Procedures for Certification of International Code for the Security of Ships and of Port Facilities

General Guidelines for Application, Verification and Certification

Doc. No. : ISPS 01
Revision : 5

Korean Register

36, Myeongji ocean city 9-ro, Gangseo-gu, Busan, 618-814, Rep. of Korea
Tel: +82 70 8799-8250
Fax: +82 70 8799-8319

Rev. No.	5	Procedures for Certification of International Code for the Security of Ships and of Port Facilities	Page	1

I. Revision Records

Revision No.	Effected Date	Content
0	2004. 01.09	- Established
1	2004.11.01	- Revised Reflected IACS PR 24(5.4, 6.5, 8.2.1, 11.7.3, 11.7.4) Specified application criteria (10.8), Inserted circumstances leading to invalidation of the certificate (12.4.2). Simplified kinds of verifications (12.4.5). Revised terms (Center → KR, audit → verification, additional audit → special verification etc.) *only some of the amended terms have been underlined*.
2	2005.07.11	- Revised Deleted an article that stipulated that verification shall not be undertaken for a ship which had its SSP not approved. Added some precedent requirements for interim verification.
3	2011.07.01	- Revised Reflected IACS PR 24(2.20~2.26, 5.4, 7.1~7.7)-
4	2012.01.01	- Revised Change the name of “System Certification Steering Committee” into “ISM Certification Steering Committee”.
5	2017.09.01	- Revised Change of Application form and Reflect the new KR logo

II. Contents

Chapter	Subject	Page
Ⅰ	Revision Records	1
Ⅱ	Contents	2
1	Objective	3
2	Scope	4
3	Definitions	5
4	General	7
5	Company's Responsibilities	8
6	Application for Verification	10
7	Verification Plan	11
8	Audit Process	12
9	Preliminary verification	15
10	SSP Approval	16
11	Verification of ships	17
12	Issuance, endorsement and maintenance of the ISSC	19
13	Transfer of Certification Body	22
14	Management of Verification Schedule	23
15	Complaints and Appeal	24
16	Confidentiality	25
	Forms	26
	Annex	27

1. Objective

The objective of this document is to provide ship owners, ship managers and ship management related persons with the necessary procedures for the approval of the Ship Security Plan and/or the undertaking of security verifications in accordance with the International Code for the Security of Ships and of Port Facilities under the provision of the SOLAS Chapter XI-2.

2. Scope

2.1 These procedures apply to the ships of the companies that are applying for the certification in accordance with the ISPS code.

2.2 These procedures stipulate general items such as the application for verification, verification scope, verification procedures and issue and/or maintenance of International Ship Security Certificate ("Security certificate") in accordance with the ISPS code

2.3 Any verification rules or regulations that are specially required by individual flag State shall supercede procedures herein.

3. Definitions

3.1 "International Ship and Port Facility Security (ISPS) Code" means the International Code for the Security of Ships and of Port Facilities consisting of Part A (mandatory) and part B (recommendatory), as adopted, on 12 December 2002, by resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 and as may be amended by the Organization in the future.

3.2 "Ship Security Assessment (SSA)" means identification of threats that may exist against the current security countermeasures, weak points and/or essential shipboard operation business with respect to shipboard infrastructures, policies and/or procedures.

3.3 "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.

3.4 "Security System" means a security system implemented on board to maintain procedures, documentations and/or relevant records in compliance with the ISPS Code

3.5 "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 port facility security officers.

3.6 "Company Security Officer (CSO)" means the person designated by the company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.

3.7 "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.

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

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

3.10 "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.

3.11 "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.

3.12 "Major Failure" means the non-fulfillment of a specified requirement that compromises the ship's ability to operate at security levels 1, 2 or 3. It may also be referred to as a Major Non-conformity.

3.13 "Failure" means the non-fulfillment of a specified requirement that does not compromise the ship"s ability to operate at security levels 1, 2 and 3. It may also be referred to as a Non-conformity.

3.14 "Observation" means a statement of fact made during an audit and substantiated by objective evidence. It may also be a statement made by the auditor referring to the SSP which, if not corrected, may lead to a Failure in the future.

