

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ



ΤΜΗΜΑ: ΝΑΥΤΙΛΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ
ΣΠΟΥΔΩΝ: ΝΑΥΤΙΛΙΑΚΗ ΔΙΟΙΚΗΤΙΚΗ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΚΑΤΕΡΙΝΑ
ΔΙΑΜΑΝΤΑΡΑ

TITΛΟΣ: HOW INTERNAL AUDIT HELPS IN MANAGEMENT OF
COMPLIANCE

ΠΕΙΡΑΙΑΣ

ΣΕΠΤΕΜΒΡΙΟΣ 2019

Contents:

1. How an internal audit helps the company to comply with ISM and ISPS Code?
(p.2-4)
2. Internal Audit (p.4-5)
3. ISM Code (p.5-6)
4. Reports and analysis of non - conformities(p.6)
5. ISPS Code part A (p.6-10)
6. Declaration of security (p.10)
7. ISPS Code part B (p.10-12)
8. The role of RSO (p.12-13)
9. Port State Control Requirements and control of ships(p.13-14)
10. Verification of ISPS Code (p.14-16)
11. Health and Safety management (p.16-17)
12. Emergency Preparedness (p.17-18)
13. Critical Operations (p.18-19)
14. Critical Equipment (p.19-21)
15. Training and familiarization (p.21)
16. Familiarization of new personnel (p.21 - 22)
17. Management leadership and commitment (p. 22-23)
18. Internal Auditor (p.23)
19. Sqa Representative (p.23-24)
20. Vessel Risk Assessment (p.24-26)
21. Office Risk Assessment (p.26-27)

How an internal audit helps the company to comply with the ISM and ISPS Code?

In every owning or managing shipping company there are methods that should be followed according to the ISM and the ISPS Code, for the safety, environmental protection and security according to the procedures. In order to review her vessels each company arranges internal audits to be ensured that all equipment on board the vessel is well, and the personnel on board is well trained and familiarized with the company's procedures. Every seaman on board the vessel do trainings for the better familiarization with the procedures, equipment on board, and to react in the best way in emergency situations such as fire, collision of the vessel, grounding of the vessel or an injury or death of the personnel. Internal audit on board the vessel is done by company's personnel, Marine Superintendents and Superintendent Engineers. Marine Superintendents and Superintendent Engineers come on board each company's vessel to do ISM, ISPS and Navigational audits. During the audits, superintendents, check, review the vessel's equipment (that everything works according to the procedures), that the vessel is seaworthy aiming to the protection of the environment, her cargo, its entity and her personnel (crew), and all the procedures and works on board the vessel have as priority the safety according to the ISM and the ISPS Code. In the case that the superintendent observes a curious situation that could lead to an injury, accident or loss, he should write non-conformity (ies) to the vessel and preventive and corrective actions that should be followed in order to resolve the said problem. Follow up is needed for the completion of this procedure. Each internal audit on board the vessel or in the company should focus on the requirements of the safety management system of the company. Internal audit of the company should be done in all departments in a period that will not exceed the 12 months (1 year). The base scope and the frequency that audits are conducted should be followed according to the requirements of the safety management system of each company, and the regulations and procedures related to the safety, environmental protection and the security. In order to accomplish an internal audit, we need an audit plan, and the results should be published for example observations or non-conformities and the procedure of follow-up should be followed. An action plan is needed in the case of non-conformities, in order to establish corrective actions and verify the corrective action effectiveness. The procedure that should be followed during an internal audit is the planning and scheduling of the audit, the conducting of audits, it follows the procedure of reporting the results of the audit

and the corrective and preventive actions taken for any deficiencies or non-conformities exist. During the closing of the internal audit we have the procedures of the following up and the records filing. Every company should also do at periodically times, do management reviews and reviews to her personnel in the company and on board the vessel to be ensured that safety management system continues to act according to the ISM code, and all the procedures of the company are followed according to this procedures which are aiming to the safety and pollution prevention. Every vessel, in order to be seaworthy, has to carry on board a safety certificate according to the ISM Code and the company's procedures. On the other hand, each managing or owning company has to have the document of compliance which is issued to the company for a period of 5 years by the Administration or the recognized security organization. The document of compliance is valid only for vessels' types that each company has. The document of compliance should be verified between the second and the third anniversary date. The document of compliance should be withdrawn by the administration or the recognized administration , if the annual verification is not done or if there is evidence of major non – conformities with the ISM Code (non – compliance). A copy of document of compliance should also exist on board the vessel. An interim document of compliance maybe issued in order to facilitate initial implementation of the Code when the company is newly established and new vessel types are added in to the existing document of compliance. The validity of interim certificate is 12 months. In special cases, the validity of an interim document of compliance may be extended in a period that not exceed the 6 months after a request by the Administration of the Company. Interim verification of the document of compliance maybe issued to verify that the document of compliance of the interim document of compliance is relevant to the vessel concerned, that safety management system of the company is followed according to the Code, and internal audits are conducted to ensure and review the regulations of the ISM and the ISPS Code according to the safety, pollution prevention and security followed in the company and on board the vessels. All verifications of the certificates on board the vessel and in the company should be in accordance with the procedures of the Code.

