Dragon Advance Tech

Sample Computer-System Security Risk Assessment Report

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) operates mission-critical systems for vessel traffic monitoring, navigation safety, and maritime coordination. HMTA operates critical systems supporting Hong Kong's marine transport operations, including vessel traffic management, berth allocation, marine communication networks, and safety-critical navigation systems.

This assessment identifies 13 High-Risk findings, 22 Medium-Risk findings, and 7 Low-Risk findings, including vulnerabilities discovered through VAPT and configuration review. A custom marine-transport cyber risk matrix is provided to reflect OT/ICS safety-of-life impacts.

This Security Risk Assessment (SRA) is conducted according to:

- Cap. 653 and Code of Practice (CoP)
- ISO/IEC 27005:2018 (risk management framework)
- IEC 62443 (industrial control/OT cybersecurity)
- DPO ISPG-SM01 (SRAA) Framework
- Associated corporate security governance policies

This assessment focuses on three critical systems:

- Vessel Traffic Management System (VTMS, Fig. 1) – OT/ICS
- Port Logistics Scheduling System (PLSS) – IT
- Marine Communication Gateway (MCG) – OT/IT hybrid

Fig. 1 Vessel Traffic Management System

1. Introduction

1.1 Purpose

The purpose of this risk assessment is to evaluate the security of HMTA and its support processes. It provides a structured qualitative review of the operational environment, focusing on sensitivity, threats, vulnerabilities, risk, and safeguards. The assessment recommends cost-effective measures to reduce threats and address exploitable vulnerabilities.

1.2 Background

HMTA is designated as a Critical Infrastructure Operator (CIO) under Ordinance Cap. 653, responsible for vessel traffic management, port logistics scheduling, and marine communication systems.

1.3 Ownership

The HMTA Computer-System Security Management Unit (CSSMU) is responsible for preparing this risk assessment and submitting a copy of this report to the Security Bureau within three months of being designated as a critical infrastructure operator in 2026.

1.4 Risk Appetite

The HMTA's CSSMU consulted senior management and stakeholders to determine the overall risk appetite for the systems in scope or critical computing systems (CCSs). Risk appetite has been set to a level of 'Cautious' – defined as a preference for safe delivery options that have a low degree of residual risk.

1.5 Review & Approvals

The CSSMU and HMTA senior management have reviewed this document.

2. Scope of Assessment

2.1 Systems in Scope

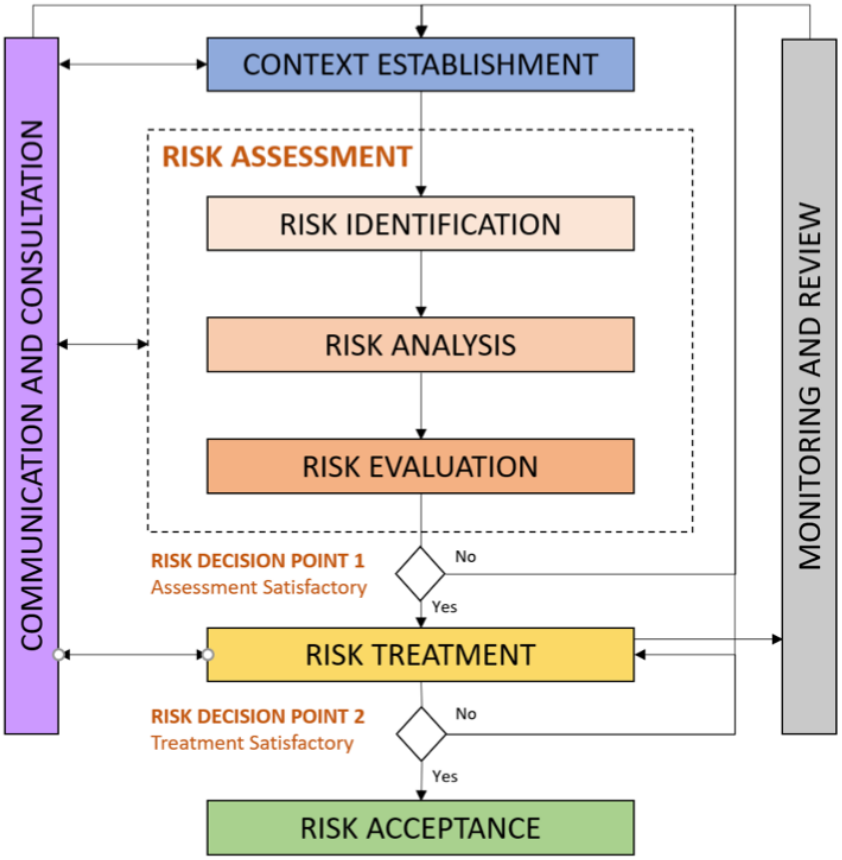
- VTMS OT / ICS radar integration, AIS tracking, maritime navigation safety; 24/7 critical operations.
- PLSS IT (Business) Logistics: scheduling, berth allocation, cargo records
- MCG Hybrid Interfaces with radio base stations, digital VHF, and internal communication networks.

