CCoP & Remote Access — A BMS Vendor's Field Analysis

A Mitsubishi Electric BMS Cyber-Sales advisory · Practical Cyber × DACTA × Apexagen

Grounded in the Cybersecurity Code of Practice for Critical Information Infrastructure — Second Edition, Revision One (CSA, in force from 4 July 2022). Every clause number in this document is quoted from that Code.

How to use this document

Your client sent you a plant network drawing and asked two things: *"What does CCoP actually require of us — clause by clause?"* and *"What remote access is possible, and what does it cost extra?"*

This document answers both, from the seat you actually sit in — the **BMS vendor**, not the auditor.

- **Part 0** — the compliance frame: who CCoP binds, and why the accountability lands on your scope even though you're not the CII owner.
- **Part A** — the full clause map. Every section of the Code, in plain English, with one column that matters to you: *does this touch what ME delivers?*
- **Part B** — the gold-standard network, decoded. Why every box on that drawing maps to a clause — and, crucially, **which boxes are yours to build and price, and which belong to the owner or the system integrator.**
- **Part C** — remote access: the headline question. The real rule (it's stricter than most vendors assume), the ladder of compliant options, and the **cost drivers** for each — so you can scope a quote, not guess a number.
- **Part D** — answer scripts: the lines to say when the client asks, and the tender-clause responses.

> **One handling note.** The reference architecture discussed in Part B is treated **client-neutral** throughout — "a Singapore water-sector CII reference architecture." It's a live critical-infrastructure job; that's how we'd want our own drawings handled, and it loses nothing as a teaching example.

Executive summary — the five things to hold

1. **Your key client is a CII owner ("CIIO"), and CCoP makes them accountable — but they cannot outsource that accountability to you.** Clause **3.8.1** says the owner *"shall remain responsible and accountable for the cybersecurity of the CII even if it engages an external party."* So they discharge

their duty by **pushing controls down to you in the contract** (clause **3.8.3**). Your scope inherits the Code whether or not "CCoP" appears in the spec.

2. **The drawing is the gold standard — comprehensive, and genuinely expensive.** Every element — the segmented layers, the dual firewalls, the data diode, the remote-access broker, the redundant controllers — maps to a specific clause (Part B). It's thorough because a CII must be; none of it is wasted. What *is* true is that **only a slice of it is ME's to deliver** — and knowing which slice is the difference between a priced-right bid and a scope (and cost) you can't hold.
3. **For a CII, on-site is the default and remote is the exception.** This is the single most misread point. Clause **5.1.3** requires that all vendor access to the CII be *"documented and pre-approved, supervised by the CIIO, and performed on-site."* Remote maintenance into the CII is not a given — it must be specifically permitted, risk-assessed, and then wrapped in the full clause **5.7** stack. Promise standing remote access lightly and you'll either overclaim or get disqualified.
4. **When remote access *is* permitted, the bar is concrete** (clause **5.7.2**): disabled unless needed, **multi-factor authentication**, strong encryption **through a secured intermediary** (a jump/bastion host), transmission integrity, malware-scanned uploads, and minimum data flow. Plus privileged access from a **hardened environment** with MFA (**5.3.1**), and telemetry out on a **one-way** path (**5.6.2 / 10.2.1**). That stack is the cost.
5. **BMS is OT, and OT carries its own section.** Section **10** applies specifically to OT CII: one-way data flow off the plant (**10.2.1**), separate OT/enterprise credentials (**10.2.3**), fail-safe behaviour (**10.2.4–10.2.5**), programme-code and firmware integrity (**10.3**), and field-controller hardening (**10.4**). Your controllers, your DDC/PLC programming, and your integrity story are all named in the Code.

Part 0 — The compliance frame

What CCoP is

The **Cybersecurity Code of Practice for Critical Information Infrastructure (CCoP)** is issued by the **Commissioner of Cybersecurity** under **section 11(1)(a) of the Cybersecurity Act 2018**. It is not guidance — it is the **legally binding minimum standard** for owners of designated CII. The current operative version is the **Second Edition, Revision One**, in force from 4 July 2022. It runs to eleven sections plus annex, and roughly 220 auditable clauses.

