International Ship and Port Facility Security (ISPS) Code

- The ISPS Code applies to passenger ships and high speed passenger craft, cargo and high speed craft 500 GRT and upwards, and mobile offshore drilling units. The Code does not apply to warships, naval auxiliaries, or other ships owned or operated by Contracting Government and used only on non-commercial service.
ISPS Code

The ISPS Code, which came into force on July 1, 2004, raises the issue that ensuring the security of ships and port facilities is basically risk analysis activity and that to determine what security measures are appropriate, a risk assessment must be conducted in each particular case.
The requirements for ships

- Company security officers
- Ship security officers
- Ship security assessment
- Onboard security surveys
- Ship security plans
- Onboard management provisions and equipment
The requirements for port facilities

- Port facility officers
- Port facility security assessment
- Port facility security plans
- Shore-side management provisions and equipment
The elements in port facility security assessment

- The identification and evaluation of important assets, infrastructures, areas and structures that may cause significant loss of life or damage to the economy of a port facility or environment if damaged.
- The identification of the actual threats to those critical assets and infrastructure in order to prioritise security measures.
- A statement of vulnerability of the port facility by the assessment of its weaknesses in physical security, structural integrity, protection systems, procedural policies, communication systems, transportation infrastructure, utilities and other areas within a port facility that may be a likely target.
Threats

Security risk could be regarded as a function of the threat of an attack associated with the vulnerability of the object and the consequences caused by such attack. **Threat** could be defined as an action or potential action likely to cause damage, harm or loss. If explained quantitatively, it would be a measure of the likelihood that a specific type of attack will be initiated against a specific target.
Vulnerability and consequences

- **Vulnerability** is a weakness in any system or equipment, or in procedures designed to protect assets. Its quantitative description could be the likelihood that various types of safeguard measures against a scenario would fail. **Consequence** (impact) is either the amount of expected loss or damage, or it is the negative effects in the shipping industry should the attack be successful.
The requirements for both ships and port facilities

- Monitoring and controlling access
- Monitoring the activities of people and cargo
- Ensuring security communications are readily available
Responsibilities of Contracting Governments

- Setting applicable security levels.
- Approving Ship Security Plan and amendments.
- Verifying the compliance of ships with SOLAS XI-2 and part A of the ISPS Code.
- Issuing the International Ship Security Certificate.
- Determining which port facilities are required to designate a Port Facility Officer.
Responsibilities of Contracting Governments

- Ensuring completion and approval of the port facility security assessment and the port facility security plan and amendments.
- Exercising control and compliance measures.
- Issuing the Statement of Compliance of a port facility.
- Communicating security information to the IMO and to the shipping and port industries.
The duties of Company Security Officer (CSO)

- Advising the level of threats likely to be encountered by the ship using appropriate security assessment and other relevant information.
- Ensuring that ship security assessment is carried out.
- Ensuring the development, the submission for approval and thereafter the implementation and maintenance of the ship security plan.
- Ensuring that the ship security plan is modified as appropriate to correct deficiencies and satisfy the security requirements of the individual ship.
- Arranging for internal audits and reviews of security activities.
The duties of Company Security Officer (CSO)

- Arranging for the initial and subsequent verifications of the ship by the administration or the recognised security organisation.
- Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspection and verifications of compliance are promptly addressed and dealt with.
- Enhancing security awareness and vigilance.
- Ensuring adequate training for personnel responsible for the security of the ship.
The duties of Company Security Officer (CSO)

- Ensuring effective communication and cooperation between the ship security officer and the relevant port facility security officer.
- Ensuring consistency between security and safety requirements.
- Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.
The duties of Ship Security Officer (SSO)

- Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained.
- Maintaining and supervising the implementation of the ship security plan, including any amendments to the plan.
- Co-ordinating the security aspects of the handling of cargo and ships stores with other shipboard personnel and with the relevant port facility security officers.
The duties of Ship Security Officer (SSO)

- Proposing modifications to the ship security plan.
- Reporting to the CSO any deficiencies and non-compliance identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions.
- Enhancing security awareness and vigilance on board.
- Ensuring that adequate training has been provided to shipboard personnel as appropriate.
- Reporting all security incidents.
The duties of Ship Security Officer (SSO)