3.15 "Audit" means a process of systematic and independent verification by obtaining objective evidence to determine whether the ship security related activities comply with the ISPS-Code and the planned arrangements of the SSP and whether these arrangements are implemented effectively to achieve the objectives of the ISPS-Code.

3.16 "Verification" is confirmation through the evaluation of objective evidence that specified requirements have been fulfilled.

3.17 Terms not otherwise defined herein shall have the same meaning as the meaning attributed to them in the SOLAS chapter XI-2 and/or ISPS Code Part A and B.

4. General

4.1 The security verifications shall be carried out in accordance with the SOLAS chapter XI-2 and/or ISPS Code Part A.

4.2 In addition to 4.1, an ISSC shall only be issued after it is verify that the section 8.1 though the section 13.8 of the ISPS Code Part B has been duly considered.

4.3 Where it is found that Korean Register of Shipping (hereinafter calls KR) has been involved in the implementation or establishment of the SSP of a specific ship, KR shall not execute the SSP approval activity or shipboard verification for such ship.

4.4 When it is found that a SSP which has not been approved by KR does not conform to the SOLAS chapter XI-2 and has not reflected ISPS Code Part A and section 8.1 to section 13.8 of Part B after reviewing the SSA and the SSP according to 5.3, KR shall inform it to the company and the Administration.

4.5 When a ship is not classed with the member or associate of IACS, KR shall not perform the SSP approval or the verification of such ship, except where permitted by the Administration.

4.6 The following shall be verified when undertaking SSP approval and the verification in accordance with the ISPS Code.

4.6.1 On behalf of administration, whether the SSP and its amendments are in agreement with the requirements of 3 security levels
4.6.2 Appropriate implementation of the requirements of ISPS Code on board.
4.6.3 Effectiveness of implementing SSP on board.

4.7 A security verification shall only be undertaken in normal operating conditions with at least the minimum number of crewmembers on board as described on the Safety Manning Certificate.

4.8 A security verification demonstrating compliance with the ISPS Code does not mean that the company, mangers and crew of a ship are exempted from the responsibilities to observe national laws and international laws or security levels in their business areas.

5. Company's responsibilities

The company has the responsibility to meet the following in relation to security verification and maintenance of certification:

5.1 Preparation for verification

- to secure necessary verification environment,
- to explain the objective and scope of the verification to its personnel,
- to designate the responsible person who will the verification team,
- to provide the verification team with necessary resources for effective and efficient verification process,
- to allow auditors access to, or provide them with an evidence required,
- to cooperate with the verification team for attaining its verification objective, and
- to commit and carry out corrective action for any failures identified during the verification

5.2 Internal security verification and review of security activities

The company shall carry out an internal security verification and review security activities of each ship in its fleet at least once a year. The company for the verification and review should present the following:

- the record of failures identified
- the corrective action taken against the failures
- the copies of internal security verification record kept on board

5.3 Where a SSP has not been approved by KR (refer to chapter 4.4), the company shall allow KR to review the SSA and/or SSP before executing the verification.

5.4 Responsibilities for notifying information (of amendments of a SSP and/or system failures)

5.4.1 Where the company wishes to revise the following parts of a SSP, the SSP shall be submitted to KR for its re-approval. This only applies in case where KR has initially approved the SSP.

- alteration of security system
- change of security equipment
- alteration of the parts related to the regulations of ISPS Code Part A/9.4.1 to 9.4.18

5.4.2 In case where a major failure that will compromise the ship's ability to carry out security duties associated with security level 1 to 3 is identified during a voyage, the company shall immediately report such major failure to KR together with the immediate action and corrective action schedule to prevent recurrence. While in a port If the ship is in a port, the company shall also report such non-compliance to the port authority.

Furthermore, if the ship is expected to pass through any coastal state on route, the coastal state shall also be notified.

5.4.3 In case where a failure that will not compromise the ship's ability to carry out security duties associated with security level 1 to 3 is identified during a voyage, the company shall report such failure to KR with immediate action and corrective action schedule to prevent recurrence.

5.5 Maintenance of verification records

The company shall maintain all internal verification records and external verification records at the company and the ship for at least 5 years. In case where a certain guideline from flag state, relative data shall be maintained by the guideline.