Who it binds

It binds the **CIIO — the CII owner** — across the essential-service sectors (energy, water, banking & finance, healthcare, transport, infocomm, media, security & emergency services, government). A water-reclamation plant operated for the national water utility is squarely **Water-sector CII**, and — because it monitors and controls physical processes — it is specifically **OT CII** (Section 10 applies).

Why it lands on *your* scope (the cascade)

You are not the CIIO. But three clauses pull you in:

- **3.8.1 — accountability can't be delegated.** The owner stays on the hook even when they hire you. So they *manage* that exposure by contract.
- **3.8.3 — the contract must stipulate your access.** The owner's agreement with you *"shall include terms stipulating the type(s) of access that the external party has to the CII… the obligations of the external party to protect the CII and report incidents… and the CIIO's right to audit the external party's cybersecurity posture."*
- **5.1.3 — your access is constrained by default.** Vendor access is *"documented and pre-approved, supervised by the CIIO, and performed on-site."*

Read together: the tender's cybersecurity section is the owner discharging their CCoP duty onto your scope. Fluency here isn't legal trivia — it's how you avoid disqualification at the security gate and win on trust.

Part A — The full clause map (what each section asks, and whether it's yours)

Legend for the **ME scope** column:
● **Core** — squarely ME's to design/deliver/evidence. ◉ **Partial** — shared; ME contributes evidence, integrates, or supports the owner. ○ **Owner** — the CIIO's duty; ME rarely touches it, but should recognise it.

§2 Audit

Clause	In plain English	ME scope	What ME provides or answers
2.1 Remediation of Audit Findings	The CIIO is audited for CCoP compliance and must remediate findings.	◉	Where an audit flags the delivered BMS, ME remediates on its own equipment and supplies evidence — the practical face of the §3.8.3(c) right-to-audit.

§3 Governance

Clause	In plain English	ME scope	What ME provides or answers
3.1 Leadership & Oversight	Named senior accountability and a governance structure for CII cyber.	○	Fit the owner's governance: named contacts, escalation, evidence on request.
3.2 Risk Management	Assess cyber risk; for OT, include **non-digital engineering/safety hazards** (3.2.3).	◉	Your delivered system is a line in their risk register — supply its risk profile, failure modes, safety interlocks.
3.3 Policies, Standards,	Maintain a policy stack down to procedures.	○	Work to the owner's site policies; hand over your own SOPs for the

Clause	In plain English	ME scope	What ME provides or answers
Procedures			delivered system.
3.4 Security-by-Design	Build security in from the design stage, not bolted on.	●	Design the BMS segmentation-ready, hardened-by-default, least-privilege from day one — and *show* it.
3.5 Cybersecurity Design Principles	Mandatory: **defence-in-depth, least privilege, segregation of duties.** Aspire to defence-by-diversity + **zero trust**.	●	Your architecture must visibly embody these — this is your design credential.
3.6 Change Management	Changes to the CII go through controlled change management.	●	Every change you make post-handover runs through the owner's change control — no silent tweaks.
3.7 Use of Cloud	Cloud services governed and risk-assessed.	◉	Only if your BMS ships cloud analytics / remote dashboards — flag it early; it changes the risk conversation.
3.8 Outsourcing & Vendor Management	Owner stays accountable (3.8.1); keeps oversight (3.8.2); **contract stipulates your access, obligations, audit rights (3.8.3)**; validates your compliance (3.8.4).	●	**This clause is about you.** Expect access-type, incident-reporting and right-to-audit terms in the contract. Be ready to be audited.

§4 Identification

Clause	In plain English	ME scope	What ME provides or answers
4.1 Asset Management	Maintain a complete, current inventory of CII assets — hardware, software, firmware.	●	Your **first deliverable**: a live register of every controller, its firmware version and support/end-of-life status.