2.2 Assessment Components

- Architecture & data-flow review
- VAPT (external, internal & OT-segmented tests)
- Configuration & hardening assessment
- Administrative control review (policies, SOPs)
- Risk analysis according to ISO 27005 and DPO ISPG-SM01 (SRAA)
- Mapping to CoP controls 6.2.5 – 6.2.27
- OT security mapping using IEC 62443-3-3 SR

3. Methodology

3.1 ISO/IEC 27005 Risk Management Process, as illustrated in Fig. 1 below:



The assessment has been conducted over several structural stages:

- Asset identification
- Threat event identification
- Vulnerability mapping
- Likelihood-Impact scoring (custom CI matrix)
- Risk estimation
- Risk treatment planning

3.2 IEC 62443 Reference

- Applied to OT systems (VTMS, MCG):
  - SR1 – Identification & Authentication Control
  - SR2 – Use Control
  - SR3 – System Integrity
  - SR4 – Data Confidentiality
  - SR5 – Restricted Data Flow
  - SR6 – Timely Response to Events
  - SR7 – Resource Availability

3.3 DPO ISPG-SM01 (SRAA) Elements

- Baseline security review
- Control effectiveness assessment
- Residual-risk determination
- Risk acceptance & governance documentation

4. Vulnerability Assessment & Penetration Test Summary

Below is a fictional but realistic set of VAPT findings for a marine-transport CI environment.

4.1 Critical & High-Risk Findings

- Finding 1 – OT Network Segmentation Bypass (High)
  - System: VTMS
  - Details: Firewall ACL misconfiguration allowed IT-to-OT communication via TCP/502 (Modbus).
  - Risk: Potential remote manipulation of PLCs feeding radar signals.
  - Reference: IEC 62443 SR5 (Restricted Data Flow) – Non-Compliant
- Finding 2 – Remote Code Execution on PLSS (Critical)
  - CVE: CVE-2024-2083 (fictional for sample)
  - Vector: Web API module
  - Impact: Full compromise of the scheduling system; cargo manifests could be tampered with.
  - CoP Mapping: 6.2.22 – Application Security Controls – Non-Compliant
- Finding 3 – Default Credentials on Radio Management Console (High)
  - System: MCG
  - Details: Factory default “admin/admin123”; console exposed to internal network.
  - Impact: Attacker can disrupt VHF communication scheduling.

- Finding 4 – Unencrypted OT Traffic (Medium–High)
    - System: VTMS
    - Details: AIS feed transmitted in cleartext; subject to spoofing.
    - Impact: Navigation data manipulation risk.
- Finding 5 – Outdated Windows Server 2012 (End-of-Life) (High)
    - System: PLSS DB Server
    - Impact: Multiple unpatchable RCE vulnerabilities.
    - CoP 6.2.17 – Patch & Vulnerability Management – Non-Compliant

4.2 Medium-Risk Findings

- Weak password history enforcement
- Patch lag of 60–120 days
- Lack of OT-specific EDR or passive monitoring
- SQL Server is using mixed authentication mode
- Missing audit logs shipped to SIEM due to a misconfigured log agent

4.3 Low-Risk Findings

- TLS settings using deprecated Cipher Suites
- Missing metadata classification labels
- Insufficient physical rack labels in the comms room

5. Custom Cyber-Risk Matrix (Marine Transport CIO)

Critical infrastructure related to maritime operations has unique risk factors, particularly concerning navigation safety, vessel collisions, and port disruptions.

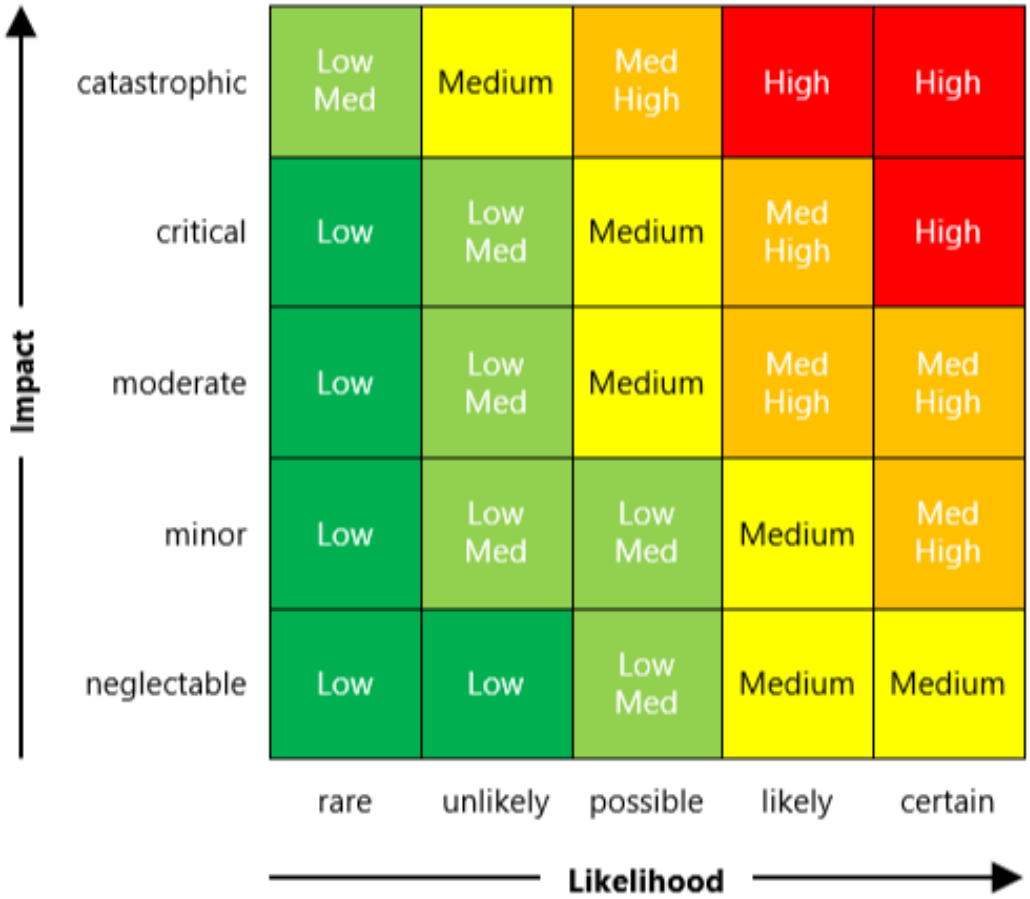
5.1 Impact Scoring (Customized)