6. Application for verification

6.1 When requesting a SSP approval, the company shall submit the SSP according to the procedures described in the chapter 10 of this document.

6.2 The company shall apply for verification at least 30 days in advance of the proposed verification date by submitting an "Application for Ship Audit (SA-04-01, 2/2)".

6.3 In case where the company applying for a verification is other than the ship owner, the company shall, along with an "Application for Ship Audit", submit a document (or report to the relevant administration) which proves that the company is the entity that is defined in the SOLAS Chapter Ⅸ-1. However, the submission of document may be exempted if the company recorded in the SMC issued by KR and the company recorded in the Application for Ship Audit are same.

6.4 Where the SSA is written in a language other than Korean or English, the company shall also submit the English version of SSA. The company shall also submit a SSP written in English when the SSP is written in a language other than English.

6.5 When applying for SSP approval, the company is also to submit a document that proves that the CSO has completed training in accordance with ISPS Code A/13.1.

7. Verification plan

7.1 A security verification, except for interim verification described in the chapter 11 herein, shall only be undertaken in normal operating conditions with at least the minimum number of crew members on board as described on the Safety Manning Certificate. No verification is to be carried out when the ship is in dry-docking or in lay-up.

7.2 The verification plan shall be established on the basis of the submitted “Application for Ship Audit” and shall be sent to the company not later than 2 days before the verification date.

7.3 A provisional auditor may be included in the verification team with the agreement of the company.

8. Audit process

8.1 Opening meeting

A team leader shall briefly explain the verification purpose, scope and verification and certification procedures to the ship's master and/or the SSO.

8.2 Verification

8.2.1 Verifications shall be executed to confirm that:

- the approved SSP is available on board
- the security system is being implemented effectively on board through representative sampling
- all security equipment specified in the SSP complies with the applicable requirements
- all security equipment specified in the SSP, including the Ship Security Alert System (SSAS) on board is operational and fit for purpose

8.2.2 Verifications are executed through investigation of documents and records, interviews, observation of work activities and various other methods.

8.2.3 Verifications include checking the ship’s survey records pertaining to the ship identification number, SSAS and Automatic Information System (AIS) as well as checking whether the current ship condition is in agreement with the Continuous Synopsis Record (CSR).

8.3 SSO meeting

The audit team shall confirm the following from the SSO.

8.3.1 Whether the company is providing necessary resources to the SSO to ensure that his/her duties and responsibilities are carried out in accordance with the SOLAS Chapter XI-2 and/or ISPS Code Part A.

8.3.2 Whether the SSO is executing his/her duties and responsibilities as defined in ISPS Code Part A and has sufficient knowledge of the ship security.

8.4 Master meeting

The audit team shall confirm the following from the master:

8.4.1 Whether the company is supporting the master with necessary resources in order to ensure the execution his/her duties and responsibilities in accordance with the SOLAS Chapter XI-2 and/or ISPS Code Part A.

8.4.2 Whether the master is executing his/her duties and responsibilities as defined in ISPS Code Part A, and has sufficient knowledge of the ship security.

8.5 On-site verification

8.5.1 A verification shall be made to confirm that all security equipment specified in the SSP is operational and duly maintained.

8.5.2 Items that need to be checked to confirm the appropriate implementation of the security system shall be verified.

8.6 Preparing and submitting verification reports

8.6.1 The audit team leader shall prepare the verification report after the completion of the verification.

8.6.2 The verification report shall contain at least following data collected through the verification.

- the completion date of the verification
- the implementation status of the SSP
- the operating conditions of all security equipment and security system

8.6.3 Where identified major failures, failures or observations which can affect the issue and maintenance of the certificate are founded at any verification, the audit team leader shall record clearly and submit to the company or the ship personnel in charge.

8.6.4 The time period for corrective schedule shall not exceed 3 months from the date of identifying such failures.

8.6.5 In case where a failures with the SSP is identified amongst non-compliances of 8.6.3, the audit team leader shall inform the concerned Administration and the Recognized Security Organization (RSO).

8.6.6 If the failures of 8.6.3 is related to the items of 8.2.3, the classification society which had issued the relevant certificate should be informed.