§5 Protection

Clause	In plain English	ME scope	What ME provides or answers
5.1 Access Control	Restrict access to authorised parties; **5.1.3 — vendor access documented, pre-approved, supervised, on-site**; 5.1.4 — auto session timeout on inactivity.	●	This governs *how you're allowed to work on their plant.* On-site by default (see Part C).
5.2 Account Management	Least privilege; no unnecessary shared accounts; monitor for anomalies; disable	●	No shared "installer" logins left behind; per-person

Clause	In plain English	ME scope	What ME provides or answers
	inactive; **review all accounts ≥ every 12 months**.		accounts; a handover account list.
5.3 Privileged Access Management	Admin access to selected accounts only; inventory of privileged accounts; **MFA for privileged use/escalation (5.3.1c)**; **privileged access from a hardened environment (5.3.1d)**.	●	Your engineers' admin access = MFA, from a hardened jump box, logged.
5.4 Domain Controller	Harden and protect domain controllers (incl. the Kerberos TGT account).	◉	Only where the BMS relies on Active Directory (the reference drawing shows DC1/DC2).
5.5 Network Segmentation	Segment by security/risk level; **limit inter-segment traffic to the minimum**; be able to **isolate** a segment during an incident.	●	Life-safety and BMS on their own segments; documented flows; an isolation story.
5.6 Network Security	Access-control rules, reviewed periodically; **not connected outside the CII unless necessary**; **one-way data flow where only one-way is needed (5.6.2b)**; internet isolation (5.6.3).	●	Justify every external connection; default to one-way out; no casual internet path.
5.7 Remote Connection	Disabled unless needed; **MFA**; strong encryption **via secured intermediary**; integrity; malware-scan uploads; minimum data flow.	●	**The headline — see Part C.**
5.8 Wireless Communication	No wireless LAN unless needed; if used, authorised + strongly encrypted + authorised devices only.	◉	Only where you propose wireless sensors/links — expect to justify and encrypt them.
5.9 System Hardening	Harden OS/apps; remove defaults and unnecessary services.	●	Every factory default password changed before handover; hardened server/HMI build.
5.10 Patch Management	Acquire, test, install patches on software/firmware.	●	A patchable design and supported firmware; flag any end-of-life kit with a containment plan.
5.11 Portable Devices & Removable Media	Control laptops/USB in the CII.	◉	Your engineers' laptops and USB media on site are in scope — clean, controlled, scanned.

Clause	In plain English	ME scope	What ME provides or answers
5.12 Application Security	Secure the applications running the CII.	●	Your BMS application: authentication, secure config, no hard-coded secrets.
5.13 Database Security	Secure databases holding CII data.	◉	Where you supply the historian/SQL layer.
5.14 Vulnerability Assessment	Periodic vulnerability assessment.	◉	Delivered kit is in scope — support the VA and remediate findings on your equipment.
5.15 Penetration Testing	Periodic penetration testing.	◉	Your delivered system may be a pentest target — expect findings to route back to you.
5.16 Adversarial Attack Simulation	Red-team style simulation.	○	Owner-level; be aware it exists.
5.17 Cryptographic Key Management	Manage cryptographic keys through their lifecycle.	◉	Where your BMS uses certificates/keys (TLS, signing) — a key-handling story.

§6 Detection

Clause	In plain English	ME scope	What ME provides or answers
6.1 Logging	Log security-relevant events, **including remote connections to the CII (6.1)**.	●	Your BMS emits logs in a form their SIEM can ingest — including who connected remotely and what changed.
6.2 Monitoring & Detection	Monitor and detect anomalies; alert; trigger response plans.	◉	Provide the telemetry and the baselines; the owner runs the SOC.
6.3 Threat Hunting	Proactively hunt for threats.	○	Owner-level.
6.4 Cyber Threat Intelligence & Sharing	Consume and share CTI.	○	Owner-level.

