• CYBER & INCIDENT RESPONSE

Cyber Incident Readiness Checklist

Can your organisation respond effectively in the first 72 hours?

HOW TO USE THIS

Answer Yes only where the control is documented, owned and practically usable during an incident. Give yourself 1 point for each Yes. The objective is not perfect cybersecurity - it is a response process that does not depend on improvisation during a crisis.

1. Governance & ownership

✓	Question	Notes
☐	Is an Incident Commander formally appointed, with a named deputy?	
☐	Are IT/security, privacy, operations, communications and management roles pre-assigned?	
☐	Are time-critical decision rights agreed in advance (e.g. system shutdown, external forensics, regulator notification)?	
☐	Is there a clear severity model with response times for Critical / High / Medium / Low incidents?	
☐	Has senior management approved the incident-response framework?	

2. Escalation & first response

✓	Question	Notes
☐	Do staff know exactly how to report a suspected cyber incident?	
☐	Is there an out-of-hours escalation route for Critical incidents?	
☐	Is an offline copy of key contacts and escalation instructions available?	
☐	Is there a standard incident intake form and an incident log / timeline template?	
☐	Can the response team preserve evidence and contain affected systems without destroying forensic value?	

3. Regulatory & stakeholder notification

✓	Question	Notes
☐	Can the organisation determine quickly whether the incident is a personal data breach under GDPR?	
☐	Are GDPR 72-hour assessment and notification responsibilities clearly allocated?	
☐	Can the organisation identify whether NIS2 / national cyber-reporting or sector-specific rules apply?	
☐	Are cyber-insurer notification requirements and panel-provider restrictions known in advance?	
☐	Are contractual notification obligations to customers, suppliers or other stakeholders readily accessible?	

4. Scenario readiness

✓	Question	Notes
☐	Is there a usable ransomware / malware playbook?	
☐	Is there a phishing / business email compromise playbook?	
☐	Is there a lost or stolen device playbook?	
☐	Is there a data exfiltration / unauthorised access playbook?	
☐	Is there a critical SaaS / business-system outage or compromise playbook?	

5. Recovery & learning

✓	Question	Notes
☐	Are business-critical systems and recovery priorities identified?	
☐	Is responsibility for business continuity and return-to-service decisions clear?	
☐	Is there a board / management incident reporting format?	
☐	Are post-incident reviews and corrective actions formally tracked?	
☐	Has the organisation run a cyber tabletop exercise during the past 12 months?	

Your result

Score	What it suggests
21-25	Strong response foundation. Validate through exercises and periodic review.
16-20	Useful foundations exist, but material gaps could slow response or notification.
10-15	Significant readiness gaps. Response may depend on ad hoc decisions during an incident.
0-9	High dependency on improvisation. Prioritise roles, escalation, notifications and scenario playbooks.