8.6.7 In case where the company does not accept non-compliance of 8.6.3 despite a clear evidence indicating so, the audit team leader shall make a note on audit report and obtain an acknowledgment from the company. In this case, the recommendation or maintenance of certification shall be suspended.

8.6.8 KR shall inform the company of the results of the review with respect to 8.6.7 in writing not later than 15 days.

8.6.9 The company shall conduct appropriate measures with respect to the results of the KR review.

8.6.10 The audit team leader shall submit the verification report prepared in accordance with 8.6.2 and 8.6.3 to the company or the SSO. The company shall keep maintain this record in the premises accordance with 5.4.

8.7 Closing meeting

The audit team leader shall explain the results of the verification to the master and/or the SSO.

8.8 Confirmation of corrective actions

8.5.1 When a Major Failure is identified during Interim · Initial · Renewal audit the ISSC is not to be issued or renewed. Immediate action is required to restore compliance. The audit team leader shall verify the implementation of these measures before the ship sails and a schedule for the implementation of preventative action shall be agreed between the Company and the auditor to prevent recurrence. At least one additional audit shall be carried out within the period agreed for the implementation of the corrective action.

8.5.2 When a Failure is identified during Interim · Initial · Renewal audit An ISSC shall not be issued or renewed until all identified Failures have been resolved and compliance has been restored. In addition, the audit team leader shall be presented and verify a schedule for the implementation of preventative action may need to be agreed between the Company and the auditor to prevent recurrence depending on the nature and seriousness of the Failure identified. Additional audits may be carried out as necessary.

8.5.3 When a Major Failure is identified during Intermediate or Additional audit An ISSC shall not to be endorsed. Immediate action is required to restore compliance, thereby permitting the Major Failure to be down-graded. The audit team leader shall verify the implementation of these measures before the ship sails and a schedule for the implementation of preventative action shall be agreed between the Company and the auditor to prevent recurrence. At least one additional audit shall be carried out within the period agreed for the corrective action.

8.5.4 During Intermediate or Additional audit an ISSC may be endorsed following identification of a Failure, provided that a schedule has been agreed between the Company and the auditor for the completion of corrective action to restore compliance and to prevent recurrence. Additional audits may be carried out as necessary

9. Preliminary verification

9.1 The company may apply for a preliminary verification having the scope of an initial verification to KR in order to find out whether a ship is prepared for a verification.

9.2 The company has no obligation to take any corrective action against non-compliance resulting from a preliminary verification.

9.3 The favorable results of a preliminary verification will not necessarily ensure a successful certification at an initial verification. Also, KR auditors do not provide consultation services such as preparation of documents for the company.

10. SSP approval

10.1 A SSP shall be approved when it is initially established, amended, or when the ship transfers her classification.

10.2 When a SSP is submitted for approval as described in 10.1, the SSA from which the SSP has been prepared shall also be submitted.

10.3 SSA is to be carried out by persons with appropriate skills to evaluate security issues and risks of each ship.

10.4 SSA must include an on-scene survey and the following elements:

10.4.1 identification of existing security measures, procedures and operations

10.4.2 identification and evaluation of key ship board operations

10.4.3 identification and risk analysis of threats to these key shipboard operations

10.4.4 identification of weaknesses in the system, including the human element, policies and procedures

10.5 Security assessments should be performed based on the investigation of specific threat scenarios, including regular trading patterns, with consideration of the vulnerability of the ship and the consequence of those scenarios.

10.6 The company shall prepare and submit a SSP of each ship to KR for approval. KR may, however, visit the company for a SSP approval if the company request to do so.

10.7 When reviewing and approving a SSP, the auditor shall verify that the Company has taken into account relevant security-related guidance and best management practices, including the latest IMO Circulars concerning piracy, hijacking and armed robbery.

10.8 When the parts of the approved SSP requiring instructions of the Administration are amended, they shall be only after re-approval. But if there is not other instruction from the Administration, the company shall comply with requirements of 5.4.1

10.9 The amendments to the SSP shall only be approved by the RSO which initially approved the SSP unless the company has changed its certification body.

