

**SKILLS FRAMEWORK FOR SEA TRANSPORT
TECHNICAL SKILLS AND COMPETENCIES (TSC) REFERENCE DOCUMENT**

TSC Category	Fleet Management					
TSC	Ship Cyber Security					
TSC Description	Maintain the cyber security of the organisation's fleet					
TSC Proficiency Description	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				STP-FMT-4005-1.1	STP-FMT-5005-1.1	STP-FMT-6005-1.1
				Facilitate the implementation of the organisation's cyber security guidelines	Formulate cyber security response plans	Drive the adoption of cyber security initiatives in fleet management
Knowledge				<ul style="list-style-type: none"> • Components of contingency plans for cyber incidents • Types of pre-assessment activities prior to Ship Security Assessment • Elements of a Ship Security Assessment • International Safety Management Code (ISM) • International Ship and Port Facility Security (ISPS) Code, Regulation 8 	<ul style="list-style-type: none"> • Types of cyber security threats • Ship-board systems that may be exposed to cyber threats: <ul style="list-style-type: none"> ○ Cargo management systems ○ Bridge systems ○ Propulsion and machinery management and power control systems ○ Access control systems ○ Passenger servicing and management systems ○ Passenger facing public networks ○ Administrative and crew welfare systems ○ Communication systems • Vulnerable information and data and potential impact levels • Risk assessment • Elements of a Ship Security Assessment 	<ul style="list-style-type: none"> • Types of cyber security threats • International Safety Management Code (ISM) • International Ship and Port Facility Security (ISPS) Code, Regulation 8 • Types of initiatives to cascade cyber security awareness in the organisation • Components of a cyber-security strategy

**SKILLS FRAMEWORK FOR SEA TRANSPORT
TECHNICAL SKILLS AND COMPETENCIES (TSC) REFERENCE DOCUMENT**

					<ul style="list-style-type: none"> • International Safety Management Code (ISM) • International Ship and Port Facility Security (ISPS) Code, Regulation 8 • Types of vulnerabilities and weaknesses • Components of contingency plans 	
Abilities				<ul style="list-style-type: none"> • Conduct pre-assessment activities to facilitate the execution of Ship Security Assessment • Oversee the conduct of a Ship Security Assessment to physically test and assess the IT and Operational Technology (OT) systems • Brief relevant crew on contingency plans in the event of cyber security incidents • Ensure adherence to the organisation's cyber security policies and procedures 	<ul style="list-style-type: none"> • Evaluate the vulnerabilities that may compromise the ship's IT and OT systems • Review proposed recommendations to enhance the ship's IT and OT systems • Collaborate with ship contractors on recommendations to mitigate ship's vulnerabilities • Formulate the organisation's strategy in handling cyber security for the fleet • Align strategy to requirements of ISM and ISPS Codes • Develop contingency plans to handle cyber security incidents 	<ul style="list-style-type: none"> • Evaluate and decide on cyber security risks that may impact on fleet management • Drive initiatives to heighten cyber security awareness in fleet management • Drive efforts to reduce cyber security risks • Endorse the organisation's strategy in cyber security