The scope of internal audit is to entire the safety management system of a Company to all departments, all elements, all personnel and all vessels. The documentation that exists in each internal audit verifies that the vessel or the company complies with any

new regulation and the management reviews results are implemented. In this way, with an internal audit, we can easily identify the functional areas of the company, the processes or activities that are followed in the company or on board the vessel. With an internal audit each company develops procedures and identify controls in order to avoid any incident, accident or any disastrous event. During the internal audit we determine the safety and/ or environmental importance of this process. With the procedure of an internal audit it should be mentioned that the system is checked and not the persons and ensures the full cooperation of all employees in order to expedite this procedure. The follow – up or verification are needed to confirm that the corrective actions were implemented and verify that non – conformity or non-conformities have not re-occurred through further sampling. To sum up, the internal audit helps not only the vessel but also the company to evaluate the system for continual improvement, for the safety, protection of the environment and security as referred in the regulations, procedures and rules of the ISM and the ISPS Code.

INTERNAL AUDIT:

The purpose of this procedure is to verify that the Company's activities and results comply with planned arrangements and the requirements of a) the ISM Code, b) the ISO 9001:2008 requirements, c) the ISO 14001:2004 requirements, d) the OHSAS 18001:2007, e) the ISO 50001:2011 requirements and as a result of all these is that the documented Company's Management System is effective. This procedure applies to internal audits carried out for all systems of the Company's Management as implemented in the Head Office and on board vessels.

The SQE Manager shall establish annual internal audit schedules for the office in Cooperation with the SQE Representative and for the managed vessels, in cooperation with the DPAs. For the Company's departments, the schedule shall be of sufficient scope to ensure that all critical and core aspects of the Company's Management System are audited at least once per Annum at intervals not exceeding 12 months. For the managed vessels, Company's Management System shipboard audits shall be conducted at least twice per year, at intervals not exceeding 12months, for all activities/procedures, except those related to ISPS Code and Ship Security Plan (security audits), which shall be conducted at least once per year, at intervals not exceeding 12 months. If circumstances permit, shipboard security audits will be combined with Company's Management System audits. When a new Master is

employed by the company, shipboard audit shall be carried out within 3 months from the time he has taken over the command to ensure his adherence to company values and Management System.

The company shall also periodically verify whether all those undertaking delegated ISM-related Tasks are acting in conformity with the company's responsibilities under the ISM Code. The verification shall be implemented with the internal audits in the office and onboard the Vessels. The schedule shall be approved by the Managing Director of the company. Additional follow-up audits may be arranged, as deemed appropriate. The audit schedules are reviewed and revised, if deemed appropriate. Prior to any planned office audit, the SQE Manager shall agree with the department to be audited the audit date(s) and scope of the audit. Similarly, the responsible DPA shall notify the vessels of the scheduled shipboard audits. Each audit shall be carried out by a trained auditor, independent of the process/department to be audited by using audit check lists, when applicable, which will require the department or vessel being audited to provide objective evidence of compliance with the applicable sections of the Management System. Results of previous audits are also taken into consideration by the auditor. When deficiencies within, or departure from the Company's Management System are identified during the audit, the auditor shall issue non-conformity reports and a time limit will be set for the implementation of corrective and preventive action(s). Observations may also be raised for areas of the Company's Management System requiring improvement. Non-Conformities and observations are duly registered and monitored.

The completed audit report shall consist of a summary report, for office audits or an Audit check list for shipboard audits and, where necessary, non-conformity reports and agreed taken corrective action, as appropriate. Each audit report shall be numbered and dated and completed within 15 days from the audit date in the case of the office audits. For the vessel audits, the audit report shall be completed within 15 days from Marine Superintendent's return to the office.

The audit reports shall be circulated as follows for the office audits: a. SQE Manager, b. Department Manager (as applicable) and the c. Managing Director.

For shipboard audits the audit reports shall be circulated as follows: a. SQE Manager, b. Marine Superintendent responsible for the vessel (if other than auditor), c. All Department Managers, d. Managing Director. The original audit reports are maintained by the SQE Representative for the office departments and by the DPA / Company's

Security Officer (CSO) for the managed vessels, while copies are also maintained by the responsible Department Managers and Masters of the concerned vessels, respectively.

