Dragon Advance Tech

Sample Computer-System Security Management Plan

HarborLink Marine Transport Authority (HMTA)

Critical Infrastructure – Maritime Operations & Vessel Traffic Management Systems (VTMS)

Prepared by: Cyber Assurance Team
Date: 1 December 2025
Version: 1.1
Classification: CONFIDENTIAL

Table of Contents

Executive Summary

HarborLink Marine Transport Authority (HMTA) manages mission-critical systems for vessel traffic monitoring, navigation safety, and maritime coordination. It supports Hong Kong's marine transport operations, including vessel traffic control, berth assignment, marine communication networks, and safety-critical navigation systems.

As a designated critical infrastructure operator, HMTA maintains strict security governance to ensure the availability, integrity, and confidentiality of all IT and OT systems supporting maritime operations.

This plan details the security management activities for the HMTA computer system, carried out in accordance with Ordinance Cap. 653 and guided by the code of practice (CoP) controls 6.2.5–6.2.27, which should follow a structured approach.

After completing the risk assessment of the identified critical computing systems (CCSs), the computer-systems security management unit (CSSMU) must address gaps in the security policies aligned with the CoP to implement the mandatory controls.

1. Governance and Responsibilities

HMOC's governance structure aligns with the Ordinance requirements:

- Accountable Officer (AO): Director of Marine Transport Systems
- Responsible Officer (RO): CISO
- System Owners: Assigned per CCS
- Computer-Security Management Unit (CSSMU): Representatives from IT, OT, Risk, Compliance, and Marine Operations

Roles and responsibilities were reviewed in Q4 2025 and remained consistent throughout the reporting year.

2. Scope

Assessment covers:

- Critical Computer Systems (CCS) are identified through the internal CCS designation process.
    - CCS-1: Vessel Traffic Management System (VTMS) (Fig. 1)
    - CCS-2: Marine Communication and Digital Signaling System
    - CCS-3: Port Operations Scheduling & Berth Allocation Platform
    - CCS-4: OT-Integrated Radar & AIS Sensor Network
    - CCS-5: Emergency Maritime Operations Centre (EMOC) System
- Coverage of the IT and OT domains impacting marine transport infrastructure
- Control Framework CoP 6.2.5 – 6.2.27 aligned with ISO 27001 & IEC 62443
- Assessment Methods: Documentation review, technical assessment, interviews, log sampling, and configuration review.

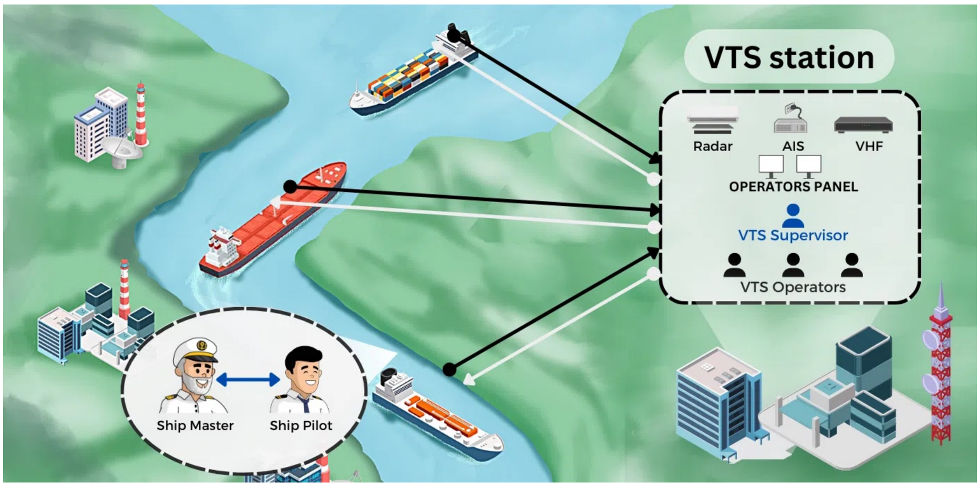

Fig. 1 Vessel Traffic Management System

3. Policies & Guidelines (Cap. 653 Compliance)

3.1 Policies for Identifying, Assessing, Monitoring, Responding to, and Mitigating Risks, Vulnerabilities, Security Threats, and Incidents

