

ISPS Code



Information on ISPS Code Certification

ISPS Code Certification

Germanischer Lloyd - your reliable partner in maritime safety and security.

Germanischer Lloyd (GL) was the first classification society to respond to the new developments in the field of maritime security by staging national and international information seminars.



Since then considerable efforts have been undertaken by GL to assist the maritime community in successfully achieving compliance with the new international mandatory requirements to enhance maritime security.

Some 150 GL specialists have been trained to act as Maritime Security Auditors and more are going to be trained in the future.

In addition GL has produced supporting tools for clients , e.g. Guidelines for the Performance of Ship Security Assessments (SSA) and Guidelines for the development of Ship Security Plans (SSP).

GL provides also a number of maritime security related seminars such as Company and Ship Security Officer Training Courses and ISPS Implementation Workshops.

- [General Information](#)
- [ISPS Code Certification Process](#)
- [Interim ISPS Code Certification](#)
- [Supporting Tools & Seminars](#)



Contacts

General Information

The security threat

Few industries depend as much as shipping on an internationally well-ordered, safe and secure environment. In the context of maritime security it is recognized that piracy, unlawful acts and stowaways already causing major problems to shipping. However recent terrorist attacks have highlighted again the vulnerability of maritime security and triggered a response of unprecedented speed and thoroughness from national and international authorities.



The clear response

IMO has recognized its responsibility for maritime security with a view to prevent "shipping from becoming a soft target for international terrorism" (William O'Neill, IMO Secretary General). Its response has been to introduce new mandatory requirements aimed at safeguarding the maritime community. These new measures have been laid down in several amendments to SOLAS and the International Ship and Port Facility Security (ISPS) Code which both have been adopted in December 2002.

The tight deadline

The amendments to SOLAS and the ISPS Code have introduced numerous new requirements for shipping companies, port facilities and administrations: These responsibilities include, for example, the performance of security assessments, preparation of security plans and the appointment of responsible security officers. All passenger ships, cargo ships of 500 GT and above, mobile off shore drilling units and port facilities serving these ships must implement the security measures and achieve compliance by 1 July 2004. This very tight deadline presents a huge challenge to the world's commercial shipping fleet.

Requirements for Shipping Companies

By 1 July 2004 every shipping company has to obtain an International Ship Security Certificate (ISSC) for each of its ships to demonstrate that the ships operate in compliance with SOLAS Chapter XI-2 and the relevant parts of the ISPS Code.

The requirements to obtain the ISSC are:

- ? Appointment of a Company Security Officer (CSO)
- ? Performance of a documented Ship Security Assessment (SSA) including on-scene security survey
- ? Appointment of Ship Security Officers (SSOI) for each individual ship
- ? Development of a Ship Security Plan (SSP)
- ? Ensuring that the SSP contains a statement emphasizing the Master's Authority with respect to ship security and ensuring that appropriate resources are provided for all personnel concerned
- ? Review and approval of the SSP by the flag State administration or Recognized Security Organisation (RSO)
- ? Implementation of the security plan onboard
- ? Ensuring that training, drill and exercises on ship security are carried out for all relevant personnel
- ? Ensuring that records of the activities addressed in the SSP are kept onboard
- ? Onboard Verification of the security system by the flag State Administration or the RSO
- ? Having on board a valid ISSC after successful completion of the verification.

Requirements for Port Facilities

By 1 July 2004 every port facility, which is serving ships on international voyages, has to demonstrate that it operates in compliance with SOLAS Chapter XI-2 and the relevant parts of the ISPS Code.

The requirements for port facilities are:

- ? Appointment of a Port Facility Security Officer (PFSO)
- ? Performance of a Port Facility Security Assessment (PFSA) by Contracting Government or by competent persons including a Recognized Security Organisation (RSO)
- ? Approval of the PFSA by the Designated Authority of the Contracting Government
- ? Development of a Port Facility Security Plan (PFSP)
- ? Approval of the PFSP by the Designated Authority of the Contracting Government
- ? Implementation of the security plan within the port facility
- ? Ensuring that training, drill and exercises on port facility security are carried out for all relevant personnel.

Requirements for Administrations

Every Contracting Government has under the provisions of SOLAS Chapter XI-2 and the relevant parts of the ISPS Code, various responsibilities, e.g.:

- ? Nomination of the national authority or authorities responsible for ship security and port facility security (Designated Authority)
- ? Nomination of the competent authority designated to receive and act upon ship security alerts
- ? Nomination of a point of contact designated to provide advice and assistance to ships within their territory
- ? Setting of Security Levels for the ships flying their flag, ships within their jurisdiction and port facilities within their territory
- ? Notification of the Security Levels to ships and port facilities
- ? Exercising control and compliance measures, i.e. control of ships in its ports, control of ships intending to enter its ports and imposing control measures (e.g. inspection, detention, expulsion from port, denial of entry, etc)
- ? Approval, verification and certification of SSPs or authorization of Recognized Security Organisations (RSO) to undertake these duties on its behalf
- ? Approval of PFSA's and PFSPs
- ? Testing the effectiveness of SSPs and PFSPs
- ? Establishing the requirements for a Declaration of Security
- ? Issuing the Continuous Synopsis Record (CSR) for ships flying its flag (SOLAS Chapter XI-1)
- ? Communication of information to IMO regarding port facilities within their territory covered
 - by approved PFSPs and of information regarding the national authorities (see above)

ISPS Code Certification Process

For obtaining the International Ship Security Certificate (ISSC) the ISPS Code requires the steps below to be undertaken:

Germanischer Lloyd's (GL's) role

GL can help you to complete the five steps for obtaining an ISSC. For the straight and successful performance of the SSA (1st step), as well as for the development and implementation of the SSP (2nd step), GL has produced guidelines as a useful tool.

