

PRACTICE TENDER — safe to paste into any AI

This is a fictional training document. Meridian One, Meridian Estates Pte Ltd, the reference number and every clause below are invented for practice. There is **no real client here** — so you can paste this into ChatGPT, Claude or Gemini freely and rehearse the whole workflow without touching a live tender. *(The one rule still holds in real life: never paste a real client's live tender into a consumer AI.)*

How to practise (Day 2 workflow):

1. Open a web AI chat. Paste the **CAGE prompt** below first, then paste **the tender** (from "TENDER" onward).
2. Ask it to **triage** every clause → Must-have / Nice-to-have / Risky red-herring.
3. Ask it to set a **posture** per clause → Comply / Not-comply (+alternative) / Clarify / N/A, each with a one-line rationale.
4. **Verify by hand.** Find the clauses that are indefensible to "Comply" to, and the ones that contradict themselves. The AI will miss some — that's the point.

The CAGE prompt (copy this in first)

You are helping a Mitsubishi Electric BMS salesperson respond to a building tender.

CONTEXT: We supply, install and maintain Building Management Systems – DDC/PLC controllers, HVAC and chiller control, fire-system integration, and the head-end software. We are the BMS vendor, not the building owner and not the network integrator. This is a practice tender.

ALIGN: Before you answer, play back in 3-4 lines how you plan to work through the clauses, and WAIT for me to say "go".

GOALS:

1. Sort every cybersecurity clause into Must-have / Nice-to-have / Risky red-herring.
2. For each clause set a posture: Comply / Not-comply (+ a better alternative) / Clarify / N/A – each with a one-line rationale.
3. Flag any clause that is indefensible to "Comply" to, any that contradicts itself, and any drafting slip.

You MUST NOT invent facts, standards or clause numbers. Mark anything uncertain as [UNVERIFIED].

EXAMPLE of the row format I want:

9.x | Must-have | Comply | "Per-engineer MFA through a recorded jump host – we do this as standard." | Pillar: Applications

Reply with your ALIGN plan only. Then wait for the tender.

TENDER

Tender Ref: BMS-2026-014

Project: Supply, Installation, Testing & Commissioning of an Integrated Building Management System (BMS)

For: Meridian One — a mixed-use commercial tower with a co-located hospital wing and a tenant data hall

Client: Meridian Estates Pte Ltd (the “Employer”)

Return by: *(practice — no deadline)*

Section 9 — Cybersecurity, Segmentation & Resilience Requirements

The Contractor shall comply with the following. Where the Contractor cannot comply, it shall state so and propose an alternative. Responses shall be made against each clause number.

9.1 The Contractor shall provide and maintain a complete inventory of every delivered device — controller, gateway, sensor and server — including firmware version and support status, updated on each change.

9.2 The BMS and building-control network shall be segmented from the corporate, guest and tenant networks. Communication out of the control network to any other network shall be restricted to the minimum necessary, and one-way where only one-way is required.

9.3 Any remote access to the delivered system shall be disabled unless required, require multi-factor authentication, pass through a secured intermediary (jump/bastion host), be session-logged, and be granted on a time-boxed, per-engineer basis.

9.4 All factory-default credentials shall be changed before handover. Any device running end-of-life or unsupported firmware shall be identified, with a containment plan.

9.5 Critical control sequences and setpoints (including the fire and smoke-control matrix) shall be baselined, backed up in restorable form, and monitored for unauthorised change.

9.6 The Contractor shall support the Employer’s incident-reporting obligations, providing logs and asset data in a form the Employer’s monitoring team can ingest.

9.7 Accounts on the delivered system shall follow least privilege, with no shared operator logins, and shall automatically log out after a period of inactivity.

9.8 The Contractor should provide a mobile dashboard application allowing the facilities team to view plant status remotely.

