Incident Response Readiness Audit Checklist

25-Point Manager Crisis Preparedness Audit

☐ Is an incident coordinator assigned?
☐ Is there a technical vendor contact list?
☐ Are hosting/provider contacts centralized?
☐ Are bank/payment escalation contacts documented?
☐ Is a communications lead assigned?
☐ Is an operations lead assigned?
☐ Is there a first-15-minute checklist?
☐ Is evidence capture documented?
☐ Are screenshots/timeline preservation expected?
☐ Is internal staff update routing defined?
☐ Is customer communication ownership defined?
☐ Is website outage procedure written?
☐ Is email compromise procedure written?
☐ Is payment fraud procedure written?
☐ Is ransomware escalation procedure written?
☐ Are suspicious login scenarios discussed?
☐ Are data exposure questions pre-considered?
☐ Are random reboots discouraged?
☐ Are vendor escalation rules clear?
☐ Are incident rumours centrally managed?
☐ Are tabletop drills run?
☐ Are confusion points reviewed after drills?
☐ Is monthly readiness review assigned?
☐ Would managers know what to do in the first hour?
☐ Would leadership look calm tomorrow?

Scoring:

21–25 = Strong incident leadership readiness
15–20 = Moderate crisis confusion risk
0–14 = High unpreparedness exposure