As numerous flag State administrations have already authorized GL as a Recognized Security Organisation (RSO), GL is capable to carry out activities relating to the 3rd, 4th and 5th step on their behalf.



Ship Security Plan (SSP) Approval

Shipping companies must submit for each of their ships the relevant SSP accompanied by the documented SSA for approval. Upon receipt, GL will review the SSP and, if the SSP is in compliance with the relevant provisions of SOLAS and the ISPS Code, GL will approve the SSP on behalf of the flag State administration.

If the review process identifies that the SSP is lacking compliance with the

requirements, GL will inform the shipping company on the detected deficiencies. It is then to the shipping company to correct the deficiencies and to provide GL with evidence of the corrective action undertaken, prior the review and approval process can be finalized.

Verification of Ships

When the shipping company considers the approved SSP to be well implemented on board the ship, a request for ISPS Code verification should be sent to GL Head Office , who will appoint a qualified auditor for an onboard verification at a convenient time and place in co-operation with the company. During the verification the following steps will be carried out:

- I. Verification that the approved SSP, any amendments to the plan and associated procedures are being implemented effectively.
- II. Verification that the security system and all associated security equipment complies with applicable requirements and is in all respects satisfactory.

Furthermore, during the verification, objective evidence shall be obtained demonstrating that security related training, drills and exercises are carried out in appropriate intervals, internal audits and reviews are conducted periodically and that the security equipment is maintained, calibrated and tested including the ship security alert system.

If the Maritime Security Auditor conducting the verification is satisfied that the ship's security plan is satisfactorily implemented and any associated security equipment fully complies with the applicable requirements, i.e. is in all aspects in satisfactory condition and is fit for the service for which the ship is intended with no deficiencies, a International Ship Security Certificate will be issued.

Consultancy

It is precluded by law that the same RSO undertaking the review and approval of the SSP for a specific ship, has been involved in either the performance of the SSA or the preparation of the SSP. Therefore, GL will only concentrate on and restrict its activity related to maritime security to the SSP approval, verification and certification and will not offer consultancy services to shipping companies.

Interim ISPS Code Certification

After the 1st July 2004 Interim ISPS Code certification is possible under the following conditions:

- a new ship is coming into service or re-enters into service
- change of flag
- change of management

Prior to issue an Interim ISSC a shipboard verification will be conducted verifying:

- whether a SSA has been carried out
- whether a SSP is onboard meeting the relevant requirements
- whether the SSP has been submitted for review and approval
- whether the SSP has been implemented onboard the ship
- whether the CSO has ensured the review of SSP for compliance with the relevant requirements
- whether the CSO has ensured that arrangements for drills, exercises and internal audits have been installed that the ship will successfully complete the verification within 6 months
- whether necessary arrangements for initial verification have been made
- whether the Master, the SSO and other ship's personnel with specific security duties are familiar with their duties and are familiar with the provisions of the SSP
- whether the information for above personnel has been provided in the working language or languages understood by them
- whether the SSO meets the requirements of part A of the ISPS Code



Only on satisfactory results of the matters listed above, with no deficiencies found, an

Interim ISSC will be issued by the flag State administration or by GL on its behalf.

The Interim ISSC shall be valid for 6 months.

Supporting Tools & Seminars

GL provides the following tools for ISPS Code Certification:

Brochures:

- ? Maritime security: Mastering the challenge - engl.
- ? Maritime security: Risiken als Herausforderung - dt.

Guidelines:

- ? Guidelines for Development and Implementation of a Methodology for the Performance of a Ship Security Assessment (including Work Sheets)
- ? Guidelines for Development and Implementation of a Ship Security Plan

If you have any further questions regarding the brochures or guideline, please do not hesitate to contact us.

Maritime Security Seminars:

- ? Company Security Officer Training Course
- ? Ship Security Officer Training Course
- ? ISPS Implementation Workshop
- ? Train the Trainer (Maritime Security)

If you have any further questions regarding the seminars, please do not hesitate to contact the staff of GL Academy.

Contacts

Germanischer Lloyd AG
Marine Management Systems Certification
Maritime Security Matters
Vorsetzen 35
D-20459 Hamburg/Germany
E-mail: security@gl-group.com
Internet: <http://www.gl-group.com>

Mr. Dirk Eggers	Head of Group Phone: +49 (0)40 36149 7055 Fax: +49 (0)40 36149 7007 E-mail: DEgg@gl-group.com
Ms. Ahlke Koehlken	Phone: +49 (0)40 36149 7451 Fax: +49 (0)40 36149 7007 E-mail: AKo@gl-group.com
Mr. Klaus Bieber	Phone: +49 (0)40 36149 7755 Fax: +49 (0)40 36149 7007 E-mail: KBie@gl-group.com
Mr. Wilhelm Loskot	Phone: +49 (0)40 36149 7587 Fax: +49 (0)40 36149 7007 E-mail: WLos@gl-group.com