11. Verification of ships

11.1 To verify that the security system and security equipment of the ship are in satisfactory condition and in full compliance with the SOLAS Chapter XI-2 and ISPS Code, the verification shall be carried out in accordance with section 8 of this document.

11.2 The following shall be satisfactorily confirmed prior to an initial verification:

11.2.1 keeping of an approved SSP on board
11.2.2 an evidence that the security system has been implemented according to an approved SSP

11.3 Intermediate verifications shall be carried out between the second and third anniversary date of the certificate.

11.4 Renewal verifications shall be carried out at intervals not exceeding five years and within three months prior to the expiry date of an existing certificate. If a renewal verification is carried out before three months prior to the expiry date of the existing certificate, a new certificate shall be issued in accordance with the section 12 of this document.

11.5 After 1 July 2004, Interim verifications will be carried out for the following cases:

11.5.1 a ship without a certificate, on delivery or prior to entry or re-entry into service,
11.5.2 transfer of a ship from one Administration to the flag of another Administration,
11.5.3 transfer of a ship to a signatory Administration from one that is not a signatory Administration,
11.5.4 change of a company which assumes the responsibility for the operation of a ship.

11.6 The following shall be satisfactorily confirmed prior to the interim verification of 11.5.

11.6.1 completion of the SSA
11.6.2 submission of SSP for approval.
11.6.3 keeping of copied version of the SSP submitted approval on board.
11.6.4 completion establishment of SSAS on board (if relevant).
11.6.5 establishment of a 6-month implementation plan for drills, exercises and internal audit to undergo an initial verification.
11.6.6 establishment of a plan for an initial verification.
11.6.7 designation and appropriate training of SSO(s) in accordance with ISPS Code.
11.6.8 preparation of SSP in the working language on board.
11.6.9 familiarization of a master, SSO and other crew on board engaged in security duties with respect to their duties and responsibilities as specified in ISPS Code Part A and the SSP kept on board.
11.6.10 undertaking and recording of at least one drill specified in the SSP.

11.6.11 maintenance of security equipment specified in the SSP in accordance with the company maintenance system.

11.7 Special verifications are carried out in the following cases.

11.7.1 When a request is received from a flag Administration
11.7.2 When an audit is requested by PSC authority
11.7.3 When a ship is detained due to security-related accident
11.7.4 When on-scene survey is inevitable for the re-approval of the SSP.
11.7.5 When the company intends to transfer a certification body
11.7.6 When the completion of the intermediate verification is completed more than 6 months before the expiry date of the existing certificate and as a result, the expiry date of the existing certificate should be changed. However, the company may request a special verification to maintain the expiry date of the existing certificate.

12. Issuance, endorsement and maintenance of the ISSC

12.1 Issue of a certificate

12.1.1 The ISSC shall be issued after an initial verification or a renewal verification in accordance with 11.2 and 11.4.

12.1.2 The ISSC shall be valid for a period not exceeding five years.

12.1.3 At the request of the company, the expiry date of the ISSC may be harmonized with the expiry date of the Safety Management Certificate(SMC) provided that such doing does not exceed the period of five years.

12.1.4 Where the Initial, Renewal and TOSC audit has been completed with satisfaction, the Manager of a Branch Office or designated personnel from him (including verification team leader) shall issue the full term International Ship Security Certificate (ISSC). But the short term ISSC shall be issued to following flag's ship in accordance with the guideline of each administration.

- Panama(5months)
- ST.Vincent(6months)
- Korea(3months after Interim and Initial audit)

12.1.5 When a renewal verification is completed within three months before the expiry date of the existing certificate, the new certificate shall be issued from the date of the completion of the renewal verification with the validity not exceeding five years from the date of the existing certificate.

12.1.6 When a renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be issued from the date of the completion of the renewal verification with the validity not exceeding five years from the date of expiry of the existing certificate.

12.1.7 When a renewal verification is completed more than three months before the expiry date of the existing certificate, the new certificate shall be issued from the date of the completion of the renewal verification with the to a date validity not exceeding five years from the date of completion of the renewal verification.

12.1.8 If a renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of existing certificate, the certificate may be endorsed and shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

12.1.9 If a ship is not in a port at the time when the certificate expires, the 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 undergo security verification. No certificate shall be extended for more than three months. Documented evidence from the Administration granting this request is to be submitted prior to the endorsement of extension.

