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

CHECKLIST · INVESTOR ODD

Investor ODD — the IT questions allocators ask

Before committing capital, institutional investors run operational due diligence (ODD) — and IT and cybersecurity are on the questionnaire. Prepare the evidence once, keep it current, and the next questionnaire becomes an attachment rather than a scramble.

What to have ready

Access & authentication

MFA enforced everywhere, including admins and remote access. A clear joiners/movers/leavers process for granting and revoking access.

Backup & recovery

What is backed up, how often, and when you last tested a restore. Your recovery time objective if systems go down.

Business continuity / disaster recovery

A written, tested BCP/DR plan — and where staff would work if the office were unavailable.

Cybersecurity controls

Endpoint protection, email security (SPF/DKIM/DMARC), patching cadence and monitoring — and how each is evidenced.

Vendor & third-party risk

Which providers touch your systems and data, with due-diligence records and SLAs on file.

Incident history & response, insurance, and regulatory alignment

A written, rehearsed incident-response plan; any past incidents; your cyber-insurance cover; and how your controls map to the SFC's cybersecurity expectations.

Komstadt's Compliance+ assembles and maintains this ODD evidence pack for you. Email **enquiry@komstadt.com** to see where your firm stands — free.