- Catastrophic (5) → Loss of navigation control, collision, major port shutdown (>24 hours), serious public safety impact
- Severe (4) → Significant disruption to cargo/logistics scheduling, multi-hour port stoppage
- Moderate (3) → Localized system outage with operational workaround
- Minor (2) → Degraded performance, no direct operational harm
- Negligible (1) → Minimal inconvenience or administrative impact (High)

5.2 Likelihood Scoring

- Very Likely (5) → Attack can be executed easily; active exploitation observed in the wild
- Likely (4) → Exploitable with some skill; weak controls identified
- Possible (3) → Requires resources or targeted capability
- Unlikely (2) → Difficult to exploit; strong controls present
- Rare (1) → Very low feasibility

5.3 Risk Matrix (5×5)



Impact and Likelihood are assigned with a qualitative value of 1 2 3 4 5

- 5 → Catastrophic → M H H C C
- 4 → Severe → M M H H C
- 3 → Moderate → L M M H H
- 2 → Minor → L L M M H
- 1 → Negligible → L L L M M

Legend: C = Critical, H = High, M = Medium, L = Low

6. Risk Register (Excerpt)

Critical infrastructure involving maritime operations has unique risk characteristics, especially regarding navigation safety, vessel collisions, and port disruptions.

ID	Asset	Vulnerability	Likeli hood	Impact	Risk	Rating	Treatment
R-001	VTMS	Firewall bypass to OT network	4	5	Critical	Immediate	enforce ACL; deploy unidirectional gateway
R-004	PLSS	RCE API vulnerability	5	4	Critical	Patch	WAF hardening; code review
R-010	MCG	Default credentials	3	4	High	Credential reset	MFA; privileged access redesign
R-015	VTMS	Unencrypted AIS links	3	4	Medium	Encrypted overlay	integrity checking
R-021	PLSS	Log agent misconfiguration	2	2	Low	Reconfigure	SIEM forwarders

7. Compliance Mapping to CoP (6.2.5 – 6.2.27)

CoP	Section	Requirement Summary	Compliance Status	Gap	Summary
6.2.3	Asset	Inventory Maintain real-time OT & IT inventory		Partial	No auto-discovery in OT
6.2.4	Access	Control MFA	least privilege	Partial	Default OT credentials
6.2.10	Patch Management	Timely patching	Non-Compliant	EOL Windows	patch delays
6.2.13	Network	Security Segmentation OT & IT	Non-Compliant		ACL bypass found
6.2.22	Application Security	Secure coding code scanning	Non-Compliant		API RCE vulnerability
6.2.26	Monitoring & Detection	SIEM logging		Partial	Missing OT visibility
7.2	Incident Respons	IR plan, drills	Compliant		Annual test conducted

8. Recommendations

8.1 Technical Controls

- Implement strict IT <> OT network segmentation in accordance with IEC 62443 zones and conduits.
- Replace EOL systems and enforce a 30-day patch SLA
- Deploy OT passive monitoring sensors (e.g., network anomaly detection)
- Enforce MFA and remove all default credentials
- Encrypt AIS, radar data feeds using secure overlay networks.

8.2 Governance Controls

- Update risk registers quarterly
- Implement a secure development lifecycle aligned to ISO/IEC 27034
- Annual code review for PLSS and MCG modules
- CI-specific cyber-incident tabletop and technical drills.

8.3 Residual Risk Acceptance

Residual risks classified as High or Critical cannot be accepted under Ordinance 653 without formal justification to the Commissioner.

9. Conclusion

The assessment concludes that HMTA has basic cybersecurity controls but requires urgent remediation for several Critical and High-Risk items related to IT–OT boundary security, legacy systems, and weak authentication mechanisms.