



Marine Management Systems Certification, Group Maritime Security

Guidelines for ISPS Code Certification

Hamburg, 07/2004



Germanischer Lloyd

General

This guideline describes the steps to be undertaken for issuing an International Ship Security Certificate (ISSC) to a ship upon verification of its security system and any associated security equipment covered by the relevant provisions of the ISPS Code and SOLAS Chapter XI-2. The certification shall ensure that the security system and associated security equipment of the ship fully complies with the Code and is in satisfactory condition and fit for the service for which the vessel is intended.

2. Scope

This guideline establishes the procedures for:

- review and approval of Ship Security Plans
- verification of compliance of ships with the requirements of part A of the ISPS Code and SOLAS XI-2 and the approved Ship Security Plan
- issuance of ISSCs (including Interim ISSCs)

This procedure is to be used for issuing the ISSC when requested by a Company, as well as when acting on behalf of the Administration during the mandatory implementation of the ISPS Code under SOLAS Chapter XI-2.

The scope of the verification carried out under these guidelines shall be restricted to the requirements of SOLAS XI-2 and ISPS Code part A. If the MarSec Auditor identifies potential deviations in compliance with other requirements, these shall be communicated to the organization issuing the relevant certificates.

2.1. Reference

- IACS PR. 24: Procedural Requirements for ISPS Code Certification
- IACS PR. 25: Procedure for Training and Qualification of Maritime Security Auditors
- IACS PR. 26: Procedure for Reporting the List of Ships complying with ISPS Code
- IACS Recommendations 81: Guidance on the ISPS Code for Maritime Security Auditors
- SOLAS Chapter V
- SOLAS Chapter XI-1 and XI-2
- International Ship and Port Facility Security (ISPS) Code

2.2. Definitions

For the purpose of this Guideline the following definitions apply:

“Convention”, in terms of this guideline, means the International Convention for the Safety of Life at Sea, 1974 as amended.

“Code”, in terms of this guideline, means “International Ship and Port Facility Security Code”.

“International Ship and Port Facility Security Code” (ISPS Code) consisting of Part A and Part B as adopted by IMO’s Diplomatic Conference on 12 December 2002.



Germanischer Lloyd

“Security system” is the component of the Ship Security Plan which includes the procedures, documentation and associated records which are in place to comply with the requirements of the ISPS Code.

“Company” means the owner of the ship, or the organization, or person such as a manager, or the Bareboat Charterer, assuming the responsibility for the operation of the ship from the owner, and when assuming such responsibility has agreed in writing to take over all the duties and responsibilities imposed by the International Safety Management (ISM) Code.

“Ship Security Assessment” (SSA) means the identification of existing security measures, procedures and operations, identification and evaluation of key shipboard operations, identification of possible threats to the key shipboard operations and identification of weaknesses in the infrastructure, policies and procedures, including human factors.

“Ship Security Plan” (SSP) means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship’s stores or the ship from the risks of a security incident.

“Ship Security Officer” (SSO) means the person on board the ship, accountable to the Master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the Company Security Officer and the Port Facility Security Officers.

“Company Security Officer” (CSO) means the person designated by the Company for ensuring that a SSA is carried out; that a SSP is developed, submitted for approval, and thereafter implemented and maintained and for liaison with Port Facility Security Officers and the Ship Security Officer.

“Port Facility Security Officer” (PFSO) means the person designated as responsible for the development, implementation, revision and maintenance of the Port Facility Security Plan and for liaison with the SSO and CSO.

“Security Incident” means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high-speed craft, or of a port facility or of any ship/port interface or any ship-to-ship activity.

“Security Level” means the qualification of the degree of risk that a security incident will be attempted or will occur.

“Security Level 1” means the level for which minimum appropriate protective security measures shall be maintained at all times.

“Security Level 2” means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

“Security Level 3” means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.



Germanischer Lloyd

“Regulation” means a regulation of the Convention.

“Chapter” means a chapter of the Convention.

“Section” means a section of the ISPS Code part A.