- Co-ordinating implementation of the ship security plan with company security officer and the relevant port facility security officer.
- Ensuring that security equipment is properly operated, tested, calibrated and maintained.
Objectives of the CSO/SSO/PFSO training

- Understand the requirements for a ship or port security assessment
- Initiate, direct and evaluate the ship/port security plan
- Manage and monitor the ship or port security systems
- Ensure that the proper training and evaluation is carried out for all personnel involved in security matters
- Implement and maintain the security plan
- Train, direct and motivate ship or port personnel involved in security
Outline of the training course by DNV

- Duties of the CSO, SSO and PFSO
- SOLAS/ ISPS Code
- Ship or Port Security Assessment (SSA or PSA)
- The Threat
- Threat Scenarios
- Port-State Security
- SSA or PSA Exercise
- Weapons and WMD
- Port Facility Overview
- Ship Security Plan
- Security Levels
- Crowd Control
- Security Equipment
Certificate of Completion

Alexander Reckling
Date of Birth: 19.09.1969, Place of Birth: Hannover
Nationality: German

has from 25.06.2004 until 27.08.2004 successfully completed the following course:

Port Facility Security Officer (PFSO)

The following skills were obtained with the goal to enhance the awareness for Port Security:
- Relevant international conventions, codes and recommendations incl. responsibilities and functions of the government and other relevant security organizations
- Methodology of port security assessment
- Implementation and evaluation of the port facility security plan
- Methods of port security surveys and inspections
- Coordinating the security aspects of all ship and port operations and conditions
- Competences in contingency preparedness and contingency planning
- Handling sensitive security-related information and communication incl. reporting all security incidents
- Knowledge of current security threats and patterns
- Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security
- Knowledge about security equipment and systems, in any case their operational limitations incl. detection of weapons and dangerous substances
- Multitude of combating audits, inspections, control and monitoring
- Instruction techniques for security trainings and exercises

This training course is based on COLAS XI.2 in connection with the International Ship and Port Facility Security Code (ISPS Code) and the STCW Convention. The course meets the requirements of Chapter 17, Part A of the ISPS Code combined with Chapter 14, 15, 16 & 18 of Part B.

Duration: 18 lessons & 60 minutes.

Issued in Hamburg,
27.08.2004

Managing Director
CSO/SSO training course certificate
PFSO training course certificate

DET NORSKE VERITAS
TRAINING COURSE CERTIFICATE

Issued under the provisions of DNV Seafarer™ Standard for Certification of Learning Programmes

Port Facilities Security Officer Course

Issued by:

Hadson Marine Management Services
Shekows Corporate Center II
4709 Hadsonfield Road
Suite 302
Fremont, NJ 08080
USA

THIS IS TO CERTIFY that the above-mentioned course has been reviewed by DNV and that upon completion of the course DNV is satisfied that the course was in compliance with the DNV Seafarer™ Standard for Certification of Learning Programmes and the following other standards:

- Regulations 18.1 of Part 8 of the International Ship Port Facility Security Code
- ISO 14001
- BS OHSAS 18001
- ISO 9001

Important assumptions and conditions related to maintenance and delivery of the course are found in:


Provided the requirements for retention of the certificate will be complied with and unless the certificate has been withdrawn (this Certificate is valid until):

2008-01-06

Issued at Havik on 2005-01-07 for Det Norske Veritas AS

[Signatures]

Review

Head of Function

Det Norske Veritas, Veritasveien 1, NO-1322 Havik, Norway. Tel. +47 67 77 99 00, Telefax: +47 67 77 99 11
Obligations of the company

- The appointment of the CSO and SSO.
- The development of the security procedures.
- The incorporation of the security-related practice into the shipping safety-related drills.
- A clear statement contained in the ship security plan, emphasising the Master’s overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance from the Company or any Contracting Government if necessary.
Obligations of the company

- The necessary support for the CSO, Master and SSO to fulfill their duties and responsibilities in accordance with Chapter XI-2 and the ISPS Code of SOLAS.
Ship security assessment (SSA)

- Identification of existing security measures, procedures and operations.
- Identification and evaluation of key ship board operations to be protected.
- Identification of possible threats and the likelihood of their occurrence.
- Identification of security weakness, including human factors in the infrastructure.
The ability required by CSO when conducting SSA