§7 Response & Recovery

Clause	In plain English	ME scope	What ME provides or answers
7.1 Incident Management	A Cybersecurity Incident Response Plan and CIRT; thresholds; evidence preservation.	◉	Support their IR: reachable contacts, logs, asset data, and preserve state before you “fix” during an incident.
7.2 Crisis Communication Plan	Plan for crisis communications.	○	Owner-level.
7.3 Cybersecurity Exercise	Run cyber exercises.	◉	You may be asked to participate for the systems you delivered.

§8 Cyber Resiliency

Clause	In plain English	ME scope	What ME provides or answers
8.1 Backup & Restoration Plan	Backups that can actually be restored.	●	Baseline critical sequences/setpoints; restorable configuration backups; alert on change.
8.2 Business Continuity & Disaster Recovery	Continuity and recovery of essential service after disruption.	◉	Support recovery of the BMS to a defined state within the owner’s RTO/RPO.

§9 Cybersecurity Training & Awareness

Clause	In plain English	ME scope	What ME provides or answers
9.1 Awareness Programme	Security awareness for CII staff.	○	Owner-level (your own staff competency is governed via 3.8/5.1).
9.2 Training & Skills	Role-specific cyber skills for CII staff.	○	Owner-level.

§10 Operational Technology (OT) Security — *applies specifically to OT CII (BMS is OT)*

Clause	In plain English	ME scope	What ME provides or answers
10.1 Application	This section applies to CII that are OT systems.	—	Confirms the plant BMS is in Section 10’s scope.
10.2 OT Architecture & Security	OT not on enterprise net except **one-way OT→enterprise (10.2.1)**; monitor those flows (10.2.2); **separate OT/enterprise credentials (10.2.3)**; **fail-safes (10.2.4)**; physical-process baselines + fail-safe on deviation (10.2.5); **SIS**	●	Architect the BMS this way: one-way telemetry out, distinct OT logins, fail-safe on anomaly,

Clause	In plain English	ME scope	What ME provides or answers
	isolated to authorised field devices (10.2.6); replace legacy where possible (10.2.7).		safety system ring-fenced.
10.3 Secure Coding	**Verify firmware integrity (10.3.1)** and **programme-code integrity (10.3.2)**; **interlocks in fail-safe controllers (10.3.3)**; **input validation (10.3.4)**; **no unauthorised code/value changes (10.3.5)**; register-block separation (10.3.6); modularise code (10.3.7).	●	Your DDC/PLC programming is named here — integrity checks, interlocks, validated inputs, change control on logic.
10.4 Field Controllers	**Separate comms module to external nets (10.4.1a)**; authenticate data transmission (10.4.1b); prevent unauthorised writes (10.4.1c); safe fault-state comms (10.4.1d); password protection (10.4.1e); investigate all alerts (10.4.2); **monitor for alert suppression (10.4.3)**; **operational baselines — cycle time, uptime, memory (10.4.4)**.	●	Your controllers must authenticate, refuse rogue writes, protect against alert suppression, and run to a monitored baseline.

§11 Domain-Specific Practices

Clause	In plain English	ME scope	What ME provides or answers
11.2 DNSSEC	Enable DNSSEC validation where DNS is used.	○	Owner-level unless your BMS resolves DNS.

Reading the column: the **●-Core** rows are your bid. Governance (§3.4, §3.5, §3.8), the whole access/network/hardening cluster (§5.1–5.3, §5.5–5.7, §5.9–5.10, §5.12), asset management (§4.1), logging (§6.1), backup (§8.1), and **the entire OT section (§10)** are where ME is measured. The **○-Owner** rows you *recognise* so you can speak to them — but you don't price them.