“Paragraph” means a paragraph of the ISPS Code part B.

“Ship” when used in this guideline, includes mobile offshore drilling units (MODU) and high-speed craft as defined in regulation XI-2/1.

“Non-compliance” means non-fulfillment of a specified requirement or the subject matter is inappropriate for the ship.

“Failure” means the non-fulfillment of a specific requirement which occurs subsequent to an ISSC being issued.

“Verification” means the evaluation of the SSP implementation on board a ship by a Maritime Security Auditor. This means a sample audit of all operational (non-technical) security measures, to the level necessary for the auditor to verify the whole operating system, and a 100% verification of all technical equipment, specified in the SSP, has to be conducted.

“Recognized Security Organization” (RSO) means an organization with appropriate expertise in security matters and appropriate knowledge of ship and port operations authorized to undertake certain security-related activities.

“AIS” means Automatic Identification System required by SOLAS V/19.

“CSR” means Continuous Synopsis Record required by SOLAS XI-1/5.

“Ship Security Alert System” means equipment as required by SOLAS XI-2/6

“ISSC” means the “International Ship Security Certificate” required by ISPS Code A/19.

“MarSec” means Maritime Security

“MarSec Auditor” means an auditor who has been trained as a maritime security auditor and appointed by Germanischer Lloyd to verify and approve SSPs and to conduct security verifications on board ships.

3. Duties and Responsibilities

3.1. Germanischer Lloyd



Germanischer Lloyd

Germanischer Lloyd (GL), acting as RSO¹, is authorized by flag State administrations to carry out the following security-related activities: review and approval of Ship Security Plans, verification of compliance of ships with the requirements of the ISPS Code and SOLAS XI-2 and issuance of ISSCs (including Interim ISSCs).

It is precluded by the ISPS Code 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.

GL is responsible for ensuring that the verification and certification process is performed in accordance with these guidelines and relevant flag State requirements, if any.

For the purpose of this guideline, duties and responsibilities of GL include the following:

- ensuring that certification services are carried out by those who have knowledge of the certification process and practices
- ensuring expertise in relevant aspects of security
- ensuring appropriate knowledge of ship and port operations
- holding the capability to assess the likely security risks and how to minimize those risks
- ensuring that MarSec Auditors meet the relevant education, training and verification experience in accordance with IACS PR 25
- having implemented a documented system for qualification and continuous updating of the knowledge and competence of MarSec Auditors. This includes theoretical training and training in security systems and procedures relevant to the certification process as well as practical training under supervision
- monitoring the continuing trustworthiness of the MarSec Auditors
- monitoring MarSec Auditors in accordance with IACS PR 6 at least once every two years
- maintaining appropriate measures to avoid unauthorized disclosure of, or access to, security-sensitive material
- having knowledge of the requirements of SOLAS XI-2, the ISPS Code, relevant national and international legislation and security requirements
- having knowledge of current security threats and patterns
- having knowledge of recognition and detection of weapons, dangerous substances and devices
- having knowledge of recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security
- having knowledge of techniques used to circumvent security measures
- having knowledge of security and surveillance equipment and systems and their operational limitations
- approving SSPs and amendments to a previously approved SSP
- assigning qualified MarSec Auditors to carry out shipboard verifications (if more than one auditor is assigned to carry out a specific verification, one of them has to be appointed as the Lead MarSec Auditor)
- performing of shipboard verifications
- evaluating verification reports from MarSec Auditors
- issuing of ISSCs (including Interim ISSCs)

¹ GL as RSO meets the competence requirements outlined in ISPS Code part B/4.5 and those outlined in MSC/Circ. 1074 Appendix 1, paragraphs 3 to 5



Germanischer Lloyd

- reserving the right to perform additional verifications, if deemed necessary by GL
- reserving the right to check the associated procedures of the Safety Management System (SMS) and review security-related procedures during the ISPS Code certification process

3.2. The Company

For the purpose of these guidelines, the company has to ensure the following duties and responsibilities according SOLAS XI-2 and ISPS Code including, but not limited to, the following:

- designating of a Company Security Officer (CSO) acc. ISPS Code A / 11
- performing of a documented Ship Security Assessment (SSA) including on-scene security survey for each individual ship according ISPS Code A / 8
- designating of Ship Security Officers (SSO) for each individual ship acc. ISPS Code A / 12
- developing of a Ship Security Plan (SSP) for each individual ship acc. ISPS Code A / 9
- 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 according ISPS Code A / 6
- ensuring that the SSP together with the documented SSA is submitted to GL for review and approval according ISPS Code A / 9.1 and A / 9.2
- ensuring the implementation and maintenance of the SSP onboard by the CSO and SSO according ISPS Code A / 11.2.3 and A / 12.2.2
- ensuring that training, drills and exercises on ship security are carried out for all relevant personnel acc. ISPS Code A / 13
- ensuring that records of the activities addressed in the SSP are kept onboard according ISPS Code A / 10
- ensuring that Declarations of Security (DoS) are completed, if required according ISPS Code A / 5
- ensuring that the ship always acts on the security levels set and ensuring the implementation of the security measures appropriate for those security levels according ISPS Code A / 7
- ensuring the onboard verification of the security system by GL according ISPS Code A / 19
- ensuring that a valid ISSC is issued and maintained onboard the ship after successful completion of the verification acc. ISPS Code A / 19

For the purpose of these guidelines, the company has to ensure the following duties and responsibilities related to the certification process.

- having clear objectives how to satisfy the requirements of SOLAS XI-2 and the ISPS Code
- considering the establishment of a security policy stating how the objectives of the above requirements are to be achieved (suggested but not mandatory)
- ensuring that during the performance of the SSA and the development of the SSP the relevant requirements of SOLAS XI-2 and ISPS Code Part A have been taken into account.
- ensuring that paragraphs 8.1 – 13.8 of ISPS Code part B have been given particular consideration and that those considered relevant by the company have been addressed in the SSP. This has to be documented by the company in its SSP.
- ensuring that all non-compliances identified by GL during the review of the SSP are properly corrected and that objective evidence for this has been submitted to GL for review prior the SSP being approved



Germanischer Lloyd

- ensuring that, prior to the initial verification, at least one security drill has been performed, the security equipment has been properly tested, calibrated and maintained, and that training for all shipboard personnel on ship security has been provided (objective or documentary evidence for the above to be available on the occasion of the initial verification)
- ensuring that all relevant information, issued under the provisions of the statutory conventions and class rules to which the ship is certified and classed, is provided to GL
- informing GL of any relevant changes including name and address of the Company, flag, class or other significant details of its ships, and any other developments resulting in changes of their security system and any associated security equipment
- ensuring that the initial, intermediate and renewal verification is performed only under operating conditions and with the ship fully manned in accordance with the Safe Manning Certificate
- informing GL if the ship identified on the ISSC is out of operation (out of service) for a period exceeding three (3) months
- notifying GL of due dates for intermediate, renewal and additional verifications 10 to 14 days in advance
- nominating person(s) to liaise with the MarSec Auditor
- agreeing with the MarSec Auditor on time and performance of shipboard verifications at the opening meeting
- co-operating with the MarSec Auditor, to permit the verification objectives being achieved
- informing the shipboard personnel about the objectives and scope of the verification
- appointing responsible members of staff to accompany the MarSec Auditor
- providing all resources needed by the MarSec Auditor to ensure an effective and efficient certification process
- providing access and evidential material as requested by the MarSec Auditor
- maintaining verification reports for a minimum period of 5 years
- resubmitting ISSCs which become invalid for any reason
- ensuring that internal audits and reviews of the security activities are carried out at least once every twelve (12) months onboard each ship. This includes that records of any non-compliances identified, any corrective action applied relative to the identified non-compliances, and copies of internal audit reports and reviews are maintained on board the ship
- ensuring any amendments to the security system, the security equipment and the approved Ship Security Plan are submitted to GL for review and approval prior implementation on board

The verification and certification of compliance with the requirements of the ISPS Code does not relieve the company, its management, its seafarers of their obligation to comply with national and international legislation or security levels in the area they are employed or operating.