- Knowledge of current security threats and patterns.
- Recognition of weapons, dangerous substances and devices.
- Methods used to circumvent security measures and cause security incidents.
- Familiarity of marine engineering, ship and port operations.
The information needed when conducting SSA

- The general layout of the ship.
- The location of areas which need to have restricted areas.
- The location and function of each actual or potential access point to the ship.
- Changes in the tide which may have an impact on the vulnerability and thus, the security of the ship.
- Cargo spaces and stowage arrangements.
- Locations where the ship stores and essential maintenance equipment is stored.
The information needed when conducting SSA

- Locations where unaccompanied baggage is stored.
- Emergency and stand-by equipment available to main essential services.
- Number of ship personnel, any existing security duties and any existing training requirement practices of the Company.
- Existing security and safety equipment for the protection of passengers and ship personnel.
The information needed when conducting SSA

- Escape and evacuation routes and assembly stations which need to be maintained.
- Existing agreements with private security companies providing ship and waterside security services.
- Existing security measures and procedures in effect, including inspection and control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents, alarms, lighting, access control etc..
The identification of important elements to be protected when conducting SSA

- Ship personnel, passengers, visitors, port facility personnel, repair technicians etc..
- Cargo, in particular dangerous goods.
- Ship security communication equipment and systems.
- Ship security surveillance equipment and systems.
Possible threats to be considered by SSA

- Damage to, or destruction of the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism.
- Hijacking of the ship or persons onboard.
- Tampering with cargo, essential ship equipment or systems or ship stores.
- Unauthorised access or use, including presence of stowaways.
- Smuggling weapons or equipment.
Possible threats to be considered by SSA

- Use of the ship to carry those intending to cause a security incident.
- Use of the ship itself as a weapon or as a means to cause damage or destruction.
- Attacks from seaward whilst at berth or at anchor.
- Attacks whilst at sea.
Security guidance to be determined when conducting SSA

- Restricted areas.
- Response procedures to fire or other emergency conditions.
- Level of supervision of the ship personnel, passengers, visitors, vendors, repair technicians, dock workers etc..
- Frequency and effectiveness of security patrols.
Security guidance to be determined when conducting SSA

- Access control systems, including identification systems.
- Security communication system and procedures.
- Security doors, barriers and lighting.
- Security and surveillance equipment and systems.
On-scene ship security survey (OSS)

- What is the function or what is stored here?
- What are the regular security measures?
- Who does what?
- When was it last done?
- What actually happens?
- How does the responsive security measure really work?
Ship security plan (SSP)

- Measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorised from being taken on board the ship.
- Identification of the restricted areas and measures for the prevention of unauthorised access to them.
- Measures for the prevention of unauthorised access to the ship.
Ship security plan (SSP)

- Procedures for responding to security threats or breaches of security, including the provisions for maintaining critical operations of the ship or ship/port interface.
- Procedures for responding to any security instructions Contracting Government may give at security level 3.
- Procedures for evacuation in case of security threats or breaches of security.
- Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects.
Ship security plan (SSP)

- Procedures for auditing the security activities.
- Procedures for training, drills and exercises associated with the plan.
- Procedures for interfacing with port facility security activities.
- Procedures for the periodic review of the plan and for updating.
- Procedures for reporting security incidents.
- Identification of the SSO.
- Identification of the CSO including the 24-hour contact details.
Ship security plan (SSP)

- Procedures to ensure the inspection, testing and maintenance of any security equipment provided on board.
- Frequency for testing any security equipment provided on board.
- Identification of the locations where the ship security alert system activation points are provided.
- Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting.
The ISPS security levels

- Security level 1: the level of which minimum appropriate protective security measures shall be maintained at all times.
- Security level 2: 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: 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.
Missions of SSOs in security level 1

- Brief crewmembers on watch on any special security conditions.
- Deploy a 24-hour deck watch/roving patrol.
- Issue a Ship security bill designating personnel assignments.
- Equip the Watch Officer and Engine Room Watch Officer with portable hand-held communication devices.
- Secure all identified access points.
- Strictly control access on and off the ship; verify the identity of all persons.
- Search the baggage and all carry-on items before embarkation.
- Limit and/or restrict access to critical ship areas to authorized personnel.
Missions of SSOs in security level 1