A1. Risk Identification & Assessment

- HMTA adopts a hybrid approach aligned with:
  - ISO 27005
  - IEC 62443-3-2 (risk for OT)
- Conduct an annual enterprise-wide risk assessment that includes:
  - Vulnerability assessments for network segments, OT systems, sensors, AIS receivers, and vessel traffic platforms.
  - Business impact assessment for the loss of VTMS availability.
- Maintain a Risk Register updated quarterly
- Detailed policies and procedures are included in a separate document.

A2. Vulnerability Management

- Weekly automated scans (Nessus/Qualys equivalent).
- Prioritized remediation based on CVSS scores.
  - Critical: ≤ 72 hours
  - High: ≤ 14 days
  - Medium: ≤ 30 days.
- Manual review of OT assets (CCS-2 & CCS-5) and the communication protocols (Radar, AIS, VHF), where scanning may impact operations.

A3. Threat Monitoring

- Subscription to marine-sector cyber intelligence feeds[1] (e.g., GPS spoofing advisories, AIS manipulation campaigns).
- Correlating real-time logs with SIEM through anomaly-detection algorithms.

A4. Incident Response & Mitigation

- 24/7 SOC and Cybersecurity Incident Response Team (CSIRT)
- Incident Response Plan aligned with CoP 7.2.3:
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Post-incident review

[1] https://threatscene.com/blog-update/rogue-waters-why-maritime-cyber-attacks-are-surging-in-2025/

- Mandatory reporting to the regulator within the required time frames, CoP 7.3.8 (Serious incidents: within 12 hours).

3.2 Detecting Computer-Security Threats & Incidents

B1. Detection Framework (CoP 6.2.26)

HMTA uses multiple layers of detection measures.

- Security Information and Event Management (SIEM) monitors all critical logs (AD, firewall, VTMS servers, OT: AIS communication relays & sensors).
- Intrusion Detection Systems (IDS):
  - Network IDS: Monitors port-core and vessel-traffic networks.
  - Host IDS/EDR: Deployed on all critical servers and terminals.
- Anomaly Detection: AI-based models identify unusual AIS traffic patterns or spoofing attempts in the VHF maritime mobile band: 161.975 MHz (AIS 1) and 162.025 MHz (AIS 2)
- Integrity Monitoring: OT integrity control for configuration drift on PLCs and radar controllers.
- Alarms & Trigger Rules:
  - Unauthorized privileged login
  - Sudden spike in AIS message frequency
  - OT network packet anomalies
  - Malicious inbound connections from unusual geolocations

3.3 Controlling Access and Preventing Acts Without Lawful Authority

C1. Access Control Policies (CoP 6.2.10 & CoP 6.2.18)

- Multi-Factor Authentication (MFA) for:
  - All administrative accounts
  - Remote connections.
- Least Privilege Enforcement: Role-based access for marine traffic controllers, IT operators, and port-logistics officers.
- Privileged Access Management (CoP 6.2.11):
  - Time-based privilege elevation
  - Fully recorded sessions
- Physical Access Controls (CoP 6.2.14):
  - Card and biometric access control for rooms and data centers
  - Surveillance with a 180-day retention period
- Network Segmentation: Separation of (CoP 6.2.21):
  - Corporate IT network
  - OT vessel traffic network
  - AIS/GPS sensor network

3.4 Ensuring Changes Are Overseen, Managed & Controlled

D1. Change Management Process (CoP 6.2.20–6.2.21)

- All changes require:
    - Formal change request
    - Security impact assessment
    - CSMC approval for major changes.
- Types of changes:
    - Routine, Emergency, Major System Upgrade
- Mandatory testing in a segregated staging environment for:
    - VTMS software updates
    - Firmware updates for radars, AIS transponders, and PLCs
- Post-implementation validation must be completed within an acceptable risk period.

