

SAMPLE DELIVERABLE · ILLUSTRATIVE

IT & Cyber Assessment — Findings Report (sample)

An illustrative example of the report you receive after the free assessment — so you know what you're getting before you engage us. A real report is specific to your environment; ratings below are for illustration only.

Executive summary

Good foundations in identity and backup, but material risk from unsupported systems and an unprotected email domain. Four items need action within 30 days. Overall posture: **Amber — improvement required**.

Where the firm stands — a snapshot

Asset & end-of-life systems	Red
Patch management	Amber
Access control & MFA	Green
Email security (DMARC)	Red
Backup & recovery	Green
Incident response	Red

Example finding

Email domain can be spoofed (no enforced DMARC)

What we found — your domain publishes SPF but has no DKIM signing and no DMARC policy, so anyone can send email in your firm's name.

Why it matters — business-email-compromise fraud and phishing of your clients become far easier; it is also an area the SFC examines.

Recommendation — enable DKIM, publish a DMARC record, monitor for two weeks, then move to quarantine and reject.

Priority: High · target 30 days

Recommended roadmap

- ✓ **Quick wins (0–30 days):** enforce DMARC, retire the end-of-life server, close two dormant admin accounts
- ✓ **Strategic (30–90 days):** managed EDR rollout, tested-restore schedule, incident-response plan and drill

Your findings report is yours to keep, whether or not you engage us. Book the free assessment at enquiry@komstadt.com.