Part B — The gold-standard network, decoded

Here is the reference architecture in words, kept client-neutral — read top (least trusted) to bottom (the physical process). The clause each layer answers is in the table just below.

```
least trusted   ↑ external
┌─ CSM    monitoring net · DATA DIODE → SOC
├─ DMZ    proxy · REMOTE-ACCESS broker
├─ PMN    servers · domain controllers · historian
├─ PAN    redundant automation ring
└─ FIELD  control + standby · RIO · package PLCs
most trusted    ↓ physical process
```

Every box → its clause → whose scope

Element on the drawing	The clause it satisfies	Whose scope
Five separated layers (CSM / DMZ / PMN / PAN / field), following the Purdue model	**5.5** Network Segmentation; **10.2.1** OT not on enterprise net	SI / owner (architecture); **ME conforms** the BMS to it
Dual firewalls at each boundary	**5.6** Network Security	SI / owner
Data diode (one-way out to the monitoring net)	**5.6.2(b)** one-way flow; **10.2.1** one-way OT→enterprise	SI / owner
Cyber-Security-Monitoring net with log servers, EDR/EPM	**6.1** Logging; **6.2** Monitoring & Detection	Owner (SOC); **ME feeds logs**
Remote-access server in the DMZ, behind proxy + firewalls	**5.7** Remote Connection (the "secured intermediary")	Owner-provided path; **ME uses it, doesn't own it**
Proxy server / brokered access	**5.7.2(c)** secured intermediary	Owner / SI
Domain controllers (DC1/DC2), patch server/WSUS	**5.4** Domain Controller; **5.10** Patch Management	Shared — **ME where the BMS uses them**
Historian + historian mirror, SQL nodes	**5.13** Database Security; **8.1** Backup	◉ ME where supplied
Control **+ Standby** controllers, **PRP** dual-path switches	**3.5** defence-in-depth; **10.2.4** fail-safe	● **ME** (the BMS control layer)
RIO racks, HMIs, package PLCs at field level	**10.3** Secure Coding; **10.4** Field Controllers	● **ME**
Separate OT vs enterprise credentials	**10.2.3**	● **ME** (BMS accounts)

The verdict for the client

This is the gold standard for a Water-sector OT CII — thorough, and genuinely expensive to build and run. Each element earns its place against a clause; none of it is wasted. But two things are worth saying plainly to the client:

1. **Most of the heavy infrastructure — the diode, the DMZ, the firewalls, the monitoring net, the remote-access broker — is the owner's / system integrator's scope, not the BMS vendor's.** ME conforms to it; ME doesn't build the whole thing. Pricing the BMS as if it must deliver the entire CII stack is how a bid gets mis-scoped.
2. **ME's slice is specific and defensible:** a segmentation-ready, hardened, least-privilege BMS (§3.4, §3.5, §5.5, §5.9); an asset register (§4.1); secure controller programming with integrity, interlocks and validated inputs (§10.3); hardened field controllers that refuse rogue writes and run to a monitored baseline (§10.4); one-way telemetry out (§10.2.1); restorable config backups (§8.1); and logs the SOC can use (§6.1). *That* is the winning, priceable scope.

Part C — Remote access: what's possible, and what it costs extra

The rule, stated correctly

Most vendors assume "remote access + VPN + MFA = compliant." For a CII that's only half the picture, and the missing half is the expensive half.

The stack that actually governs remote maintenance of a CII:

1. **Default position — on-site (5.1.3).** *All* vendor access to the CII shall be **documented and pre-approved, supervised by the CIIO, and performed on-site.** For the CII itself, on-site supervised access is the baseline, not remote.
2. **Remote is the exception, and it's disabled by default (5.7.2a).** Remote connections are *disabled except where necessary for operating the CII.* So remote vendor access exists only where the owner specifically decides it's necessary, risk-assesses it, and permits it in the contract (**3.8.3a** — access type must be stipulated).
3. **When permitted, the full 5.7.2 controls apply:**
   - **(b) Multi-factor authentication** to establish the connection.
   - **(c) Strong encryption, through a secured intermediary** — i.e., a **jump server / bastion host** (the Code names these).
   - **(d) Transmission security and message integrity.**
   - **(e) Uploads malware-scanned** before they reach the CII.
   - **(f) Data flow limited to the minimum** for the task.
4. **Privileged actions are stricter still (5.3.1):** MFA for privileged use/escalation, and privileged access initiated **from a hardened environment**.
5. **Telemetry leaves one-way (5.6.2b / 10.2.1):** monitoring data flows *out* of the OT plant on a one-way path (the data diode) — never a two-way tunnel into the process.
6. **It's all logged (6.1):** remote connections are explicitly a logged event class.

