<table>
<thead>
<tr>
<th>TSC Category</th>
<th>Fleet Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSC</td>
<td>Ship Cyber Security</td>
</tr>
<tr>
<td>TSC Description</td>
<td>Maintain the cyber security of the organisation's fleet</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TSC Proficiency Description</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>STP-FMT-4005-1.1</td>
<td>STP-FMT-5005-1.1</td>
<td>STP-FMT-6005-1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitate the implementation of the organisation’s cyber security guidelines</td>
<td>Formulate cyber security response plans</td>
<td>Drive the adoption of cyber security initiatives in fleet management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Knowledge**

- 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
- Types of cyber security threats
- Ship-board systems that may be exposed to cyber threats:
  - Cargo management systems
  - Bridge systems
  - Propulsion and machinery management and power control systems
  - Access control systems
  - Passenger servicing and management systems
  - Administrative and crew welfare systems
  - Communication systems
- Vulnerable information and data and potential impact levels
- Risk assessment
- Elements of a Ship Security Assessment
- International Safety Management Code (ISM)
- 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

| Abilities | • 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 | • 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 | • 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 |

**Abilities**

1. International Ship and Port Facility Security (ISPS) Code, Regulation 8
2. Types of vulnerabilities and weaknesses
3. Components of contingency plans

©SkillsFuture Singapore  
Effective date: April 2017, Version 1.1  
Page 2 of 2