3.3. The MarSec Auditor

For the purpose of these guidelines, duties and responsibilities of the MarSec Auditor include the following:

- reviewing and approving the SSP
- communicating and clarifying the non-compliances immediately
- preparing the shipboard verification
- performing the shipboard verification effectively and efficiently
- organizing special technical assistance required to fulfill the compliance requirements



Germanischer Lloyd

- ensuring that the shipboard verification is conducted in compliance with the requirements of SOLAS chapter XI-2, the ISPS Code, relevant national, international legislation and directives
- verifying that the security system and any associated security equipment of the ship fully complies with the applicable with the requirements of SOLAS chapter XI-2 and the ISPS Code and is in satisfactory condition and fit for service for which the ship is intended
- verifying the implementation of the security system as outlined in the SSP
- ensuring during the onboard verification that the requirements of the SSP has been implemented
- planning and carrying out the assigned verification effectively and efficiently
- reporting the verification results clearly, conclusively and without undue delay
- issuing the relevant verification documents, including any certificate, if authorized, to the ship and forwarding all relevant documents to GL Head Office according “Instructions for the Performance of ISPS Shipboard Verifications”, Annex 1 to 5
- reporting any obstacles encountered in performing the verification
- verifying actions taken by the Ship/Company as a result of the verification
- supporting the Auditor/Lead Auditor (if the verification is performed by a team)
- ensuring confidentiality of documents pertaining the certification and treating privileged information with discretion
- encouraging companies to adopt recommended guidelines and standards developed by the IMO, Administrations and classification societies into their SSP and relative guidelines

All personnel participating in the ISPS Code certification process shall ensure confidentiality of documents pertaining to the certification and treating privileged information with discretion.

4. Certification Procedures

4.1. Criteria for certification

Criteria for verification of compliance with the requirements of the ISPS Code shall be in accordance with the applicable sections of the SOLAS XI-2 and the ISPS Code Part A

The ISSC shall only be issued when it can be demonstrated during the verification that ISPS Code Part B/ 8.1 to 13.8 have been taken into account

GL will not verify the implementation of an SSP that GL has not approved. However, in cases where the Administration has not delegated the responsibility for SSP approval, or where SSP approval is carried out by another IACS society or non IACS Society acting as RSO, or due to transfer of certification, this may be necessary. In such cases GL will consider each application for certification on a case by case basis.

In cases where the SSP review and approval is carried out by an organization other than GL, GL has the right to perform a full review of the SSP prior or during the shipboard verification. Final decision to be made by GL H.O.

During the validity of the ISSC, GL will not approve amendments to any SSP which initially was approved by another RSO or flag Administration. In other words, GL will only approve amendments of SSPs which has been initially approved by GL itself.



Germanischer Lloyd

GL has implemented a documented system ensuring that the certification process is performed in compliance with IACS PR 24. This system includes, inter alia, procedures and instructions for the following:

- contract agreements with Companies in respect of their ships
- scheduling and performing SSP approvals and verifications
- reporting results from SSP approvals and verifications
- issuing of ISSCs (including Interim ISSCs)

4.2. Certification Process

4.2.1. General Requirements

SSP review and approval and on-board verification shall:

- determine that the SSP and/or amendments to a previously approved SSP meet the provisions for the three security levels as defined by the ISPS Code on behalf of the flag Administration
- determine compliance with the approved SSP on board ships
- determine the effectiveness of the implementation of the SSP on board ships

The MarSec Auditor is entitled to acquire any information he needs from any other RSO or, if relevant the flag State administration, in order to check the veracity of the information presented to him by the Company or ship management personnel.

Initial, intermediate and renewal onboard verifications will be performed only under operating conditions and with the ship fully manned in accordance with the Safe Manning Certificate.

