

Marine Management Systems



International Ship and Port Facility Security Code

Practical Pack

International Ship and Port Facility Security (ISPS) Code:
A practical approach to ship security



Using the Practical Pack

This Practical Pack is intended to help company security officers meet the challenges posed by the introduction of the International Ship and Port Facility Security (ISPS) Code. By adopting a practical approach, this pack provides a methodology for conducting ship security assessments, performing on-scene security surveys, developing ship security plans and writing the necessary security procedures to aid onboard implementation.





Company security officers, ship security officers and managers involved in maritime security will benefit from this Practical Pack through a greater understanding of the processes involved in complying with the ISPS Code.

When working through the Practical Pack reference should be made to **The International Ship and Port Facility Security (ISPS) Code (including SOLAS amendments)** and **USCG Navigation and Vessel Inspection Circular NVIC 10-02** to better understand the principles upon which the Practical Pack is based.

Lloyd's Register of Shipping, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as the 'Lloyd's Register Group'. The Lloyd's Register Group assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register Group entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

Conventions

The following standard conventions are used in Lloyd's Register, Marine Services training documentation:

| Symbol | What it highlights |
|-----------------------------------------------------------------------------------|------------------------------------------------|
|  | Hints and tips – and recommended methods |
|  | Where to go for help or additional information |
|  | Important information |
|  | Critical information |

Additional standard conventions used in this document



Example document

These documents are not intended to be reproduced verbatim in company security documentation; rather they are intended to be used as possible examples of what will be required.

Text in blue italics is intended to give possible examples of the information a company may need to include in the ship security assessment and ship security plan.

A section number in bold thus, section 9.4 subsection .2, .4, .5, .7, **.15**, .17 and .18, indicates that a quote from this section follows below.

Contents

Using the Practical Pack

Introduction

- Achieving your Ship Security Plan
- Ship Security Assessment
- Producing a Ship Security Assessment
- The steps to producing a Ship Security Assessment
- Conducting a Ship Security Assessment