- Raise and/or secure all ladders, ramps, and gangways when not in use.
- Illuminate the main deck, all active access points, and the inboard/outboard sides during periods of darkness.
- Verify the cargo and the ship’s stores against a manifest.
- Verify the integrity of the cargo and ship’s stores to ensure there has been no tampering.
- Restrict access to the cargo area at sea.
- Keep unmanned areas, such as storerooms, locked.
- Secure all hatchways in controlled areas.
- Conduct spot checks to ensure security at access points.
- Activate security equipment, such as alarms, automatic intrusion detection devices, and surveillance cameras.
Missions of SSOs in security level 2

- Assign additional personnel to guard access points.
- Assign personnel to guard restricted areas.
- Increase the frequency and detail of security patrols.
- Coordinate waterside boat patrols with the port facility.
- Limit the number of access points; identify and secure closed access points.
- Advise passengers and crew not to leave packages/baggage unattended.
- Check seals on containers and other cargo lockers.
- Provide security briefings to all crew and passengers on any specific threats and the need to be vigilant.
Missions of SSOs in security level 2

- Maintain close communications with security authorities.
- Provide additional shore side lighting by coordinating with the port facility.
- Restrict access to the bridge, engine room, and other restricted areas to specific crewmembers.
- Escort and strictly control all visitors.
- Advise shore authorities if a visitor declines to accept security measures.
- Augment bridge watches and lookouts.
- Increase verification and checking of cargo and ship’s stores.
Missions of SSOs in security level 3

- Modify crew liberty of shore leave so the Master can get underway on short notice.
- Limit access to a single location.
- Restrict visitor access to official business; continuously escort all visitors.
- Post additional personnel to ensure the ship perimeter is constantly under surveillance.
- Intensify roving patrols, especially on deck.
- Assign a Watch Officer to all active ladders, ramps, and gangways.
- Consider postponing the delivery of all stores.
- Prohibit all vehicles, workboats, and barges from coming alongside while at port.
Missions of SSOs in security level 3

- Place additional light on the main deck, access areas, and inboard/outboard sides at night.
- Lay out fire hoses at access areas and ensure they can be manned on two-minute’s notice.
- Check all crew lockers and storage locations.
- Inspect the hull while in port and where practical.
- Lock all door/hatches from the inside to control access.
- Brief all personnel on potential threats, procedures, and the necessity to remain vigilant.
- Get or stay underway, if necessary and possible.
Crucial security related actions onboard ships

- Monitoring access to the ship.
- Monitoring the deck areas and areas surrounding the ship.
- Monitoring the embarkation of persons and their carry-on items.
- Supervising the handling of cargo and ship stores.
Missions for monitoring restricted areas to ensure authorised persons only in security level 1 by SSO

- Instruct crew on what are restricted areas and who has access permissions.
- Lock or otherwise prevent access to unattended spaces where passengers and visitors may have access such as storerooms, auxiliary machinery rooms, etc.
- Lock and secure access points.
- Utilize surveillance equipment, such as closed circuit TV (CCTV).
- Deploy security guards and patrols.
- Utilize automatic intrusion detection devices to alert the crew of unauthorized access to restricted areas.
Missions for monitoring restricted areas to ensure authorised persons only in security level 2 by SSO

- Secure additional access points and areas adjacent to access points.
- Utilize continuously monitoring surveillance equipment such as CCTV.
- Dedicate personnel to guarding and patrolling restricted areas.
- Use additional automatic intrusion devices on areas adjacent to restricted areas.
- Provide security briefings to all crew prior to ship or cargo operations on any specific threats and the need for vigilance and reporting of suspicious persons, objects, or activities.
- Increase the frequency and detail of inspecting persons, carryon items for prohibited weapons, explosives, etc.
Missions for monitoring restricted areas to ensure authorised persons only in security level 3 by SSO