4.2.2. Application for certification

A Company seeking ISPS Code certification is requested to contact GL Head Office (department BSML) or one of its local offices in written form. Upon receipt of such an enquiry, GL Head Office or one of its local offices shall provide the Company with a "Questionnaire for ISPS Code certification" and the form "Application for the Certification of a Ship Security System".

Upon receipt of the completed questionnaire, GL will prepare an "Offer for ISPS Code Certification" to be submitted to the Company. If the Company accepts the offer, the completed and signed application form has be returned to GL Head Office indicating the acceptance of the offer.

Once the signed application form is received by GL Head Office the certification process can commence consisting of the following steps:

- Review and approval of the SSP
- Verification and certification of ships



Germanischer Lloyd

GL may provide the Company with a copy of the "Verification List for Ship Security Plan Approval". To facilitate the certification process, the Company is invited to complete this list by marking the references between the requirements and the relevant sections of its SSPs.

4.3. Review and approval of the SSP

4.3.1. General

The Company is to prepare and submit to GL a SSP for each of its ships for review and approval. The SSP and amendments are to be accompanied by the SSA from which the SSP has been developed.

In order to maintain the secure integrity of SSPs and SSAs, GL requires that such documents to be either hand carried or to be sent by a courier mail service with a tracking capability to GL Head Office.

4.3.2. Documentation Requirements

In addition to the documentation requirements specified in SOLAS XI-2 and ISPS Code part A, the documented SSP shall address the provisions specified in ISPS Code part B, which are considered relevant by the Company, and as well as the following:

- the SSP has to contain a statement that the relevant provisions of ISPS Code part B (paragraphs 8.1 – 13.8) have been taken into account by the Company during the development of the SSP and that all provisions of those paragraphs have been addressed which are considered relevant (The above paragraphs to be taken into account are specified in MSC/Circ.1097)
- evidence must be available that the SSA report has been reviewed and accepted by the Company according ISPS A/8.5
- If possible security threats acc. ISPS Code B/8.9 are not considered in the SSA, the SSA has to contain a statement by the Company clearly outlining the reason why these points have not been considered relevant
- the SSA report has to indicate the following acc. ISPS Code B/9.3:
 - Type of ship and cargo carried
 - Area in which the ship is currently employed and for which the SSP has been developed (e.g. voyage schedule)
 - Composition of the crew employed on board the ship and for which the SSP has been developed (e.g. crew list)
- The SSP has to contain a list of ship's particulars acc. ISPS Code B/9.1
- in cases where the Master is not the SSO, the SSP has to establish that the SSO has the authority on board to enable the duties and responsibilities acc. ISPS Code A / 12.2 to be carried out effectively
- The SSP has to identify all access points to the ship
- The SSP has to identify security systems and equipment provided on board acc. ISPS Code B/9.2.3 and 9.7.5
- If the SSP does not establish that the CSO and appropriate shore-based company personnel have knowledge of and received training acc. ISPS Code B/13.1, the company



Germanischer Lloyd

should submit objective evidence indicating that the CSO and appropriate shore-based company personnel are duly qualified to carry out assigned tasks. (This might be done, for example, by a company statement or the certificate of attendance of a training course)

- the SSP has to establish that all shipboard personnel should have sufficient knowledge of and be familiar with the relevant provisions of the SSP and their assigned security duties according to the knowledge requirements of ISPS Code B/13.4 (This might be done, for example, by security familiarization, briefings, practical demonstrations, drills and exercises)
- the SSP has to establish that drills and exercises are carried out in frequencies specified in the ISPS Code B/13.6 and 13.7
- the SSP has to establish procedures to ensure that internal audits and reviews of the SSA and SSP are conducted at least once every 12 months and additionally when it is identified that the SSP/SSA are inappropriate. (This might be identified during training, drills, or following a security incident and in response to experience or when circumstances identified in the SSA significantly change, e.g. change of trade, change of composition of the crew, change of cargo carried, etc).

The SSP shall be written in the working language, or working languages, of the ship. If the language, or languages, used is not English or German a certified translation into one of these languages is to be provided. For approval purposes the SSP version written in English, French or Spanish will only be considered.