> **The honest one-liner for the client:** *"For your CII, on-site supervised access is the default the Code assumes. Remote support is possible, but it's something you choose to permit and risk-assess — and once you do, it comes wrapped in MFA, a hardened jump host, session control and one-way monitoring. We design our support model to fit whichever you choose."*

The options ladder — and the cost drivers

Costs below are given as **drivers**, not dollar figures — the actual price depends on the owner's existing infrastructure, headcount, and SLA. **A firm number needs a quote against the specific site.** What follows lets you scope that quote and explain the trade to the client.

Cost-driver key: **CAPEX** (one-time kit), **LICENSE** (recurring software/subscription), **INTEG** (one-time engineering/integration), **OPEX** (recurring running/labour cost).

Tier 0 — On-site only + one-way telemetry out *(the CCoP default)*
- **What it is:** No remote path into the CII. Engineers attend site, supervised, pre-approved (5.1.3). Health/telemetry leaves via the owner's one-way diode (5.6.2b / 10.2.1) so ME can *see* status without a route *in*.
- **Clauses satisfied:** 5.1.3, 5.7.2(a), 5.6.2(b), 10.2.1 — fully, by construction.
- **ME scope vs owner:** ME supplies the BMS + telemetry feed; the diode/monitoring net is the owner's.
- **Cost drivers:** ↑↑ **OPEX** (truck rolls, engineer day-rates, travel, slower response); low cyber CAPEX. The cost is *operational*, not technical.
- **When to recommend:** highest-sensitivity plants; owners who want zero inbound path. **Lowest cyber risk, lowest kit cost, highest running cost.**

Tier 1 — Ride the owner's remote-access rig *(client-owned VPN + MFA + shared jump host)*
- **What it is:** The owner already operates a compliant remote-access broker (the "Remote-Access server" in the DMZ on the reference drawing). ME requests time-boxed access through *their* path when needed.
- **Clauses satisfied:** 5.7.2(b–f), 5.3.1 — via the owner's existing controls.
- **ME scope vs owner:** Owner owns the rig; **ME's cost is process, not hardware.**
- **Cost drivers:** low CAPEX/LICENSE for ME; modest **INTEG** (onboarding to their PAM/jump host, account provisioning); **OPEX** = per-session request/approval overhead. Best value where the owner is already built out.
- **When to recommend:** mature CII owners (most designated plants). **The usual answer for a well-built site.**

Tier 2 — ME-supplied hardened jump host + MFA + session logging
- **What it is:** Where the owner lacks a broker, ME proposes a dedicated, client-approved **bastion/jump host** in the DMZ: MFA, encrypted, session-logged, request-based access; no standing tunnel.
- **Clauses satisfied:** 5.7.2(b–f), 5.3.1(d) hardened environment, 6.1 logging.
- **ME scope vs owner:** ME supplies + hardens the jump host; owner approves placement and firewall rules.
- **Cost drivers: CAPEX** (appliance/host) + **INTEG** (hardening, firewall integration, sign-off) one-time; modest **LICENSE** (MFA); **OPEX** (patching + periodic access review, 5.2.2 / 5.6.1).
- **When to recommend:** owners without their own broker who still want remote support. **Mid-tier; a concrete line item you can quote.**