- Secure all access points and areas adjacent to access points.
- Post personnel to continuously guard all restricted areas.
- Assign personnel to continuously patrol restricted areas and areas adjacent to restricted areas.
- Deny access to additional areas in proximity to the security incident or believed location of the security threat.
- Search restricted areas as part of a security sweep of the ship.
Procedures of controlling access to the ship performed by SSO in security level 1

- Verify everyone’s identity before allowed onboard.
- Deny or revoke a person’s authorization to be on board if unable or unwilling to establish ID. Any such events must be reported to SSO and CSO.
- In liaison with port facility, ensure that secure areas are established, in which inspection of vehicles and their contents can take place (this is especially critical for Car Carriers, RO/RO ships and other passenger ships).
- Limit and/or restrict access to critical ship areas to authorized personnel.
Procedures of controlling access to the ship performed by SSO in security level 2

- Assign additional personnel to guard access points.
- Limit the numbers of access points to the ship; identify closed access area and the means to secure them.
- Assign additional personnel to patrol decks during periods of reduced ship operations.
- In coordination with a port facility, extend perimeter security beyond the immediate port area.
Procedures of controlling access to the ship performed by SSO in security level 3

- Assign additional personnel to guard access points and areas adjacent to access points.
- Limit entry to the ship to a single access point.
- Protect electronic information systems.
- Grant access only to those responding to the security incident or threat.
- Evacuate the vessel.
- Move the vessel.
Methods for monitoring of deck areas and areas surrounding the ship in security level 1 by SSO

- Deploy guards and patrols.
- Utilize automatic alarms and surveillance equipment.
- Illuminate a Ship’s deck and access points to a ship when conducting Ship/port interface activities.
- Use maximum available lighting consistent with safe navigation while underway.
- Ensure that security equipment or system failures or malfunctions are identified and corrected.
Methods for monitoring of deck areas and areas surrounding the ship in security level 2 by SSO

- Increase the frequency and detail of security patrols.
- Increase the use of security equipment.
- Assign additional personnel as security lookouts.
- Coordinate waterside boat patrols with the port facility.
- Provide additional shore side lighting by coordinating with the port facility.
- Coordinate with shore-side foot or vehicle patrols, when provided.
Methods for monitoring of deck areas and areas surrounding the ship in security level 3 by SSO

- Increase the number and frequency of security patrols to ensure continuous monitoring.
- Increase the number and frequency of waterside boat patrols with the port facility to ensure continuous monitoring.
- Use spotlights and floodlights to enhance the visibility of the deck and areas surrounding the Ship.
- Use lighting to enhance the visibility of the surround water and waterline.
- Use divers to inspect the underwater pier structures prior to a Ship’s arrival, upon the Ship’s arrival, and in other cases deemed necessary.
- Initiate measures, including slow revolution of propeller(s), to deter underwater access to the ship hull.
Procedures for controlling the embarkation of persons and their effects in security level 1 by SSO

- Segregate embarking and disembarking passengers,
- Verify the reason personnel are embarking from the Ship by using tickets, boarding passes, and work orders.
- Inspect persons and their belongings before being allowed onboard (crew is not required to engage in inspection/screening of other crewmembers).
- Ensure checked persons and their personal effects are segregated from unchecked persons.
Procedures for controlling the embarkation of persons and their effects in security level 2 by SSO

- Provide security briefings to all crew and passengers prior to departing on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.
- Increase the frequency and detail of inspecting persons, carry-on items for prohibited weapons, explosives, etc.
- Positively identify personnel prior to each embarkation.
Procedures for controlling the embarkation of persons and their effects in security level 3 by SSO

- Inspect all persons, carry-on items for prohibited weapons, explosives, etc.
- Provide security briefings to all crew and passengers, prior to each embarkation and disembarkation, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.
- Escort all service providers or other personnel who need to board.
- Assign additional personnel to guard designated areas.
- Assign personnel to continuously patrol designated areas.
- Increase the detail and frequency of controls used for people boarding the ship.
- Suspend embarkation or disembarkation.
Methods for supervising the handling of cargo and ship’s stores in security level 1