12.1.10 A certificate is be reissued when it is lost, damaged, revised or a change of entry has been made. The validity of re-issued certificate is the same as the original one.

12.1.11 When the company applies for the re-issue of a certificate due to a modification of entry in the certificate, a copy of the supporting document, such as a national certificate or classification certificate, shall be attached for verification.

12.1.12 The ISSC needs to be stamped in red.

12.2 Issue of an interim ISSC

12.2.1 When an interim verification is completed in compliance with the section 11 of this document, the interim ISSC shall be issued and remain valid until 6 months from the date of issue or before the issue of the full-term ISSC.

12.2.2 The extension of an interim ISSC shall be permitted under any circumstances.

12.3 Endorsement of a certificate

12.3.1 When an intermediate or additional verification is completed without any non-compliance or with non-compliance for which corrective action has been taken satisfactorily in accordance with 8.8.2 and 8.8.4, the audit team leader shall endorse on the endorsement form of the certificate so as to ensure its continuous effectiveness until the next audit.

12.3.2 If an intermediate verification is completed before the period specified in 11.3, the expiry date shown on the certificate shall be amended to a date which shall not exceed more than three years from the date on which the intermediate verification was completed.

12.3.3 If an intermediate verification is completed before the period specified in 11.3, then the expiry date may remain unchanged provided one or more additional verifications are carried out. In this case, the audit team leader shall endorse the certificate in accordance with 12.3.1. However, under no circumstance, the interval of the verifications shall exceeds three years from the verifications of the section 11.3 and 11.4 of this document.

12.4 Invalidation of a certificate

12.4.1 In the following circumstances, the relevant certificate shall be invalidated:

.1 When a verification specified in the section 11 of this document is not carried out by the due date
.2 When a certificate is not endorsed in accordance with the section 12.3 of this document
.3 When the responsible company for the ship's operation is changed
.4 When the flag state of a ship is changed
.5 When a SSP that shall be required for approval specified in 5.4 is implemented without an approval
.6 When the company's license or register is withdrawn
.7 When the corrective action for any identified failure is not completed within the agreed period
.8 When the company requests for its invalidation (including a company's waiver and/or sale)
.9 When the classification society of a ship is transferred to a class other than the member or associate of IACS (except in case where KR is the only designated RSO by the flag Administration)

12.4.2 In the following circumstances, the certificate may be invalidated after due deliberations of KR ISM Certification Steering Committee.

.1 When any significant change to the security system is not informed to KR.
.2 When the company's responsibilities as described in 5 are not observed.
.3 When certification fee is not paid.
.4 When a ship brings about public criticism e.g. PSC detention.

12.4.3 When a certificate is invalidated in accordance with 12.4.1 and 12.4.2, KR shall notify, such fact to the company, Administration and other parties concerned.

12.4.4 When the Administration approves or instructs the withdrawal of the certificate as the result of 12.4.3 or by any other reason, the company shall return the relevant certificate to KR without delay.

12.4.5 For reinstatement of the withdrawn certificate, an initial verification shall be carried out after the SSP approval. The validity of reinstated certificate shall succeed the validity of the withdrawn certificate.

13. Transfer of Certification body

13.1 In case of transferring certification from the member of associate of IACS to KR (hereinafter called "TOC"), the following procedures shall be applied and the validity of a new certificate shall succeed the validity of previous certificate.

13.1.1 TOC verification shall be a shipboard audit and shall be carried out under a condition that there is no change of flag State or the company, and shall not be carried out in the period between the SSP approval and the initial verification.

13.1.2 The company requesting the TOC verification shall notify the following to KR, and complete unresolved non-compliance raised by the previous certification body before the execution of TOC verification.

.1 whether the existing certificate is valid.

.2 whether any verification carried out by the previous certification body has been satisfactorily completed.

.3 whether any non-compliance raised by the previous certification body has been completed.

13.1.3 The scope of TOC verifications is as follows. TOC may not take place, unless the verification is satisfactorily completed.

.1 All requirements of ISPS Code.

.2 All requirements of a flag State.