4.3.3. Performance

This SSP will be reviewed and approved on behalf of the administration of the ship's flag State based on the requirements of SOLAS XI-2 and ISPS Code part A the relevant provision of part B, as well as additional national requirements.

During the review process it will be determined that the SSP and/or amendments have met the provisions for the three security levels as defined by part A of the ISPS Code, taking into account paragraphs 8.1 to 13.8 of part B of the ISPS Code.

Working documents are to be used by the MarSec Auditor according "Instructions for Review and Approval of Ship Security Plans".

Working documents should not restrict additional activities or investigations which may become necessary as a result of information gathered during the review.

If, during the review of the SSP, it has been found that the SSP is not in compliance with the applicable requirements, GL will inform the Company about any identified non-compliances.

It is then the Company's responsibility to rectify the detected non-compliances and to ensure that all non-compliances are properly corrected and that objective evidence for this will be submitted to GL for review prior the SSP to be approved.

When GL has reviewed the SSP and the SSP has been found to be in compliance with the applicable requirements, GL will consider the SSP as approved.



Germanischer Lloyd

Evidence should be sought that the CSO has received training in compliance with ISPS Code A/13.1. If evidence is not provided by the Company or there is objective evidence that the CSO has not received such training, the MarSec Auditor shall inform the Company and shall require evidence that such training will be received prior to the SSP approval.

To indicate this approval, GL will stamp and retain copies of the following pages:

- SSP approval letter
- SSP title page
- SSP index
- SSP revision history

All other pages of the approved SSP will be appropriately marked to indicate approval.

When a company wishes to keep its SSP in an electronic format, GL will review the SSP and will print the pages stated above. To indicate the approval of the SSP GL will stamp those pages as approved. GL will keep copies of those pages indicating the approval.

The process of verification of implementation of approved amendments shall be decided by GL H.O. but may require an additional shipboard verification to be performed.

4.3.4. Follow-up

Once the review and approval of the SSP has been finalized, GL will return the SSP together with an SSP approval letter to the Company.

4.4. Verification of ships

4.4.1. Initial and renewal verification

“Initial” verification means verification before the ship is put into service or before the ISSC is issued for the first time. This shall include a complete verification of the ship’s security system and any associated security equipment.

“Renewal” verification means verification at intervals specified by the flag State administration, but not exceeding five (5) years. This verification shall ensure that the ship’s security system and any associated security equipment remains in full compliance with the applicable requirements.

The initial or the renewal verification consists of the following steps:

- verification through a representative sample that the security system, i.e. operational (non technical) security measures specified in the SSP, is being implemented effectively,
- 100 % verification of all security equipment, i.e. technical security measures specified in the SSP, is in all respects satisfactory, i.e. is fully operational and is fit for the service for which it is intended, complies with applicable requirements and has been maintained and calibrated in accordance with the provisions of SSP and the manufacturer’s instructions.



Germanischer Lloyd

Note: The verification through representative sample shall be to the level necessary for the MarSec Auditor to verify the whole operating system.

On satisfactory completion of the verification an ISSC with a limited validity not exceeding five (5) months will be issued by the MarSec Auditor, if authorized. A copy of this ISSC and the verification documents shall be transmitted to GL Head Office for evaluation according Annexes 1 to 5 of "Instructions for Performance of ISPS Shipboard Verifications".

Upon satisfactory completion of the evaluation of the verification report, GL Head Office will issue a "full term" ISSC, if authorized. A copy of the ISSC and a copy of the verification report will be transmitted to the flag State administration as soon as practical, if required.

If not authorized by the flag State administration to issue ISSCs, GL Head Office will transmit a copy of the verification report as soon as possible,

If the above verifications are not satisfactorily completed, i.e. "non-compliances" are identified, an ISSC is not to be issued

4.4.2. Intermediate and additional verification

"Intermediate" verification means verification between the second and the third anniversary date of the ISSC. This shall include an inspection of the ship's security system and any associated security equipment to ensure that it remains satisfactory for the service for which the ship is intended. Such verification will be endorsed on the ISSC.