ISM Code:

According to the ISM Code, a safety management system of a Company should ensure compliance with the mandatory rules and regulations of the Code, and consideration of all applicable Codes, guidelines and standards recommended by the International Maritime Organization, Administrations, classification societies and maritime industry organizations. The ISM Code requirements should be applied to all vessels (all types of vessels: RO/RO, passenger vessels, and merchant - cargo vessels).

One of the most significant aims of the ISM Code is the construction of a Safety Management System which will be unique for each Company. With the construction of a Safety Management System, according to the ISM Code, every single owning or managing shipping company, will have a safety and environment protection policy, defining the level of responsibility and authority of each person on board the vessel and offshore, and defining the lines of communication between the vessel and the Company. A safety management system will conduct to safe vessels' operations, to the protection of the environment and of the sea, to the accident reporting and preventing the incidents to become accidents, identifying the level of risk and the measures that should be taken. It should also reporting in a safety management system the non- conformities and the major non- conformities, the internal audits, the management review and the emergency preparedness in case that we have an emergency situation.

In order to enhance the safety and the protection of the environment, the Company must ensure that all the procedures and guidelines of the ISM Code, are followed step by step not only on board the vessel but also in the Company (offshore). In order to maintain a safety management system of the Company, internal audits are conducted to review that all guidelines, rules and regulations of the Code, concerning the safety and the environmental protection are followed by the Company. "The Company according to the requirements of the Code should define and document the responsibility, authority and interrelation of all personnel who manage, perform, and verify work relating to and affecting safety and pollution prevention." The most common way that a company uses to show the relationship between the shore side and the vessel personnel, and their

duties and responsibilities, according to the safety and the protection of the environment is the use of an organization chart. In this organization chart of the company, it should be referred the duties, the responsibilities and the authority of personnel who manage, perform or verify work, affecting safety and pollution prevention according the ISM Code. In the Safety Management system, of each company, it should be indicated that the company will be responsible have adequate resources and shore - based support in order to help the designated person(s), to accomplish his task for the safety and the protection of the environment. In the Company's resources may be included: the equipment and materials, the money, the technical resources and well trained personnel (trained auditors), experience of all personnel in all the vessel types that a company manages. The designated person(s), is a person authorized by the company and is the link between the office and the vessels, and the shipboard personnel. The designated person must have direct access to the highest level of management and his responsibilities and authority should include the monitoring, the safety, and the pollution prevention from the operation of the vessels and to ensure that adequate resources and well trained personnel is used on board the vessels and in the Office. A designated person has the role of the "management representative" in a quality or environmental management system, but should not be directly responsible for the safety management system implementation. The responsibilities and the authorities of the designated person of the company are referred to the ISM Code 3.2. Master's responsibility and authority: the Company should ensure that the safety management system is also operating onboard the vessel. The Master of the vessel has authority and responsibility to make decisions about safety and pollution prevention according to the safety management system and request Company's assistance as may be necessary. The company should be ensured that the Master of the vessel is well qualified for the command of the vessel and his crew, is fully trained about safety management system and Companies procedures and regulations. The company should also be ensured that each vessel is manned with qualified seafarers, certified and medically fit, that meet national and international requirements and regulations. According to the ISM Code, every seaman has be well qualified for his position. The vessel's crew complement must meet flag requirements (safe manning certificate) and also the ILO and STCW requirements. The company should also establish procedures to check and review that each person is well qualified for his position and has already deep knowledge and understanding of the SMS rules, regulations, codes and guidelines. Training should be

take place periodically in order to achieve a well trained and qualified personnel according to the safety management system of the company and aiming to the safety and the protection of the environment.

Reports and analysis of non - conformities:

The aim according to the safety management system of the company which is mandatory for each managing or owning shipping company according to the ISM Code, the report of non- conformities and observations is to reduce and eliminate the number of incidents and accidents caused on board the vessel. The records of non- conformities handling should be kept, and each company should set up a system to notify appropriate personnel ashore and on board the vessel. The control of non – conformities is done via identification, the documentation, the evaluation of what caused the non – conformity, the corrective and preventive actions that should be followed in order to eliminate the cause ,the verification of effectiveness and finally the notification. The corrective action of a non – conformity begins with the detection of a non – conformity, incident, accident or any other hazardous situation. In order to correct any hazardous situation or incident we have to find the circumstances that lead to that hazardous event, deciding what are the most appropriate measures to resolve the situation. The corrective action should result in a documented system change to prevent reoccurrence of that situation caused. A corrective action taken, should be appropriate in order to impact that situation may have on safety or pollution prevention and commensurate with risks involved in each situation separately. In each corrective action should be defined the responsibility and the authority to set up and maintain a corrective action system, it should also have implement a change and allow the change to work for a predetermined period of time, the follow – up stage of a corrective action should be done in order to ensure the implementation and effectiveness of this action.