9.9 The Contractor should provide energy-analytics reporting suitable for the building’s Green Mark submission.

- 9.10** The Contractor shall warrant that the delivered system is **100% secure against all cyber threats** for the full duration of the maintenance contract.
- 9.11** All products supplied under this contract shall be **CCoP-certified**.
- 9.12** Anti-virus software shall be installed, running and kept updated on **every field controller and DDC** in the building.
- 9.13** All data in transit and at rest within the BMS shall be protected using **quantum-proof encryption**.
- 9.14** Remote vendor access to the control network shall be **permanently disabled at all times**. The Contractor shall also provide **24/7 remote support** with a guaranteed 2-hour remote response to critical faults.
- 9.15** User passwords for the head-end software shall be a minimum of **eight (12) characters**, changed every 90 days.
- 9.16** The Contractor shall be **responsible for the cybersecurity of the entire building network**, including all tenant and corporate systems connected to it.
- 9.17** The Contractor shall align the delivered system to recognised standards such as IEC 62443 (zones and conduits) and the CSA Cybersecurity Code of Practice for CII, where applicable to the Contractor's scope.

— End of Section 9 —

— FACILITATOR KEY — *(try the tender yourself first)*

Suggested triage + posture. The interesting rows are the traps (9.10–9.13, 9.16) and the Clarify slips (9.14, 9.15).

#	Triage	Posture	Why	Pillar / CCoP
9.1	Must-have	Comply	Asset register is our first deliverable.	Visibility · CCoP 4.1
9.2	Must-have	Comply	BMS on its own OT segment; one-way telemetry out.	Network · 5.5 / 10.2.1
9.3	Must-have	Comply	MFA, recorded jump host, request-based — standard.	Applications · 5.7
9.4	Must-have	Comply	Factory passwords changed pre-handover; EOL kit flagged.	Devices · 5.9 / 5.10
9.5	Must-have	Comply	Baseline sequences, restorable backups, change alerts.	Data · 8.1

#	Triage	Posture	Why	Pillar / CCoP
9.6	Must-have	Comply	We provide logs + asset data to their monitoring.	Automation/Visibility · 6.1 / 7.1
9.7	Must-have	Comply	Least privilege, no shared logins, session timeout.	Identity · 5.1 / 5.2
9.8	Nice-to-have	Comply (if scoped)	Real but non-critical — price it, don't over-invest.	—
9.9	Nice-to-have	Comply (if scoped)	Green Mark reporting — cheap value-add.	—
9.10	Red-herring	Not-comply	"100% secure" is indefensible — no one can warrant it. Offer: defence-in-depth + a defined risk posture.	—
9.11	Red-herring	Not-comply / Clarify	CCoP binds the operator (CIIO) , not a product — a product can't be "CCoP-certified." Offer: we design to CCoP-grade controls.	Governance
9.12	Red-herring	Not-comply (+ alt)	A DDC/field controller can't run an AV agent — "Comply" is a lie an auditor catches. Offer: segmentation + monitoring + application whitelisting as compensating controls.	Devices · 10.4
9.13	Red-herring	Not-comply / Clarify	"Quantum-proof" is a marketing red flag. Offer: strong current encryption (TLS, standards-based), crypto-agility.	Data
9.14	Trap	Clarify	Self-contradiction — "permanently disabled" AND "24/7 remote support." Can't be both. Ask the Employer which they want; if remote is permitted it comes with the 9.3 stack.	Applications
9.15	Trap	Clarify	Drafting slip — "eight (12) characters." Which is it? Don't blindly Comply to a contradiction — the expert notices it.	Identity
9.16	Trap	Clarify / Not-comply	Scope over-reach — we secure the BMS segment , not the tenant/corporate networks. Clarify the boundary before pricing, or you own a risk you can't control.	Network
9.17	Must-have	Comply	We design to the same zone-and-conduit, least-privilege principles — here's the map.	All

Teaching points: an eager "Comply" on 9.10–9.13 or 9.16 loses the bid (and creates liability). The wins are the **honest Not-comply + alternative** and the **Clarify** on 9.14–9.16 — that's what makes the salesperson look like the expert. And notice the AI will often "Comply" its way straight through 9.10–9.13 with confident, wrong wording — the **Eloquence Trap**. Verify every posture by hand.

Practice tender for the BMS Cyber-Sales Training. Fictional — safe to paste into AI. Practical Cyber × DACTA × Apexagen.