Section 1 – Documentation

Section 2 – Declaration of Security

Section 3 – Ships General Arrangements

Section 4 – Ship Access

Section 5 – Restricted Areas

Section 6 – Emergency Evacuation Routes

Section 7 – Existing Security Systems

Section 8 – Threat Evaluation and Risk Assessment

Section 9 – On-Scene Security Survey

Section 10 – Ship Communications

Section 11 – Embarkation of Persons and Baggage

Section 12 – Cargo and Ship's Stores Handling

Section 13 – Security Monitoring

Section 14 – Contingency Plans

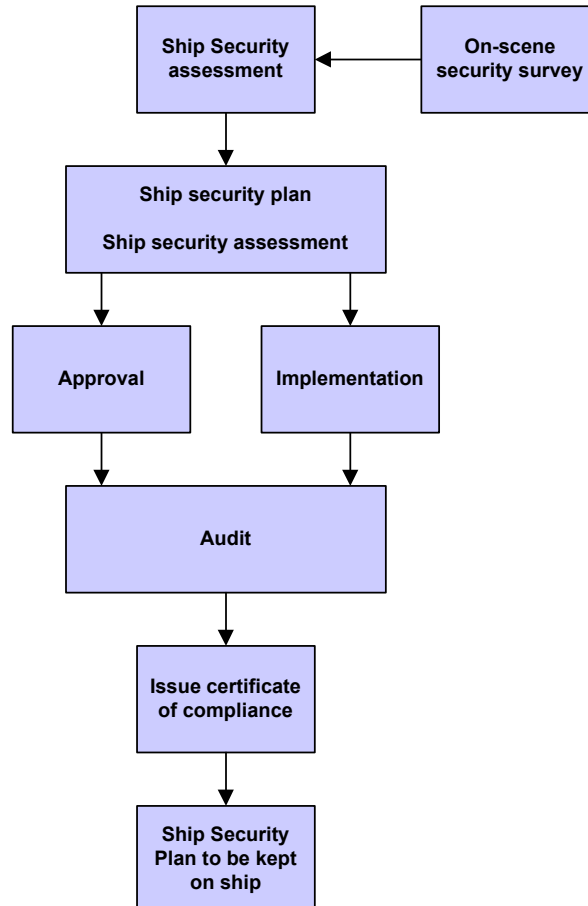
Introduction

The Practical Pack provides a methodology that company security officers can use when conducting ship security assessments and developing ship security plans in accordance with the requirements of the ISPS Code. Recognising that there is no “one size fits all” solution, the Practical Pack is not a ship security plan “template”; rather it is an effective tool for both understanding and complying with the requirements of the ISPS Code.

Three key phases are involved in working through the Practical Pack. These are:

1. Conducting **ship security assessments** (including conducting the on-scene security survey). The ship security assessment identifies the security measures that will need to be included in the ship security plan
2. Developing the **ship security plan**, based on the outcome of the ship security assessment. The ship security plan details the measures that are required to be implemented onboard
3. Developing **ship security procedures**. These procedures are to be attached to, and form part of, the approved ship security plan. Whereas the ship security plan details the security measures, the procedures provide the detail as to how these measures are to be implemented. If the ship security plan details “what has to be done”, the security procedures detail “when it has to be done, who shall do it, how it shall be done, what records are to be kept, etc.”

Achieving your Ship Security Plan



The time span from the time the plan goes on board to the date of audit remains to be confirmed (awaiting guidance from IMO; early indications are 2 months from the date the ship security plan goes on board for implementation; however this may vary from Flag to Flag).

Ship Security Assessment

A ship security assessment is a mandatory and essential part of the process to develop a ship security plan. Company security officers are responsible for ensuring that a ship security assessment is carried out for each ship they are responsible for.

The ship security assessment:

- is to be carried out by persons with the appropriate skills and knowledge to evaluate the security of the ship and must contain an on-scene security survey for that specific ship
- must be documented, reviewed, accepted and retained by the company
- must accompany the ship security plan when put forward for approval

Upon completion of the ship security assessment, a report shall be prepared, consisting of:

- a summary of how the assessment was conducted
- a description of each vulnerability found during the assessment
- a description of counter measures that could be used to address each vulnerability.

The report shall be protected from unauthorised access or disclosure.

If the Company has not carried out the ship security assessment, it must be documented that the report of the ship security assessment has been reviewed and accepted by the company security officer.



It is not a requirement to keep the ship security assessment with the ship security plan, however, it is highly recommended to do so for ease of review, amendment and access in the event of a security incident.



The ship security assessment, unlike the ship security plan, is not classed as **confidential** or **restricted**. However, due to the nature of the information within the ship security assessment it should be given the same degree of protection as the ship security plan.

Producing a Ship Security Assessment

A ship security assessment can be produced in two ways.

