



Australian Government

MARF040 Manage ship security (Ship Security Officer)

Release: 1

MARF040 Manage ship security (Ship Security Officer)

Modification History

Release 1. This is the first release of this unit of competency in the MAR Maritime Training Package.

Application

This unit involves the skills and knowledge required to manage ship security.

This unit applies to people working in the maritime industry in the capacity of:

- Ship Security Officer.

Licensing/Regulatory Information

This unit is equivalent to and delivers the objectives of the following STCW provisions:

- STCW Reg VI/5 and Code Section A-VI/5 (1-4), Table A-VI/5.

Legislative and regulatory requirements are applicable to this unit.

- This unit is one of the requirements to obtain Australian Maritime Safety Authority (AMSA) certification as a Ship Security Officer and to meet regulatory requirements this unit must be delivered consistent with Marine Orders and with the relevant sections of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW).
- Those regulatory requirements include STCW International Maritime Organization (IMO) model course competencies and areas of knowledge, understanding and proficiency, together with the estimated total hours required for lectures and practical exercises. Teaching staff should note that timings are suggestions only and should be adapted to suit individual groups of trainees depending on their experience, ability, equipment and staff available for training.

Pre-requisite Unit

Not applicable

Competency Field

F – Operational Quality and Safety

Unit Sector

Not applicable

Elements and Performance Criteria

ELEMENTS

Elements describe the essential outcomes.

PERFORMANCE CRITERIA

Performance criteria describe the performance needed to demonstrate achievement of the element.

- | | |
|--|---|
| 1 Supervise and maintain the implementation of ship security plan | 1.1 Ship security plan is implemented and modified in accordance with the International Ship and Port Facility Security (ISPS) Code and the International Convention for the Safety of Life at Sea (SOLAS), as amended

1.2 Legislative requirements for security are identified correctly

1.3 State of readiness is established and maintained in accordance with procedures to ensure changes in maritime security levels are responded to

1.4 Communication in the Ship Security Officer's area of responsibility for supervising and implementing ship security plan is clear, concise and understood

1.5 Implementation of ship security plan is coordinated with Company Security Officer and relevant Port Facility Security Officer |
| 2 Assess security risk, threat and vulnerability | 2.1 Risk assessment procedures and actions are implemented in accordance with the ISPS Code and SOLAS, as amended principles

2.2 State of readiness is established and maintained in accordance with procedures to ensure changes in maritime security levels are responded to

2.3 Communication in the Ship Security Officer's area of responsibility for assessing and maintaining threat and vulnerability is clear, concise and understood

2.4 Security incidents are reported to Company Security Officer in accordance with workplace procedures |
| 3 Undertake regular ship inspection | 3.1 Ship inspection procedures and actions are implemented in accordance with the ISPS Code and SOLAS, as amended

3.2 State of readiness is established and maintained in accordance with procedures to ensure changes in maritime security levels are responded to |

- | | | |
|----------|--|--|
| | 3.3 | Security inspections are conducted to ensure that appropriate security measures are maintained |
| | 3.4 | Communication in the Ship Security Officer's area of responsibility when undertaking inspections is clear, concise and understood |
| | 3.5 | Deficiencies and non-conformities are identified during inspections conducted as part of internal audits, periodic reviews and verifications of compliance and reported to the Company Security Officer and corrective actions are implemented |
| 4 | Establish security equipment and systems are properly operated, tested and calibrated | |
| | 4.1 | Ship inspection procedures and actions are implemented in accordance with the ISPS Code and SOLAS, as amended |
| | 4.2 | Security equipment is operated, tested, calibrated and maintained in accordance with security ship procedures |
| 5 | Maintain security awareness and vigilance | |
| | 5.1 | Ship inspection procedures and actions are implemented in accordance with the ISPS Code and SOLAS, as amended |
| | 5.2 | Communication in the Ship Security Officer's area of responsibility when maintaining vigilance is clear, concise and understood |

Foundation Skills

Foundation skills essential to performance are explicit in the performance criteria of this unit of competency.

Range of Conditions

Range is restricted to essential operating conditions and any other variables essential to the work environment.