- Verify the cargo and the Ships stores against a manifest.
- Unless unsafe to do so, routinely check cargo and storage spaces prior to cargo handling or stores delivery, for evidence of tampering.
- Verify the integrity of the cargo and Ships stores to ensure there has been no tampering using equipment as described by the Company Security officer:
  - visual and physical examination;
  - scanning/detection equipment, canines, etc.; and/or
  - coordination with the shipper or other responsible party.
- Ensure stores are controlled or immediately and securely stowed following delivery.
Methods for supervising the handling of cargo and ship’s stores in security level 2

- Increase the frequency and detail of checking cargo and cargo spaces for evidence of tampering
- Intensify checks to ensure that only intended cargo is loaded
- In liaison with facility, increase frequency and detail in checking seals and other methods used to prevent tampering
- Increase frequency and detail of visual and physical inspections
- Coordinate enhanced security measures with the shipper or other party in accordance with established agreement and procedures
Methods for supervising the handling of cargo and ship’s stores in security level 3

- Verify all cargo and ship’s stores against the manifest.
- Continuously conduct visual and physical examination of the cargo and ship’s stores.
- Suspend loading or unloading of cargo
- Restrict or suspend delivery of vessel stores and bunkers (up to refusing to accept vessel stores onboard)
- Verify the inventory and location of any hazardous materials carried on board.
Declaration of security (DoS)

A DoS is a declaration that address the security requirements that could be shared between a port facility and a ship (or between ships) and will state the responsibility for security each shall take.
Request of the completion of a DoS by a ship/port when

- Operating at a higher security level than the port facility or another ship it is interfacing with.
- An arrangement exists on a DoS between Contracting Governments, covering certain international voyages or specific ships on those voyages.
- There has been a security threat or a security incident involving the ship or involving the port facility.
- The ship is at port which is not required to have and implement an approved port facility security plan.
- This ship is conducting ship-to-ship activities with another ship not required to have and implement an approved ship security plan.
Security records

- Training, drills and exercises.
- Security threats and security incidents.
- Breaches of security.
- Changes in security level.
- Communications relating to the direct security of the ship such as specific threats to the ship or to port facilities.
- Internal audits and reviews of security activities.
- Periodic review of the SSA and SSP.
- Implementation of any amendments to the plan.
- Maintenance, calibration and testing of any security equipment provided on board, including testing of the ship security alert system.
Functions of recognised security organisations (RSO)

- Approval of ship security plans or amendments.
- Verification and certification of compliance of ships.
The competency of an RSO

- Expertise in relevant aspects of security.
- The knowledge of the requirements of chapter XI-2 and part A of the ISPS Code and relevant national and international legislation and security requirements.
- Appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design and construction if providing services in respect of port facilities.
- The capability of assessing the likely security risks that could occur during ship and port facility operations and how to minimise such risks.
The competency of an RSO

- The knowledge of current security threats and patterns.
- The knowledge on recognition and detection of weapons, dangerous substances and devices.
- The knowledge on recognition of characteristics and behavioral patterns of persons who are likely to threaten security.
- The knowledge on techniques used to circumvent security measures.
- The knowledge of security related equipment and systems and their operational limitations.
Training for all ship crewmembers

- Security awareness training.
- Understanding the relevant provisions of the SSP.
Security drills

- Damage to or destruction of the ship.
- Hijacking of the ship.
- Hostage taking onboard.
- Tampering with cargo, essential ship equipment or systems or ship stores.
- Unauthorised access, including presence of stowaways.
- Smuggling of weapons or equipment.
- Use of the ship to carry persons or equipment intended to cause damage or destruction.
- Attacks from seaward whilst at berth or at anchor.
- Attacks whilst at sea.
Certification of ship security

Upon successful completion of the initial verification, an International Ship Security Certificate will be issued. The certificate is issued either by the administration or a Recognised Security Organisation acting on behalf of the administration.
Ceases of the ISSC validity

- If the relevant verifications are not completed within the periods specified.
- If the certificate is not endorsed in accordance with the Code.
- When a vessel undergoes a change of the ownership or management.
- When a vessel changes the flag.
Issue of interim certificates

- A ship is on delivery or prior to its entry or re-entry into service.
- A vessel changes the flag.
- A vessel changes flag from a State which is not a Contracting Government.
- A vessel undergoes a change of ownership or management.
- A vessel undergoes the first verification conducted by the administration or an RSO and during the period of correcting the deficiencies which will be examined by a subsequent verification.