.3 Any non-compliance identified by the previous certification body.

13.1.4 The TOC verification shall be carried out before the execution of any other kind of verification.

14. Management of verification schedule

KR shall notify the company at the beginning of the month (within 10th of each month) of the due range of the next verification that falls within the following month.

15. Complaints and appeal

15.1 Complaints and appeal to KR

15.1.1 The company may launch an appeal to KR for complaints in relation to a verification. The appeal can be made verbally but, in principle, it shall done in writing by preparing "Appeal for complaints (FI-11-01-04)". An appeal in relation to approval/withdrawal of a certificate or the execution of verification shall be done in writing to KR.

15.1.2 KR shall inform the result of appeal to the company in writing within a month of receipt.

16. Confidentiality

Auditors shall not reveal any information acquired during the verification to a third party. The data pertaining to a company's security system kept in KR shall not be accessed by any third party without written consent from the company, unless requested by the Administration.

Forms

Application for Ship Audit/Inspection	SA-04-01, 2/2,	01.09.2017
Appeal for Complaints	FI-11-01-04,	01.09.2017

Annex

Ship security audit scenarios

No.	Scenario	Condition	Type of Audit	Ship Security Plan	Scope of Audit and Certification
1	***Change of ship's name***	If conducted by a surveyor	Verification on board	1. Verify correct name on all certificates and in the title page, index page and revision page of SSP. 2. Change name on SSP Approval Letter (PAL) 3. Send copy of amended PAL to issuing office if appropriate. *Note: A surveyor is not authorized to issue a PAL.*	1. Amend ISSC with new name. 2. Send copy of amended certificate to issuing office. 3. Issuing office issues replacement ISSC with same expiry date as the original certificate if appropriate. *Note: One RSO cannot amend or endorse the ISSC of another.*
		If conducted by an auditor	Verification on board	1. Review and approve amendments to the SSP as required by PR24 6.4. 2. Issue replacement PAL if appropriate. A PAL should only be issued, if changes to the SSP apply, which go beyond the change of vessel's name.	1. Issue replacement ISSC with same expiry date as previous one if appropriate.
2	***Change of ship's flag***	When SSP has not yet been approved and when authorized to approve SSPs	Additional Audit	1. Carry out SSP approval. 2. Issue a PAL on behalf of the new Administration.	1. Verify compliance with the requirements of the SSP. 2. Issue a replacement certificate with the same expiry date as the original certificate.
		When SSP has not yet been approved and when **not** authorized to approve SSPs	Interim Audit	1. Check that the SSP is on board. 2. Check that SSP addresses ISPS Code A/9.4.1 to 9.4.18. 3. Check that a copy of the SSP has been submitted to the Administration or its RSO for approval.	1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC.
		When SSP has already been approved	Additional Audit	_	1. Verify compliance with the requirements of the SSP. 2. Issue a replacement certificate with the same expiry date as the original certificate.

No.	Scenario	Condition	Type of Audit	Ship Security Plan	Scope of Audit and Certification
3	***Ship more than 6 months out of service***	ISSC is not valid	Interim Verification	1. Carry out a SSP approval (if required) and issue a PAL. 2. If not authorized by the flag Administration to carry out SSP approval on its behalf, check that the SSP is on board, that ISPS Code A/9.4.1 to A/9.4.18 has been addressed and that a copy has been submitted to the flag Administration for approval.	1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC.
4	***Change from non-convention to convention***	–	Additional Audit	1. Approve SSP and issue PAL on behalf of the flag administration.	1. Issue replacement ISSC with same expiry date as non-convention ISSC.
5	***Change of Company name and address***	–	–	1. Request Company to confirm that SSP contains no amendments. Issue replacement PAL. 2. If SSP does contain amendments, company to submit SSP for approval. Issue replacement PAL.	1. Issue replacement ISSC with same expiry date as previous ISSC.

Note 1: The above instructions apply in the absence of any flag administration requirements to the contrary.
Note 2: The instructions relating to re-activation following lay-up do not apply to ships for which seasonal lay-ups are a normal part of their operational routine.