"Additional" verification means verification as determined by the flag State administration, by GL or by officers duly authorized officers of a Contracting Government.

The intermediate verification consists of the following steps:

- verification through a representative sample that the security system, i.e. operational (non technical) security measures specified in the SSP, is being implemented effectively,
- 100 % verification of all security equipment, i.e. technical security measures specified in the SSP, is in all respects satisfactory, i.e. is fully operational and is fit for the service for which it is intended, complies with applicable requirements and has been maintained and calibrated in accordance with the provisions of SSP and the manufacturer's instructions.

The scope of additional verification depends on the nature and/or extent of the identified non-compliances or failures.

4.4.2.1. Failures that compromise the ship's ability to operate at security level 1 to 3

If at an intermediate or additional verification, the MarSec Auditor identifies through objective evidence a "failure" in the security system or any associated security equipment that **does** compromise the ship's ability to operate at security levels 1 to 3, the MarSec Auditor will report



Germanischer Lloyd

immediately to the company who should contact the flag State administration and include the “Remedial Action Plan” proposed by the company or the ship.

If authorized by the flag State administration to do so, the MarSec Auditor will verify the implementation of any “alternative security measures” and approve the “remedial action plan” before the ship sails.

An additional verification will be requested from the flag Administration to be carried out before the expiry date of the approved Remedial Action Plan to verify that the Remedial Action Plan has been completed, i.e. that the agreed and approved corrected actions have been implemented and /or the ship has returned to its original condition as specified in the SSP.

4.4.2.2. Failures that do not compromise the ship’s ability to operate at security level 1 to 3

If at an intermediate or additional verification, the MarSec Auditor identifies through objective evidence a “failure” of the security system or any associated security equipment, or the suspension of a security measure which **does not** compromise the ship’s ability to operate at security levels 1 to 3, the MarSec Auditor will report immediately to the company who should contact the flag State administration and include the Remedial Action Plan proposed by the Company or ship.

If authorized to do so, the MarSec Auditor will approve the remedial action plan. The completion of the Remedial Action Plan will be verified no later than the next scheduled verification.

4.4.3. Shipboard Verification Process

4.4.3.1. Preparation

GL assigns a MarSec Auditor to conduct the verification or an audit team, where necessary. The shipboard verification shall only be performed if there is objective evidence that the ship has on board an approved SSP.

4.4.3.2. Performance

The shipboard verification shall be performed according “Instructions for the Performance of ISPS Shipboards Verifications” taking the relevant Annex to the instruction into account.

Each verification will consist of an opening meeting, collecting objective evidence and of a closing meeting.

Verification documents shall be issued according the relevant Annex of “Instructions for the Performance of ISPS Shipboard Verifications”.

Should any technical or other operational deficiencies be noted these should be communicated to the organization issuing the relevant certificate, by using the communication procedures described in section “Communication with flag State administrations and other IACS societies” of these guidelines.



Germanischer Lloyd

4.4.3.3. Follow-up

4.4.3.3.1. Evaluation of verification reports

GL H.O. will evaluate the verification documentation and finally decide on the issuance of an ISSC. If certification is not granted, GL Head Office will inform the Company and detail any required corrective actions to satisfactorily complete the certification process. GL Head Office will verify the implementation of corrective action as considered necessary which may include an additional verification.

4.4.3.3.2. Identification of technical or other operational deficiencies

Where the MarSec Auditor identifies technical or other operational deficiencies during a shipboard verification, which are likely to present a serious threat to safety or harm to the environment, he shall verify if the Company has taken appropriate action to correct the technical or operational deficiencies and if the responsible class society has been informed accordingly. In any case the MarSec Auditor shall ensure, that technical or other operational deficiencies found are dealt with by the responsible class society by using the communication procedures described in section "Communication with flag States and other IACS societies" of these guidelines.

4.4.3.3.3. Communication with flag State administrations and other IACS societies

In case technical or other operational deficiencies are identified during a shipboard verification the MarSec Auditor shall inform the flag State administration and society having the ship in class via GL Head Office in writing.