3.5 Securing, Managing & Controlling All Components

E1. Configuration Management (CoP 6.2.15)

- Hardened baseline configuration for all servers and controllers.
- Continuous monitoring for unauthorized changes using:
    - OT configuration integrity tools
    - File integrity monitors
- Encryption (CoP 6.5.4):
    - AES-256 for data at rest
    - TLS 1.3 for data in transit
    - Secure key management using HSM

E2. Patch Management (CoP 6.2.17)

- Monthly patch cycle for IT systems.
- Quarterly risk-approved patch cycle for OT systems with operational constraints.

3.6 Security Integration Throughout the System Development Life Cycle (SDLC)

F1. Secure SDLC Framework (CoP 6.2.8, CoP 6.2.22)

- Security by Design principles embedded from initiation:
    - Static application security testing (SAST) during development
    - Dynamic security testing (DAST) before deployment
- Mandatory code review by two independent security engineers.
- Security gates at:
    - Requirements phase
    - Design phase
    - Pre-production
    - Go-live

3.7 Ensuring Availability During Disruption

G1. Business Continuity & Disaster Recovery (CoP 7.2.4)

- Redundant VTMS Control Centers are located in separate fire zones.
- Active-standby failover for:
  - Radar data servers
  - AIS gateway servers
  - Navigation safety systems
- Recovery Point Objective (RPO): 15 minutes
- Recovery Time Objective (RTO): 2 hours
- Monthly failover drills and annual resilience stress tests.

3.8 Managing Contracts With Suppliers to Ensure Compliance

H1. Supply Chain Security (CoP 6.2.25)

- All suppliers must meet:
  - Cybersecurity clauses in contracts
  - Secure coding and maintenance obligations
- Security assessment for:
  - OT hardware vendors
  - AIS data service providers
  - System integrators
- Contractors must undergo:
  - Background checks
  - Annual security training
- Mandatory reporting of third-party breaches within 48 hours.

3.9 Reviewing the Computer-Security Management Plan

I1. Annual Review & Audit (CoP 6.2.27)

- The CSSMP is reviewed:
  - Annually by the CISO office
  - After major incidents
  - After significant technology changes
- An independent external audit is conducted every 24 months.
- All findings are recorded in the CSSMP Improvement Register with designated owners and deadlines.

4. Policies Mapped to the Code of Practice

Below is a comprehensive section-by-section report, including control objectives, HMTA implementations, examples, gaps, and recommendations.

Code of Practice	InfoSec Controls	In Compliant
6.2.5 Computer-System Security Management Unit	F.1: A.5 Organizational Controls	Compliant
6.2.6 Policies, Standards and Guidelines		Planned Q1 2026
6.2.7 Computer-System Security Risk Management Approach		Planned Q1 2026
6.2.8 Security by Design	F.4: A.8.25 Secure Development	Compliant
6.2.9 Asset Management		planned Q1 2026
6.2.10 Access Control and Account Management	F.4: A.8.5 Secure Authentication	Partial Q1 2026
6.2.11 Privileged Access Management	F.4: A.8.2 Privileged Access Rights	Compliant
6.2.12 Cryptography	F.4: A.8.24 Cryptographic Controls	Compliant
6.2.13 Password Management		Planned Q1 2026
6.2.14 Physical Security	F.3: A.7 Physical Controls	Compliant
6.2.15 Configuration Management and System Hardening	F.4: A.8.9 Configuration Management	Compliant
6.2.16 Change Management		Planned Q1 2026
6.2.17 Patch Management		Alternative OT control
6.2.18 Remote Connection		Alternative OT control
6.2.19 Storage Media		Alternative OT control
6.2.20 Backup and Recovery	F.4: A.8.13 Information Backup	Compliant
6.2.21 Network Security		Planned Q2 2026
6.2.22 Application Security	F.4: A.8.28 Secure Coding	Partial Q2 2026
6.2.23 Log Management	F.4: A.8.15 Logging	Compliant
6.2.24 Cloud Computing Security		Alternative OT control
6.2.25 Supply Chain Management		Alternative OT control
6.2.26 Monitoring and Detection	F.4: A.8.16 Monitoring Activities	Compliant
6.2.27 Computer-System Security Training		Alternative OT control