Unit Mapping Information

This is a new unit. No equivalent unit

Links

Companion Volume implementation guide can be found in VetNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=772efb7b-4cce-47fe-9bbd-ee3b1d1eb4c2>

Assessment Requirements for MARF040 Manage ship security (Ship Security Officer)

Modification History

Release 1. This is the first release of this unit of competency in the MAR Maritime Training Package.

Performance Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements and performance criteria on at least one occasion and include:

- applying International Ship and Port Facility Security Code (ISPS) Code and International Convention for the Safety of Life at Sea (SOLAS)
- assessing security risk, threat and vulnerability
- communicating clearly and concisely within scope of responsibility
- conducting ship inspection
- establishing state of readiness using correct procedures
- identifying legislative requirements relevant to ship security plan
- implementing ship security plan
- implementing state of readiness using correct procedures
- operating, testing and calibrating security equipment and systems in accordance with relevant procedures
- reporting deficiencies and non-conformities to Company Security Officer.

Knowledge Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements and performance criteria and include knowledge of:

- controlling access to ship and restricted areas onboard a ship
- crowd management and control techniques
- enabling recognition, including:
 - non-discriminatory basis of persons posing potential security risks
 - weapons, dangerous substances, devices and awareness of the damage they can cause
- handling sensitive security-related information and security-related communications
- implementing and coordinating searches
- international maritime security policy and responsibilities of governments, companies and designated persons, including elements that relate to piracy and armed robbery
- maritime security levels and the consequential security measures and procedures aboard ship and in the port facility environment
- maritime security terms and definitions, including elements that relate to piracy and armed

robbery

- methods and effective monitoring of deck areas and areas surrounding the ship
- methods and procedures used to modify the ship security plan
- methods for physical searches and non-intrusive inspections
- methods for assessing the effectiveness of drills and exercise
- methods for controlling the embarkation, disembarkation and access while onboard of persons and their effects
- methods for enhancing security awareness and vigilance onboard a vessel
- methods for testing, calibrating and maintaining security systems and equipment, particularly whilst at sea
- procedures to be employed in implementing a ship security plan and reporting of security incidents, purpose of and the elements that make up a ship security plan, related procedures and maintenance of records, including piracy and armed robbery
- procedures, instructions and guidance on the use of ship security alert systems
- requirements and procedures for conducting internal audits, on-scene inspections, control and monitoring of security activities specified in ship security plan
- requirements and procedures for reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews and security inspections
- requirements for designating and monitoring restricted areas
- risk assessment and assessment tools
- security aspects relating to the handling of cargo and ship's stores with other shipboard personnel and relevant port facility Security Officers
- security assessment documentation and Declaration of Security
- security-related contingency plans and the procedures for responding to security threats and breaches of security, including:
 - elements that relate to piracy and armed robbery
 - provisions for maintaining critical operations of the ship/port interface
- security training and requirements
- techniques used to circumvent security measures, including those used by pirates and armed robbers
- training, drill and exercise requirements under relevant conventions, codes and International Maritime Organization (IMO) circulars, including those relevant to anti-piracy and anti-armed robbery
- various types of security equipment and systems and their limitations, including those that could be used in case of attacks by pirates and armed robbers.

Assessment Conditions

Assessors must hold credentials specified within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must satisfy the Principles of Assessment and Rules of Evidence and all regulatory requirements included within the Standards for Registered Training Organisations current at the

time of assessment.

Assessment processes and techniques must be appropriate to the language, literacy and numeracy requirements of the work being performed and the needs of the candidate.

Practical assessment must occur in a workplace or realistic simulated workplace, under the normal range of workplace conditions.

Simulations and scenarios may be used where situations cannot be provided in the workplace or may occur only rarely, in particular for situations relating to emergency procedures and adverse weather conditions where assessment would be unsafe, impractical or may lead to environmental damage.

Resources for assessment must include access to:

- applicable documentation, such as legislation, regulations, codes of practice, workplace procedures and operational manuals
- tools, equipment, machinery, materials and relevant personal protective equipment (PPE) currently used in industry.

Links

Companion Volume implementation guide can be found in VetNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=772efb7b-4cce-47fe-9bbd-ee3b1d1eb4c2>