ISPS Code:

ISPS Code is the International Ship and port Facility Code which was adopted on December 2002 and it was done mandatory from 01 July 2004. This Code aims to special measures to enhance Maritime Safety and special measure to enhance Maritime Security as per chapter XI of SOLAS.Chapter XI of SOLAS, regulation XI-1/3 requires

a ship's identification number in a visible place in the ship's hull or superstructure. As per chapter XI-1 of SOLAS the measures that taken to enhance maritime security are according to regulation no.3, the ship's identification number. In the same chapter of SOLAS, regulation XI-1/5 it is mandatory for the vessels' to have a Continuous Synopsis Record (CSR) in order to be recorded the on-board history of the vessel. The chapter XI-2 is applied to the vessels which are engaged on international voyages, passenger vessels (including high speed craft, of 500 gross tonnage and upwards, offshore drilling units and port facilities serving such vessels on international voyages. The ship security alert system when activated, shall initiate and transmit a ship-to shore security alert to a competent authority designated by the Administration, which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the vessel in under threat or it has been compromised. The ship security alert system when it is active shall not send the security alert system to any other vessels, not raising any alarm in-board the vessel and continue the ship security alert until deactivates and/or reset.

Ship Security Alert Systems:

The implementation of that ship security alert systems aims to send a covert signal or message from the ship, it is agreed with Administration is a part of ship security plan and is individual. This means that each vessel has its own ship security plan and its own ship security alert systems. That systems may employ tracking equipment provided by traffic service providers, may utilize modifications to existing GMDSS equipment, may utilize the exchange of messages containing key words between the vessel and the Company. The equipment usually used in that ship security alert systems are cellular phones, GMDSS, VHF/MF/HF, satellite services which are depending on the areas that vessel sails. The ship security alert system requires two activation points one of which should be on the bridge of the vessel.

ISPS Code Part A:

This part of the Code is mandatory for all the vessels. Part A of ISPS Code, outlines detailed maritime and port security - related requirements. The contracting government can delegate certain responsibilities to RSO (Recognized Security Officer) with the exception of setting of applicable security level, reviewing and approving a PFSA, requirement of designation of a Port facility Officer, Reviewing and approving a PFSP

(Port Facility Security Plan), exercising control measures according to reg. XI-2/9 and establishing requirements of DoS (declaration of Security). It is required by the contracting government a DoS (declaration of security). A vessel can request a completion of declaration of security when a ship is at higher security level than port/ship, the agreement of Dos between contracting governments, a security threat/incident has taken place and when a vessel is conducting activities with another ship not required to have approved SSP (ship security plan).

Ship Security Assessment:

A ship security assessment includes a part of SSP (ship security plan). Ship security assessment can be done by recognized security organization. The ship security assessment shall include security survey on board the vessel including: the existing security and operations, the key security operations, the potential threats to shipboard operation and weakness including human factor / human error. The ship security assessment should be documented and retained by Company of the vessel. A ship security assessment is a mandatory and essential process to develop a ship security plan. The responsible person(s) for the development of ship security assessment is/are Company Security Officer(s) that ensure that ship security assessment is carried out for the vessels that the Company has under her responsibility. A ship security assessment should be carried out by persons with appropriate knowledge and background in this field. The ship security assessment should be documented, reviewed and retained by the Company. It should accompany the SSP (ship security plan) when put forward for approval. Upon completion of ship security assessment, it is prepared a report. In this report, that is written after the ship security assessment, included a summary if how the assessment was carried out, a description of each vulnerability found on the assessment and a description of counter measures that could be used to address each vulnerability. The report that conducted after the completion of the ship security assessment should be protected from unauthorized access or disclosure. According to the ISPS Code it is not compulsory to keep the ship security assessment with the ship security plan but it is highly recommended to do so for ease review, amendment and access in the event of security incidents. Contrary to the ship security plan (SSP), the ship security assessment is not classed as confidential or restricted.

On -Scene Security Survey:

The on-scene security survey constitutes an integral part of Security Assessment. In this way, during the on-scene security survey it is examined that ships security plans reflect ship specific aspects. During an on-scene survey is addressed mainly to security monitoring, contingency plans of the vessel, embarkation of persons and luggage, vessel's communications and cargo and ship's stores handling.

Ship Security Levels:

In order to prevent an incident or accident it is very important to identify the existing security measures, procedures and operations, for the protection of the dangers that may lead to a serious accident or incident. The identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security threats and the identification of weaknesses. The ship security level is a qualification of degree of risk that a security incident or threat will be take place. In security level 1: the appropriate protective security measures shall be exist at all times. In this security level exist the everyday security measures. In this level, the potential of a threat or an unlawful act against another vessel is not likely, only possible. In security level 2: there are additional appropriate protective security measures that exist for the period of time that the level of risk of happening an accident or incident is more heightened. In security level 3: further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent. In this security level, may not exist the possibility of identifying the specific target.