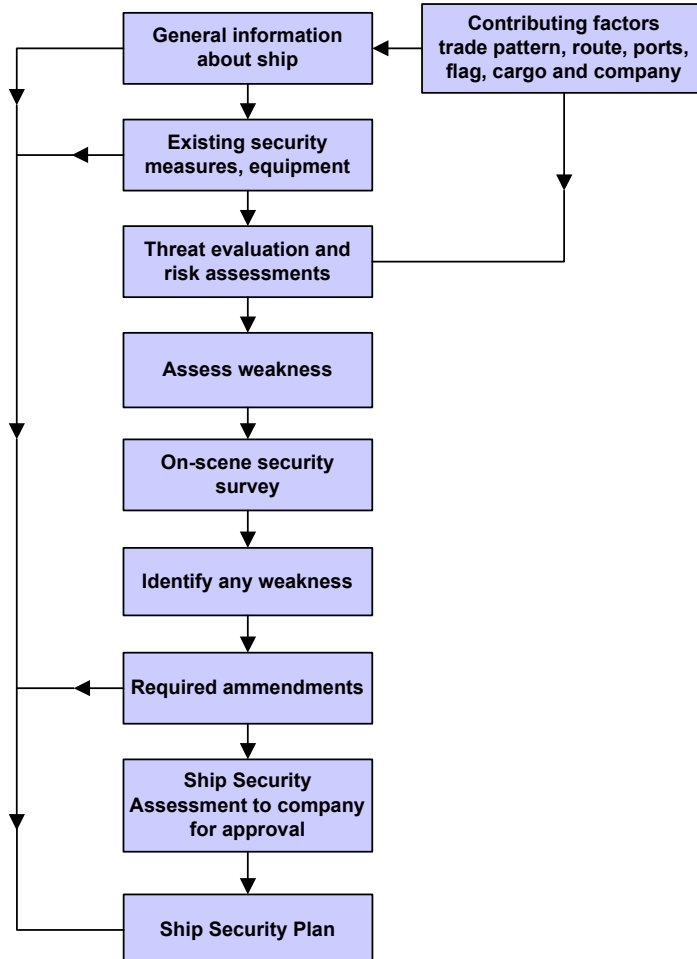
Individual

A ship security assessment including the required on-scene security survey compiled for a single specific ship.

Generic

A company may produce a generic ship security assessment that covers the assessment of security risk across a part of their fleet, or their entire fleet, provided that an “on-scene security survey” has been carried out on each individual ship and the ship security assessment reflects all relevant “ship specific” aspects.

The steps to producing a Ship Security Assessment



Conducting a Ship Security Assessment

Step 1

Obtain and record the following information required to conduct an assessment.

4. Ship and Company Documentation as detailed within Section 1 (this should contain the relevant information that will identify any contributing factors to be included in the Threat Evaluation and Risk Assessment phase of the assessment).
5. Record and document the following information in detail:

| Information | Complete |
|------------------------------------------------------------------|----------|
| Authorised access points as detailed within Section 4 | |
| Restricted areas as detailed within Section 5 | |
| Escape and Evacuation routes as detailed within Section 6 | |
| Existing Security Equipment/Systems as detailed within Section 7 | |

6. A copy of the ships General Arrangement Plan annotated with the following information:

| Information | Complete |
|------------------------------------------------------------------|----------|
| Authorised access points as detailed within Section 4 | |
| Restricted areas as detailed within Section 5 | |
| Escape and Evacuation routes as detailed within Section 6 | |
| Existing Security Equipment/Systems as detailed within Section 7 | |

Once the above information has been compiled, this then becomes the relevant sections within the ship security assessment.

This information is also copied into the relevant sections of the ships security plan.

Step 2

Conduct and document a detailed Threat Evaluation and Risk Assessment for the ship as detailed within Section 8. This must include the Contributing Factors identified earlier in Step 1.

Examine all the information gathered and assess for any weaknesses. Weaknesses should be noted and addressed during the on-scene security survey.

Once these tasks have been completed, a copy is retained as the relevant sections within the ship security assessment.

ISPS Code – Practical Pack

Step3

Conduct the On-Scene Security Survey, during which all previous details and information gathered about the ship must be confirmed and any weaknesses identified, as detailed within Section 9.

Once this task has been completed, a copy is retained as the relevant sections within the ship security assessment.

Step 4

Once the On-Scene Security Survey has been completed, any amendments or additions required to the information, procedures and measures documented in the previous steps must be incorporated at this point.

Amendments and additions are to be documented and a copy retained within the On-Scene Security Survey section of the ship security assessment.

A copy of all additions and amendments are also copied into the relevant sections of the ship security plan.

Step 5

The ship security assessment is presented to the company for review and acceptance.

Once accepted and documented, the ship security plan can be finalised with any amendments from the review.

Step 6

The ship security plan, accompanied by the assessment, is put forward for approval by the Administration or Recognised Security Organisation (RSO).