Tier 3 — Privileged Access Management (PAM) with full session recording
- **What it is:** A PAM platform (CyberArk / BeyondTrust-class): credential vaulting, **just-in-time** access, full **session recording**, no shared or standing credentials. Directly answers "prove who connected and what they changed."
- **Clauses satisfied:** 5.3.1(a–d) in full, 5.7.2, 5.2.1 (no shared accounts), 6.1 (rich session logs).
- **ME scope vs owner:** usually **owner-owned** enterprise platform; ME integrates its accounts and workflow into it.
- **Cost drivers:** ↑ **LICENSE** (per-admin/subscription, the dominant cost), **INTEG** (integration), **OPEX** (session-review labour). Highest software cost of the tiers.
- **When to recommend:** owners with strict audit needs or many vendors. **Strongest evidence story; highest licensing cost.**

Tier 4 — Full DMZ + proxy + data-diode + broker pattern *(the reference drawing)*
- **What it is:** The complete pattern on the client's SAD — remote-access server + proxy in a DMZ, one-way diode to the monitoring net, dual firewalls, SOC integration.
- **Clauses satisfied:** the whole Protection + Detection + OT set — 5.5, 5.6, 5.7, 6.1, 6.2, 10.2.1.
- **ME scope vs owner: overwhelmingly owner / system-integrator scope.** ME integrates the BMS into it; ME does not build it.
- **Cost drivers:** ↑↑ **CAPEX** (diode, firewalls, DMZ hosts) + ↑↑ **INTEG** + **OPEX** (SOC). This is a plant-infrastructure programme, not a BMS line item.
- **When to recommend:** it's the owner's architecture decision. **ME's honest position: "we conform to it; it isn't ours to price."**

The "who pays for what" split (say this out loud)

Layer	Typically ME's cost	Typically the owner's / SI's cost
Segmentation-ready, hardened BMS	● design & build	—
Secure controller programming (§10.3/10.4)	●	—
Asset register, config backups, logs	●	—
Jump host / bastion (Tier 2)	● if ME supplies	○ if owner supplies
PAM platform (Tier 3)	◉ integration only	● licence & platform
DMZ, firewalls, **data diode**, SOC (Tier 4)	—	●

> **The mis-scope trap:** if a client waves the gold-standard drawing and asks "can you do all this?", the wrong answer is a yes that quietly prices the whole CII stack into a BMS bid. The right answer separates **the BMS scope you own and price** from **the plant-security infrastructure the owner/SI provides** — and shows you know exactly where the line is. That precision *is* the credential.

Part D — The answer scripts

When the client asks "what remote access can you give us?"

> *"For a CII, the Code's default is on-site, supervised, pre-approved access — so we don't assume a standing remote path. If you decide remote support is worth permitting, we run it request-based: multi-factor, through a hardened jump host you approve, session-logged, with monitoring flowing out one-way only. We'll fit your existing remote-access broker if you have one, or supply a hardened one if you don't. Either way, you can always show your auditor exactly who connected and what changed."*

When the client asks “is all this necessary — isn’t it a lot?”

> *“It’s the gold standard for a Water-sector CII — every layer maps to a clause, so none of it is wasted. It’s also genuinely expensive, and most of that infrastructure is your / your integrator’s to build, not ours. Our part is the BMS done to the same bar — hardened, segmented, securely programmed, with the asset register, backups and logs your CCoP audit will ask for. We’ll help you spend where it counts and not gold-plate our scope.”*

Tender-clause quick responses (carry CCoP as a credential)

Clause you’ll meet (typical wording)	The winning answer
“Remote access shall require MFA and be logged.”	“All remote support is per-engineer, MFA, through a recorded jump host — request-based, never a standing back-door (5.7.2, 6.1).”
“Vendor access shall be controlled, time-limited and auditable.”	“On-site by default (5.1.3); where you permit remote, it’s time-boxed, session-recorded, and fully attributable.”
“OT shall be segmented from enterprise/corporate networks.”	“BMS sits on its own OT segment; telemetry leaves one-way only — nothing routes back into the process (5.5, 10.2.1).”
“A complete asset inventory shall be provided and maintained.”	“Our first deliverable — a live register of every controller, firmware and support status (4.1).”
“Default credentials changed; unsupported firmware identified.”	“Every factory password changed before handover; end-of-life kit flagged with a containment plan (5.9, 5.10).”
“Critical setpoints backed up and change-monitored.”	“We baseline the sequences, alert on change, and keep restorable backups (8.1, 10.4.4).”
“Field controllers shall be secured against unauthorised modification.”	“Integrity-checked programme code, interlocks, validated inputs, no unauthorised writes (10.3, 10.4).”
“Systems shall align to CSA CCoP / IEC 62443.”	“We design to the same zone-and-conduit, least-privilege, defence-in-depth principles these require — here’s the map.”