Developing ship security measures:

There are some main ways of developing ship security measures: Ship security assessments helps in identifying the security measures that will need to be included in the SSP (ship security plan). The second way that is used in the development of ship security measures is the SSP (ship security plan). The ship security plan includes the measures that are required to be implemented on board the vessel. In order to develop ship security measures it is required to develop detailed procedures which will be a part of ship security plan.

Ship Security Plan:

According to the ISPS Code Part A, each vessel must carry an approved SSP (ship security plan). A ship security plan is approved either by RSO (recognized security person) or by administration. But, the Recognized Security Person approving SSP cannot develop SSP (ship security plan) or SSA (ship security assessment). Ship security plan should be kept on board the vessel, and must be written in working language(s) of the ship. It should also exist a copy of Ship security plan in English, in French and in Spanish. The Ship Security plan is a guidance for the further development for ISPS Code Part B. A Ship Security plan, is specific for each vessel and it is based on ship security assessment and it is based on board. It is unique, every vessel has its own ship security plan, which must be approved by flag Administration or by RSO (recognized security person). A submission of SSP must be accompanied by the SSA (ship security assessment). The security arrangements, systems and the provisions that a vessel shall follow are identified in her Ship Security Plan. The Ship Security Plan of a vessel should be at least annually reviewed. In this review of the plan, is recorded the effectiveness of the plan, any audit findings, corrective action(s) and amendments to plan or security equipment. A copy of the review of the Ship Security Plan should be given to SSO (ship security Officer).

Safety Management System:

Each company should establish procedures in order to ensure that each vessel is well maintained and in accordance with rules and regulations of the ISM and the ISPS Code and any additional requirements established by the Company. According to these requirements the Company should ensure that inspections to the vessels are conducted to appropriate intervals, in order to ensure that all equipment of the vessel is well and that the vessels' are manned with qualified and well trained personnel. All non-conformities should be reported and corrective and preventive actions should be taken. Training of personnel on board should be by the Company, in order to increase the familiarization of the vessel's personnel with company's procedures and equipment used in each type of vessel. Each company according to hew own safety management system should ensure that valid documents are available not only on board the vessel but also in the managing/owning company and should also be ensured that these documents and certificates are reviewed periodically.

Records of the ISPS Code Part A:

According to the ISPS Code Part A records of the following activities should be kept: training, drills and exercises, security threats and incidents, communication relating to security, internal audits and review of security activities and security breaches. All the records of the Code should be maintained relative to the operation and maintenance of the security plan. The records should be kept in the working language(s) of the vessel and translation to English, French or Spanish. The records should be maintained on board for a minimum of five years.

ISPS and Drills:

Company Security Officer (CSO) shall advise the level of security to be followed. Company Security Officer (CSO) and Ship Security Officer (SSO) communicate with Port Facility Security Officer (PFSO). The Company Security Officer is responsible for the arrangement of Internal Audits and review of activities. A Company Security Officer may be assigned either one or more vessels. The Ship Security Officer is responsible to propose modification to Ship security plan and provided adequate training on board (drills). The Company Security Officer (CSO) and the Ship Security Officer should coordinate for the effectiveness of training and drills on board the vessel and of the shipboard personnel. The shipboard personnel have duties and responsibilities on board the vessel according to STCW requirements. Drills have to take place on board to the shipboard personnel at appropriate intervals in order to affect any danger on board.

Declaration of Security:

The declaration of security consists a documented agreement between the vessel and the Port Facility (PF) relating to specific security measures that each one will undertake. When a Declaration of Security is required, it is determined by the contracting governments. The Declaration of Security shall be completed by the Master or the Ship Security on behalf of the vessel and the Port Facility Security Officer or contracting government on behalf of the Port Facility. A copy of the Dos (declaration of security) shall be kept by the vessel and the port facility. The port facility security is applied to the ship/port interface, to the port facility security Officer (PFSO), to the port facility security assessment (PFSA) and port facility security plan (PFSP) and to the coordination with ship security Officer (SSO).

Port Facility Security Officer:

The completion of a Port facility assessment for each port facility within each territory that serves vessels engaged on international voyages has to be ensured by the Contracting government. The Port Facility Security Assessment consists a risk analysis of all aspects of a port facility operation. Security risk is seen as a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack. After the completion of the analysis, it is produced an overall assessment for the level of the risk. The Port Facility Security Assessment will help determine which port facilities are required to appoint a Port Facility Security Officer to prepare a Port Facility Security Plan. The Port Facility Security Plan must contain all the security measures that a Port Facility should take to ensure that it always operates at security level 1. The plan should also indicate the additional security measures that the port facility can operate at security level 2 and all the possible preparatory actions that the port facility can operate at security level 3.

