Komstadt Managed Services
enquiry@komstadt.com · +852 2806 8188

FREE TOOL · 2-MINUTE SELF-CHECK

The SFC Cyber Self-Check

Ten questions that mirror the areas the SFC examines in a licensed firm. Answer each honestly with a Yes or No, then count your Yes answers. Most small firms score 4–6.

1	You keep a current inventory of every device and system	Yes / No
2	Nothing runs on end-of-life software (e.g. Windows 10, unsupported servers)	Yes / No
3	Security updates are applied within 30 days, and verified	Yes / No
4	MFA is enforced on email, remote access and every admin account	Yes / No
5	Staff connect remotely only via a company VPN with session timeouts	Yes / No
6	Your email domain is protected against spoofing (DMARC enforced)	Yes / No
7	Microsoft 365 has conditional access and least-privilege admin roles	Yes / No
8	Backups are encrypted and test-restored — including Microsoft 365	Yes / No
9	Staff had phishing-awareness training or a simulation in the last year	Yes / No
10	You hold vendor due-diligence records and SLAs for your IT providers	Yes / No

8–10 · Solid footing. Keep the evidence current — the SFC expects records, not recollections.

4–7 · Exposed. You're relying on luck in the areas flagged industry-wide.

0–3 · At risk. One phishing email or inspection could become an expensive week.

Scored below 8? Komstadt will verify your answers for free — one short visit and a written, RAG-rated findings report you keep. Email **enquiry@komstadt.com** to book.