment changes require callback verification.

☐ Vendor banking changes are independently verified.

☐ Financial escalation procedures are documented clearly.

☐ Urgent payment requests require additional review.

Employee Awareness & Reporting Culture

☐ Employees receive regular phishing awareness training.

☐ Executive impersonation awareness is included in training.

☐ Employees understand how to report suspicious emails.

☐ Reporting culture encourages operational transparency.

☐ Awareness training is reinforced continuously.

Vendor & Operational Governance

☐ Vendor communication procedures are documented.

☐ Procurement teams verify payment requests carefully.

☐ Vendor risk exposure is reviewed regularly.

☐ Operational accountability is clearly assigned.

☐ Leadership maintains visibility into BEC risks.

Incident Preparedness & Resilience

☐ BEC incident response procedures exist.

☐ Financial fraud escalation procedures are tested.

☐ Operational continuity planning includes BEC scenarios.

☐ Remote workforce communication risks are evaluated.

☐ AI-driven fraud risks are discussed operationally.

Scoring Results

40–50 Points — Strong BEC Defence Maturity

Your organisation demonstrates strong operational discipline, fraud prevention maturity, and resilience-focused governance.

Continue strengthening:

- awareness culture,
- operational visibility,
- and continuous improvement practices.

20–39 Points — Moderate Fraud Exposure

Your organisation has foundational protections but may still face:

- operational inconsistencies,
- awareness gaps,
- or verification weaknesses.

Focus on:

- payment controls,
- awareness reinforcement,
- governance visibility,
- and reporting culture improvements.

0–19 Points — High Business Email Compromise Vulnerability

Your organisation may face significant exposure involving:

- weak verification procedures,
- poor awareness maturity,
- inconsistent governance,
- or limited operational discipline.

Immediate priorities should include:

- MFA enforcement,
- payment verification improvements,
- awareness training,

and incident preparedness planning.