CYBER RISK CHECKLIST

1. CHECKLIST DETAILS

Location/Department:	Assessed by:	Site:
	Position:	Date:
	Ref:	Review date:

2. CYBER RISK MANAGEMENT STRATEGY

(**x** as applicable)

- ☐ Has a cyber risk assessment been documented?
- ☐ Are cyber policies communicated to all relevant individuals?
- ☐ Are cyber policies periodically tested?
- ☐ Have management responsibilities been assigned for cyber risk?
- ☐ Have outsourced ICT services been risk assessed?
- ☐ Are policies in place covering all cyber risk areas?
- ☐ Are cyber policies periodically reviewed?
- ☐ Are cyber policies periodically audited against?
- ☐ Are regular meetings held on cyber risk?
- ☐ Are key ICT third parties vetted, monitored and audited?

Comments:

3. RESILIENCE AND BUSINESS CONTINUITY

(**x** as applicable)

- ☐ Has a Business Continuity Plan (BCP) been documented?
- ☐ Is the BCP in line with agreed recovery time objectives?
- ☐ Do key parts of ICT systems have suitable protections?
- ☐ Is the usage and capacity of key systems forecast and monitored?
- ☐ Are key system support and replacement standards agreed?
- ☐ Is software development undertaken away from live systems?
- ☐ Is the BCP based upon a business impact assessment?
- ☐ Do critical ICT systems avoid single points of failure?
- ☐ Is key data backed-up or replicated off site?
- ☐ Is all key hardware subject to planned maintenance?
- ☐ Are software and firmware updates tested before deployment?
- ☐ Is role and knowledge sharing employed in the ICT dept?

Comments:

4. SYSTEM SECURITY

(**x** as applicable)

- ☐ Do systems comply with a recognised IT security standard?
- ☐ Are internal and external networks segregated?
- ☐ Are software and firmware security patches applied immediately?
- ☐ Are users prevented from installing executable files?
- ☐ Authorised applications are white listed.
- ☐ Are secure audit trails of user activity generated?
- ☐ Are communications authenticated and encrypted?
- ☐ Do key ICT areas have physical & electronic security measures?
- ☐ Are user password changes enforced periodically?
- ☐ Do accounts lock after a number of incorrect access attempts?
- ☐ Are old user accounts and passwords removed immediately?
- ☐ Is anti-virus and intrusion detection software in place?
- ☐ Is anti-virus and intrusion detection software regularly updated?
- ☐ Are operating systems security hardened?
- ☐ Do systems flag suspicious behaviour?
- ☐ Is system vulnerability scanning undertaken periodically?
- ☐ Is system penetration testing undertaken periodically?
- ☐ Is the identity of users authenticated, e.g. by passwords?
- ☐ Do all users have unique logins?
- ☐ Do passwords contain a mixture of character types?
- ☐ Is the use of default accounts and passwords prohibited?
- ☐ Other (specify in comments below)

Comments:

5. DATA PROTECTION

(**x** as applicable)

- ☐ Does personal data storage comply with the Data Protection Act?
- ☐ Do systems prevent large quantities of data from being removed?
- ☐ Are databases located within protected internal networks?
- ☐ Is data on redundant hardware fully erased?
- ☐ Do data protection controls apply to those with remote access?
- ☐ Is access to sensitive data restricted to authorised users?
- ☐ Is sensitive data storage encrypted?
- ☐ Are portable devices and media writers disabled?
- ☐ Do data protection controls apply to data back-ups?
- ☐ Do data protection controls apply to those with smart phones?

Comments:

6. WEBSITE, INTERNET AND EMAIL USE

(**x** as applicable)

- ☐ Is third party content on websites vetted and/or moderated?
- ☐ Do websites use security protocols, such as SSL or TLS?
- ☐ Do cookies and marketing emails comply with legislation?
- ☐ Do internet browsers detect and filter unsafe/inappropriate sites?
- ☐ Do email systems protect against spam and spoof emails?
- ☐ Do website users have to register and accept T&C's?
- ☐ Are protections on phishing and MITB in place?
- ☐ Are staff trained on appropriate internet and email usage?
- ☐ Are rules in place on non-authorised communication methods?
- ☐ Do email systems detect and filter inappropriate content?

Comments:

7. PAYMENT CARD TRANSACTIONS

(**x** as applicable)

- ☐ Do relevant ICT systems comply with the PCI data security standard?

Comments:

LEGAL NOTICE