Verification and Certification:

Through the method of audits, the contracting governments can review, approve, verify and certify the implementation of approved security plans. Recognized security person(s) may review, approve, verify and then certify the security plan on behalf of the contracting government.

International Ship Security Certificate (ISSC):

This security certificate it is issued on behalf of the flag, it is valid for five (5) years, with intermediate verification (between second and third anniversary). This certificate it may issued with the same validity with SMC in order to harmonize permit with ISM. In order to issue or renew a security certificate it should be followed the steps of: verification through a representative sample that the security system is being implemented effectively, verification that all equipment specified in the Ship Security Plan complies with the applicable requirements and the verification that all security equipment specified in the Ship Security Plan is operational and fitted for intended service. The interim verification of the security certificate is required from 01 July 2004. But, prior to Interim Certification it is required a ship security assessment to have been completed. A copy of Ship Security plan exists on board and can be submitted for

review and approval. During the Interim verification the Company Security Officer is responsible to arrange drills, exercises and internal audits to ensure the verification of the certificate every six months. On the other hand, during the interim certification not only the Master of the vessel but also the Ship Security Officer and the vessel's personnel have to do drills and training in order to be familiarized with their duties and their responsibilities relating to security. It has to be mentioned that the interim certificate is valid for six months.

ISPS Code Part B:

Contrary to Part A of the Code which is mandatory for all the vessels and for all the shipping companies, Part B of the ISPS Code acts as a guidance. Part B of the Code has a recommendatory character. Arrangements needed to achieve compliance with SOLAS XI-2 and part A of ISPS Code. Responsibilities of contracting governments are given to Part B of the Code. The contracting governments can designate authorities within contracting governments to undertake security duties and to provide certain information to International Maritime Organization. According to B/4.26 there are some alternative security arrangements: the flag administration is not party to the agreement, it covers any interface by vessels and the agreement is continually monitored, as needed and reviewed every five years. There are some security requirements, relating to ship security not covered SOLAS XI- 2 and/or ISPS Code, such as the automatic identification system, the ship identification number and the continuous synopsis record. According to security SOLAS 1974 Convention there are some amendments in order to enhance maritime security on board vessels and at ship or port areas. Between these amendments of SOLAS Convention 1974, it was created a new chapter in SOLAS to deal with maritime security, which in turn contains the compulsory requirement for vessels to comply with ISPS Code. According to chapter V of SOLAS, which is about safety of navigation, is referred to carriage requirements for shipboard navigational systems and equipment. The Chapter XI of SOLAS is referred to special measures to enhance maritime safety, one of which is ship's identification number. According to this measure each vessel has a unique number marking on a horizontal surface visible from the air (for passenger vessels), and in a visible place either on ship's hull or superstructure (for merchant vessels). This vessel's unique number should be marked and to the vessel's internally space. In the same chapter of SOLAS Convention 1974, it is referred and the Continuous Synopsis Record,

which is a documentary record of vessel's history to be available on board for verification purposes. The flag state is responsible for the issuance of Continuous Synopsis Record for all vessel's flying its flag. The continuous synopsis record shall contain at least the IMO number of the vessel, its name, and the name of flag state, the date that the vessel has been registered, the name and address of owner or bareboat charterer, the name and address of ship Management Company and the name of class society.

Key Players in ISPS Code:

The major players in the application of the ISPS Code and SOLAS Convention 1974, for the safety environment of vessels', their cargo, their crew or passengers and the environment avoiding an accident of collision or of a grounding that would had effects to all these factors and simultaneously it would pollute the environment. The flag administration shall review, approve, verify and certify, the recognized security persons act on behalf of the flag administration the last major player but not least are the contracting governments. The contracting governments which set the guidelines in order to improve the protection of the environment from threats. The companies from their own side, implement and maintain their ship security plan and provide support to Ship Security Officer, to the Company Security Officer and to the Master of the vessel. On the other hand, the vessels or the port facilities operate within the security level based on the Ship security plan or in the port facility security plan.

The Role of RSO:

RSO is an organization with expertise in security matters and with all background and knowledge of vessel and port operations. This organization is responsible to carry out an assessment, approval, verification and certification under part A of the ISPS Code. Each classification society has to meet the requirements of RSO. The approval is needed from various flags for classification societies in order to act as their RSO. The Recognized security organization may be authorized by the contracting governments to undertake security activities. The security activities that a RSO organization may rise could be the approval of a Ship Security plan, or amendments of ship security plans on behalf of the Administration. It could also be the verification and the certification of compliance of vessels with the requirements of chapter XI-2 and part A of the ISPS Code on behalf of the Administration and the Port Facility Assessments which are

required by the contracting government. A ship security assessment or a ship security plan or a port facility security plan can be done by an RSO organization. When the contracting governments give the authorization to an RSO organization to do a ship security assessment, or a port facility plan, the RSO should comply with the requirements as referred in the part A of the ISPS Code.