The precision guardrail (this *builds* trust)

Know **exactly** who CCoP binds. Don’t tell a non-CII commercial landlord “you’re legally mandated to comply” — they’re not, and a savvy buyer will check. For CII clients, be precise about which clause drives which control. **Every claim you make, you must be able to defend** — that’s Decision Survivability applied to the security gate.

Appendix — Verified section index & source

Full section structure (CCoP for CII, 2nd Edition, Rev 1):

- **1** Preliminary (citation, glossary & interpretation, compliance dates)
- **2** Audit Requirements — 2.1 Remediation of Audit Findings

- **3** Governance — 3.1 Leadership & Oversight · 3.2 Risk Management · 3.3 Policies/Standards/Guidelines/Procedures · 3.4 Security-by-Design · 3.5 Cybersecurity Design Principles · 3.6 Change Management · 3.7 Use of Cloud · 3.8 Outsourcing & Vendor Management
- **4** Identification — 4.1 Asset Management
- **5** Protection — 5.1 Access Control · 5.2 Account Management · 5.3 Privileged Access Management · 5.4 Domain Controller · 5.5 Network Segmentation · 5.6 Network Security · 5.7 Remote Connection · 5.8 Wireless Communication · 5.9 System Hardening · 5.10 Patch Management · 5.11 Portable Computing Devices & Removable Storage Media · 5.12 Application Security · 5.13 Database Security · 5.14 Vulnerability Assessment · 5.15 Penetration Testing · 5.16 Adversarial Attack Simulation · 5.17 Cryptographic Key Management
- **6** Detection — 6.1 Logging · 6.2 Monitoring & Detection · 6.3 Threat Hunting · 6.4 Cyber Threat Intelligence & Information Sharing
- **7** Response & Recovery — 7.1 Incident Management · 7.2 Crisis Communication Plan · 7.3 Cybersecurity Exercise
- **8** Cyber Resiliency — 8.1 Backup & Restoration Plan · 8.2 Business Continuity Plan & Disaster Recovery Plan
- **9** Cybersecurity Training & Awareness — 9.1 Awareness Programme · 9.2 Training & Skills
- **10** Operational Technology (OT) Security — 10.1 Application · 10.2 OT Architecture & Security · 10.3 Secure Coding · 10.4 Field Controllers
- **11** Domain-Specific Practices — 11.1 Application · 11.2 DNSSEC
- **Annex A** Guidance for Strengthening Organisational Cybersecurity Posture

Source & version. Cyber Security Agency of Singapore, *Cybersecurity Code of Practice for Critical Information Infrastructure — Second Edition, Revision One*, issued under s.11(1)(a) Cybersecurity Act 2018; in force from 4 July 2022. Obtained from the CSA Codes of Practice page (csa.gov.sg/legislation/codes-of-practice). A copy of the source PDF is held at `reference/ccop/` alongside this advisory.

Currency note. The **Cybersecurity (Amendment) Act 2024** (in force from October 2025) extended CSA's oversight to third-party-owned CII, cloud service providers and data-centre operators. Confirm the operative Code edition and any sector-specific overlay (e.g. the water utility's own OT security requirements) with the client before making a formal compliance claim in a tender.

---

*Prepared for the Mitsubishi Electric BMS Cyber-Sales engagement. Companion drills at **bms.ethanseow.com**. Practical Cyber × DACTA × Apexagen.*