APPLICATION FOR SHIP AUDIT / INSPECTION

To : KOREAN REGISTER | **Application Date :**

APPLICANT

Company Name **Address**			Signature or Official Stamp
	Tel :	Fax :	E-mail :
Person in Charge		M.P. :	E-mail :

We acknowledge the obligation of the company prescribed in the relevant KR rules and procedures, and also agree to pay all audit fees and expenses which will be incurred as a result of the audit.

SHIP INFORMATION

Ship's Name :	IMO No. :
Ship type :	Registry date :
Flag :	Port of Registry :
Class :	Class No :
Gross Tonnage :	Nationality of crew :
DOC Issued by:	Expiry date of DOC :

SHIPBOARD AUDIT/INSPECTION REQUEST (Check "✓" as applicable)

Type	Interim	Initial	Interme-diate	Annual	Renewal	Additional	Reason of Additional audit
ISM	☐	☐	☐	☐	☐	☐	
ISPS	☐	☐	☐	☐	☐	☐	
MLC	☐	☐	☐	☐	☐	☐	
SSP	Approval	☐	Re-Approval		☐	Reason of Re-approval :	
DMLC II	Review	☐	Re-review		☐	Reason of Re-review :	
Desired verification date and place :							
Expired date of SMC or ISSC or MLC :					SSP approved(or submitted) date :		
Internal audit date of ISM or ISPS					DMLC Part II approved(or submitted) date :		

INVOICE CHARGE (Check "✓" as applicable)

INVOICE CHARGE (Check "✓" as applicable)					
Kind of Invoice :	☐	Invoice (Except Korean Company)	☐	Tax invoice (incl. VAT)	☐ Tax invoice (excl. VAT)
BILLING CONTACT : When the billing contact and applicant are different, please fill out the followings.					
Company Name : Address : Tel : Fax : E-mail :					

Agent Information	Company's name	Person in Charge	
		Mobile :	
	Tel :	Fax :	E-mail :

Guide for Application

○ **Ship type :**

Ship type should be selected below one(s) :
Passenger Ships / Passenger HSC / Oil Tankers / Chemical Tankers / Gas Carriers / Bulk Carriers / Cargo HSC /Other Cargo Ships / MODU

○ **Registry date :**

Registry date can be obtained in the ship's CSR (Continuous Synopsis Record)

○ **Class and Class No :**

Class and Class No. should be filled out if the Class of ship is not KR

○ **Reason of additional audit**

If you select an additional audit. you have to write the reason considering the below examples:
- Change of RO (RSO) / PSC request / change of ship's name / revisit caused by down-graded major N/C / other

○ **SSP approved (or submitted) date**

Please write SSP approved date in case where you request Initial audit and write SSP submitted date in case where you request Interim ISPS audit.

○ **Approved (or submitted) date of DMLC Part II**

- Initial MLC inspection : write the approved date of DMLC Part II
- Interim MLC inspection : write the submitted or approved date of DMLC Part II

○ **Attachment**

● **ISM audit attachment**
- A copy of DOC if a DOC was issued by other certification body
- A copy of ISM Company Declaration (if applicable)

● **ISPS audit attachment**
- A copy of ISM Company Declaration (if applicable)
- A copy of letter or an approved front page of SSP if it was approved by other certification body

● **MLC audit attachment**
- A copy of letter or a reviewed front page of DMLC part II if it was reviewed by other certification body

○ **SSP approval**

Please send an application by e-mail(kr-ssp@krs.co.kr) with below documents :
- SSP file (PDF) / SSA / CSO training certificate / Ship's registry certificate / ISM Company Declaration (if applicable)

○ **DMLC part II review**

Please send an application by e-mail(kr-dmlc@krs.co.kr) with below documents :
- DMLC part I & part II (PDF) / On board complaint procedure / C.B.A (if applicable) / BBC Charter party agreement or Ship management agreement / S.E.A /applicable document If the ISM system documents was referred to DMLC Part II / ISM Company Declaration(if applicable)

Appeal for Complaints

Korean Register

Ref. No. : **Date :**

Company Name			**Department**		
Applicant		**Telephone**		**Fax**	

Please review our complaint(s) and inform us of the results

Subject : _____

Attachment	**□ Yes □ No**	**Page(s):**	**(including this page)**