Resources

CYBER RISK CHECKLIST

strengthening digital resilience

Cyber threats continue to present significant risks to business operations, data security and reputation. This checklist helps identify common cyber exposures and practical controls to reduce risk, protect sensitive information and support business continuity.

GOVERNANCE & POLICY	
Establish a formal cybersecurity policy and update it regularly	
Define roles and responsibilities for cybersecurity oversight	
Conduct regular risk assessments and audits	
Ensure compliance with relevant regulations (e.g. GDPR)	

EMPLOYEE AWARENESS & TRAINING	
Provide ongoing cybersecurity training for all staff	
Implement phishing simulation exercises	
Enforce strong password policies and multi-factor authentication	
Create clear reporting channels for suspicious activity	

IT INFRASTRUCTURE & ACCESS CONTROLS	
Maintain an up-to-date inventory of all hardware and software	
Apply the principle of least privilege for user access	
Regularly patch and update systems and applications	
Segment networks to limit lateral movement	

THREAT DETECTION & RESPONSE	
Deploy antivirus and endpoint detection tools	
Monitor network traffic and logs for anomalies	
Establish an incident response plan and test it annually	
Set up alerts for unauthorised access attempts	

DATA PROTECTION & BACKUP	
Encrypt sensitive data at rest and in transit	
Implement secure data storage and disposal practices	
Schedule regular backups and test recovery procedures	
Use secure cloud services with strong access controls	

THIRD-PARTY RISK MANAGEMENT	
Vet vendors and partners for cybersecurity practices	
Include cybersecurity clauses in contracts	
Monitor third-party access to internal systems	
Review supply chain risks periodically	

CRISIS MANAGEMENT & RECOVERY	
Develop a business continuity and disaster recovery plan	
Identify critical assets and recovery time objectives (RTO)	
Assign a crisis response team and communication strategy	
Conduct tabletop exercises and simulations	

NOTES