Port State Control Requirements and control of ships:

How the control in vessels takes place? In order to control and comply with measures and the requirements of the Code, duly authorized Officers go on board the vessels, and verify and review the certificates, in case of the vessels are already in port. In case that the vessels intend to enter into a port, the review and the verification of the requirements of the ISPS Code, become again by duly authorized Officers, which boarded on vessels before the vessels' entrance into the port. "Every ship to which this chapter applies is subject to control when in a port of another Contracting Government by Officers duly authorized by that Government, who may be the same as those carrying out the functions of regulation I/19". According to chapter XI-2 of the Code, every vessel is subjected to control of a port of another government by duly Officers authorized by that contracting government. This control is aiming to the verification that exists on board of each vessel entering into a port of another contracting government, a valid Interim International Ship Security Certificate (ISSC), according to the requirements of part A of the ISPS Code.

In case that the contracting government, to which a foreign vessel is entering into her port, has the reason to believe that the security of the vessel, or the port facilities it has served have been compromised, the vessel may be subject to additional control measures. If there are clear grounds, that the vessel entering into foreign territory not fully comply with the requirements of the Code, or there is no valid certificate on board the vessel, then the duly Officers assigned by the contracting government, shall impose control measures on the foreign vessels. The control measures that the duly Officers of a contracting government shall impose to a foreign vessel, entering to its port, and not fully comply with the guidelines and the requirements of the Code, may be the inspection of the vessel, the delay of the vessel in the port in order to accomplish the inspection, the detention of the vessel, the restrictions to operations (including the movement into the port), the expulsion of the vessel from the port. In case of vessel's

detention, due to non - fully compliance of the vessel of the requirements of the Code, non-compliance of either a defective item of a defective equipment, or faulty documentation (not valid certificate on board the vessel), then the contracting government, may allow the vessel to sail to another port, provided that any conditions agreed between the Port States and the Administration are met.

"A contracting government may require that ships intending to enter its ports provide information to Officers duly authorized by that government to ensure compliance with Chapter XI-2 prior to entry into port, with the aim of avoiding the need to impose control measures or to take steps as specified in Regulation XI-2/9". When a vessel is entering into a port, according to the requirements of the ISPS Code, is obliged to carry a valid certificate on board and the name of its issuing authority, the security level that vessel is operating, the security level at which the vessel has operation during the last ten port of calls. The vessel should also provide to the contracting government of the foreign port, any additional measures that the vessel took in any previous port where a ship to shore operation was taking place, proof that ship security procedures were applied during ship to ship activities and other further practical security information according to the part B of the ISPS Code. These extra practical security info may include: the crew list of the vessel, the passenger list of the vessel (in the case of passenger vessel), a general description of cargo carried by the vessel, the estimated time of arrival of the vessel in the port and the location of the vessel during the time that the report was done. According to Regulation XI-2/9 paragraph 1.3 of the Code, if it is required any additional control measures, then the duly Officer authorized by the contracting government shall immediately inform in writing the administration, specifying which additional control measures were imposed to the subject vessel, and the steps taken for the imposition of such additional control measures. "The contracting government which shall impose the additional control measures, to the vessel which is not fully comply with the requirements of the Code, shall also notify the recognized security organization that issued the certificate relating to the vessel concerned and the IMO when any such control measures have been imposed or steps taken". According to the Regulation XI-2/9 paragraphs 2.4 and 2.5 the denial of entry into a port, or the expulsion from a port, shall be imposed when the duly Officers authorized by the contracting government, have clear grounds that the vessel poses threat to the security or safety of persons, vessels or other property, and that there are no other appropriate

means or measures to remove the threat. In order to such measures to be imposed, the duly Officers of the contracting government has to have clear grounds that the vessel is not fully in compliance with the requirements of the ISPS Code, part A, or Chapter XI-2. The evidence that there are clear grounds that the vessel is not fully comply with the requirements referred in the Code, when a duly authorized Officer by the contracting government is verifying the vessels ship's security certificate, ISSC or its interim ISSC. These is possibility, that the vessel carry on board a valid certificate, but there are still clear grounds that the vessel is not in compliance, based on the personal judgment of the duly authorized Officer. In case that there are clear grounds that the vessel is not fully comply with the requirements of the ISPS Code, and that clear grounds are based on professional judgment(s) of duly authorized Officers, then the Officers shall proof the non compliance of the vessel to the requirements of the Code, via a report or a complaint based on evidence gather or observations, that the Master and/or the crew of vessel are not familiarized with ship security procedures and drills, according to part A of ISPS Code or Chapter XI-2.