5. Key Performance Indicators (KPIs)

Below is a list of KPIs for the CSSMP 2025 reviews:

Area	KPI	Target	2025 Result
Vulnerability Remediation	Critical vulnerabilities patched	≤ 48 hrs	94% compliance
Incident Response	Detection-to-containment time	< 30 min	Avg. 22 min
Availability	VTMS uptime	≥ 99.97%	99.985%
Change Management	Unauthorized changes	0	0
Supplier Compliance	Supplier audits passed	100%	100%

6. Major Activities for the Year

- Completion of OT/IT network segmentation enhancement.
- Replacement of outdated AIS receiver hardware.
- Successful execution of port-wide cyber-drill simulating an AIS spoofing attack.

7. Improvement Plan (2026)

Task	Target Date	Owner
Replace microwave link with encrypted IP radio	Q3 2026	OT Engineering
Onboard all vendor accounts to PAM	Q1 2026	Cybersecurity
Centralize radar logs	Q2 2026	ICS Network Team
Replace unsupported OT devices	Q3 2026	Procurement & Operations

8. Conclusion

HMTA remains fully aligned with the requirements of Cap. 653. The organization has implemented comprehensive controls that safeguard the operational integrity of maritime traffic services, maintain high resilience levels, and ensure that both IT and OT systems are protected against evolving cyber threats.

The security program will continue to evolve with improvements to monitoring capabilities, supply-chain assessments, and automated anomaly detection for maritime navigation data.

Appendix A - Sample Information Security Plan

A.1 Purpose

This Information Security Plan establishes the framework, security controls, governance structure, and protection mechanisms required to safeguard the information assets and Critical Computer Systems (CCS) of the HarborLink Marine Transport Authority (HMTA).

The plan aligns with:

- ISO/IEC 27001:2022
- IEC 62443 for OT systems

BFig. 1 Vessel Traffic Management System

A.2 Information Security Objectives

HMTA defines the following objectives:

- Ensure availability of CCS uptime ≥ 99.98%
- Reduce cyber risks. Residual risk rating: High → Medium or below
- Improve OT security hygiene. Completion of OT hardening 100% of priority assets by Q4
- Strengthen monitoring, Log coverage 95% log centralization
- Enhance workforce cybersecurity Training completion for 100% staff annually
- Objectives are reviewed quarterly by the Cybersecurity Steering Committee.

A.3 Governance Structure

HMTA defines the Roles and Responsibilities:

- Accountable Officer (AO): Director of Marine Transport Systems
- Overall accountability for information security and compliance
- Responsible Officer (RO): Head of Cybersecurity & Technology Risk
- Oversees implementation of the ISP, policies, and security controls
- System Owners (SO): Assigned for each CCS
- IT Operations Team
- OT Engineering Team
- Internal Audit

A.4 Risk Management Framework

HMTA follows a hybrid methodology aligned with:

- ISO 27005
- IEC 62443-3-2 (risk for OT)
- Government SRAA methodology.

Risk Assessment Frequency:

- CCS: Annual + upon significant change
- Non-CCS: Every 2 years.

Example Risks

- Risk Likelihood Impact Residual Risk Controls
- Cyber intrusion into VTMS Medium Critical Medium Segmentation, MFA, monitoring
- AIS spoofing attack, High Major Medium, Data validation, anomaly detection
- OT sensor firmware tampering Medium Major Medium Firmware signing, physical.

A.5 ISO 27001 Controls Implementation

As of 2025, HMTA has partially adopted 27001 controls:

F.1 A.5 Organizational Controls

A.5.2 Information Security Roles and Responsibilities

Implementation:

- ➢ HMTA Information Security Policy v1.3, approved by AO (Mar 2025)
- ➢ Mandatory annual policy acknowledgement for all employees.

F.2 A.6 People Controls

A.6.3 Information Security Awareness & Training

Implementation:

- ➢ Annual cybersecurity training covering OT threats, phishing, and maritime-specific risks.
- ➢ Specialized scenario drills:
  - o AIS spoofing event simulation
  - o VTMS ransomware incident drill.