4.5. Duration and validity of certificates

4.5.1. Certificates issued or endorsed after initial or renewal verification

The ISSC will be issued by GL Head Office after satisfactory initial or renewal verification.

Renewal verification shall take place at intervals not to exceed five (5) years and should be carried out within the three (3) months prior to the expiry date of the existing certificate.

On satisfactory completion of the verification, to facilitate the evaluation of the verification report prior to the issue of the "full-term" certificate, an ISSC with a limited validity not exceeding five (5) months will be issued by the MarSec Auditor.

This "full term" ISSC certificate will be valid for a period specified by the flag State administration, but not exceeding five (5) years.



Germanischer Lloyd

When the renewal verification is satisfactorily completed within three months before the expiry date of the existing certificate, the new certificate will be valid from the date of the completion of the renewal verification to a date not exceeding five (5) years from the date of the existing certificate.

When the renewal verification is satisfactorily completed more than three months before the expiry date of the existing certificate, the new certificate will be valid from the date of the completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

When the renewal verification is satisfactorily completed after the expiry date of the existing certificate, the new certificate will be valid from the date of the completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

When the renewal verification has been satisfactorily completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the MarSec Auditor on behalf of the Administration may endorse the existing certificate for a period not exceeding five (5) months from the expiry date.

When a ship, which it is to be verified, is at the time when the certificate expires not in a port, the flag State administration may extend the period of validity of the certificate, but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified.

No certificate shall be extended more than three (3) months for this purpose.

Documented evidence from the flag State administration granting this request will be reviewed by GL prior to endorsement of extension.

4.5.2. Certificates endorsed after intermediate and additional verification

The ISSC will be endorsed after satisfactory intermediate verification and after any satisfactory additional verification.

Intermediate verification shall take place between the second and third anniversary date of the certificate.

When an intermediate verification is satisfactory completed before the period specified above, then:

- the expiry date shown on the certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was satisfactory completed;
- the expiry date may remain unchanged provided one or more additional verifications are carried out.

Initial, Intermediate or Renewal verification may be carried out in conjunction with an ISM audit of the ship. For that purpose, at the request of the Company, the expiry date of ISSC may be harmonized to the expiry date of the Safety Management Certificate (SMC).



Germanischer Lloyd

4.5.3. Interim certification

An Interim ISSC can only be issued after 1 July 2004 for the following reasons:

- a ship without a certificate, on delivery or prior to entry or re-entry into service,
- transfer of a ship from one flag Administration to the flag of another Administration,
- transfer of a ship to a signatory Administration from one that is not a signatory Administration,
- a Company assumes the responsibility for the operation of a ship not previously operated by the Company.

If a ship re-enters the management of the Company after a “reasonable” period of time under the management of others, confirmation will be sought from the administration as to whether it is appropriate to issue interim certification.

An Interim ISSC shall be valid for six (6) months. No extensions can be granted.

4.5.4. Invalidation of Certificates

An ISSC will cease to be valid in any of the following cases:

- relevant verifications not carried out within the periods as specified above.
- if the ISSC is not endorsed as specified above
- the Company operating ceases to operate that ship,
- upon transfer of the ship to the flag of another flag State.

4.5.5. Withdrawal of Certificates

If GL has reasons for invalidating an ISSC, these reasons are to be communicated to the ship and to the flag State administration.

The communication is to be limited to the identity of the ship, the Company, the reason for invalidation and the date of the verification or date of withdrawal.

An ISSC shall be withdrawn by the flag State administration or by GL on their behalf in the following circumstances:

- the alternative security measures agreed are not in place
- the approved remedial action plan has not been complied with

In case GL has withdrawn an ISSC under the above circumstances, GL will only re-issue the ISSC following a review and approval of a newly submitted SSP and an additional verification with the scope of an initial verification of the ship.

The expiry date of the new ISSC will be that of the withdrawn ISSC.

In case the ISSC has not been issued by GL, GL will only recommend the withdrawal to the flag State Administration.