F.3 A.7 Physical Controls

A.7.1 Physical Security Perimeter

Implementation:

- EMOC, Radar towers, and coastal sensor stations are defined as Level 3 Restricted Zones
- Access controlled by smartcards + biometric verification
- Physical barriers were added in 2025 after a threat assessment.

A.7.5 Protecting Against Environmental Threats

Implementation:

- AIS towers are equipped with lightning arresters and surge protectors.
- Active temperature alarms in marine server rooms.

F.4 A.8 Technical Controls

A.8.2 Privileged Access Rights

Implementation:

- CyberArk vault for privileged credentials.
- All CCS administrator accounts require:
- MFA
- Just-in-time access
- Session recording
- Privileged actions are reviewed daily.

Example:

- On 2025-06-18, PAM detected an unauthorized attempt to escalate privileges on the VTMS test server; it was automatically blocked.

A.8.5 Secure Authentication

Implementation:

- CIS benchmarks applied to Windows and Linux CCS servers.
- OT hardening includes:
- Disabling unused serial ports
- Blocking unauthorized USB devices
- Enforcing signed firmware on.

Example deviation:

- AIS device model AIS-TX17 cannot disable Telnet; compensating control: ACL restriction and SIEM monitoring.

A.8.9 Configuration Management

Implementation:

- IT CCS: Monthly patch cycle
- OT CCS: Semi-annual patch cycle with operational safety review
- Emergency patching allowed for critical CVEs.

Example:

- CVE-2025-30111 affecting the VTMS interface library has been patched within 48 hours.

A.8.15 Logging

Implementation:

- SIEM collects logs from VTMS, OT firewalls, and communication servers.
- OT Syslog relays are installed to avoid direct sensor-to-SIEM connections.

Example alerts monitored:

- Unusual AIS packet patterns
- Failed privileged login attempts.

A.8.24 Cryptographic Controls

Implementation:

- AES-256 for data at rest
- TLS 1.2+ for all transmission channels
- Key rotation every 6 months.

A.8.25 Secure Development

Implementation:

- AES-256 for data at rest.
- CCS-3 (Berth Allocation System) uses a DevSecOps pipeline with:
- SAST (CodeQL)
- DAST
- Dependency vulnerability checks
- Secure coding guidelines.

Example alerts monitored:

- 13 high-risk vulnerabilities were remediated during the May 2025 sprint.

A.8.16 Monitoring Activities

Implementation:

- 24×7 SOC monitoring.
- Integration with OT anomaly detection (e.g., radar signature deviation detection)
- Weekly review of security alerts.

A.8.13 Information Backup

Implementation:

- Daily incremental + weekly full backups
- Offline vault (immutable storage) for CCS data
- Quarterly restore tests.

Example:

- Successful VTMS database restore test performed on 2025-09-27.

A.8.28 Secure Coding

Example:

- Static analysis rules enforced for:
- Input validation
- Memory safety
- Maritime protocol handling (AIS, NMEA)
- Developers trained on secure handling of marine data formats.

A.6 Third-Party and Supply Chain Security

Third-Party Controls Implemented:

- Security clauses in OT vendor contracts.
- Annual assessment of AIS/Radar vendors.
- Secure remote access required (MFA, time-bound, monitored).

A.7 Business Continuity & Disaster Recovery

Implementation Examples:

- EMOC failover site is operational with a 10-minute switchover
- VTMS hot-standby replication with 10-second lag
- Disaster recovery exercises are conducted annually.

A.8 Incident Response

Implementation Examples:

- Incident Response Plan aligned with Ordinance 653.
- Reporting to the Commissioner within the statutory timeframe.
- Runbooks for:
- VTMS outage
- AIS spoofing
- Marine cyber-attack scenarios.

A.9 Continuous Improvement

Implementation Examples:

- Quarterly management review
- Annual internal audit
- Corrective actions tracked in the ISMS workflow system
- OT-specific improvement roadmap created for 2026.