Verification of the ISPS Code:

The initial verification of the ISPS Code is the complete verification of the ship security plan (SSP), and associated security equipment. The initial verification of the Code, aims to ensure that Ship Security Plan and the security equipment of the vessel, fully complies with requirements of part A of the ISPS Code and the Chapter XI-2 of SOLAS. The ISPS Code, should be renewed at intervals that not exceed the five years. The scope of the renewal verification of the Code, is the same as the initial verification of the Code. The intermediate verification of the Code, in order to verify that the vessel complies with all the safety requirements of the ISPS Code and the safety measures referred in SOLAS chapter XI-2, takes place usually between the second and the third anniversary date of the certificate. The scope of the intermediate verification is the same as it is in the initial/ renewal verification. The Administrations may require additional verification. After the completion of the initial verification, any change(s) to the ship security plan cannot be made without the sanction of the Administration. The International Ship Security Certificate (ISSC), may be issued after a successful completion of the initial or the renewal verification. The ship security certificate may be also issued by the Administration or by Recognized Security Organization. There is possibility, of another contracting government to request from the Administration to

issue, verify or endorse a ship security certificate. The copy of the ship security certificate and the verification report should be sent to the Administration as soon as possible. The ship security certificate is valid for five years. In case of a renewal verification will be conducted and completed within 3 months, and prior to anniversary date, then the new certificate will indicate the same date plus five years. When a renewal verification will be completed after the expiry date, then the new certificate will be valid from the date of existing certificate plus five years. When the renewal verification completed in more than 3 months prior to anniversary date, then the new date of the certificate will be from the date of completion plus five years. In case that a certificate is issued for a period less than five years, then the Administration, may extend to a period beyond the expiry date to the maximum period allowed providing it has completed an initial verification. If the renewal verification is completed and International Ship Security Certificate cannot be issued before the expiry date of the previous one, then the Administration or the Recognized Security Officer may endorse the existing certificate for a period that not exceeding the period of five months.

In case that the vessel is not in a port the period that its security certificate expires, the Administration may extend the validity for the purpose to complete its voyage to the port, to which it is to be verified not to exceed the period of three months. When the vessel is entering into the port, the extension is not something taken as granted and the vessel cannot leave the port, without having on board a new security certificate. A certificate will cease to be valid, when the verifications of the security certificate will not be completed within the periods specified, the certificate is not endorsed as required or in accordance with the requirements of the ISPS Code. Another possibility that a certificate is not still valid, is when the Company assumes the responsibility for the operation of a ship not previously operated by that Company, or during the transfer from ship to the flag of another state. When a vessel changes flag, the previous flag of the vessel is responsible to transfer all information of the vessel to her new flag. In case that the Company decides to transfer the operation of the vessel, to another Company, then the previous owning or managing Company of the vessel has to give all the information needed concerning the Ship Security Certificate to the new company of the vessel. The interim certification of the ISPS Code, started from the 1st of July 2004. The scope of the interim certification is for the delivery of as new-vessel or when a vessel re-entry into service, the transfer of a vessel from a previous flag to a new one,

the transfer from a state which is not a contracting government to a contracting government and when the Company assumes the responsibility for the operation of the vessel to another managing or owning Company. The interim certificate is valid for six months, and this period cannot be extended. In order to an interim verification be completed, it should be completed the ship security assessment, a valid copy of the ship security plan to be on board , the ship security alert system on board the vessel to be operational. The Company Security Officer is responsible for the organization of drills and trainings, exercises and internal audits. The Master of the vessel, the ship security Officer, and the crew members have to be familiarized with the procedures referred into the Ship Security Certificate. The Ship Security Officer meets the requirements as referred in the ISPS Code.

Health and Safety Management:

The purpose of this procedure is to: establish and promote a safe working environment on board managed vessels and ashore, to establish safeguards against identified risks, to prepare and exercise for emergency situations, to provide the ship's personnel with the necessary information on the Company's Management System in a working language understood by them and to continuously improve the Company's health, safety and environmental protection system

This procedure applies to all vessels managed by the Company, and to all shore based employees who manage, perform or verify work relating to and/or affecting health, safety and Environment. The Company is committed to provide all managed vessels with the necessary Information regarding Company's Management System and other rules, regulations, instructions and guidelines related to the implementation of a healthy & safe environment on board. Such references shall be available to all officers and crew in a language, or languages understood by them. The Master is responsible to ensure that seafarers on board have an adequate understanding of the rules, regulations, codes and other information related to their (seafarer's) rank and subsequent duties. Furthermore the Master and Chief Engineer are responsible to ensure that health, safety and environmental protection requirements, as defined in the major conventions (SOLAS, MARPOL, etc.) and the Management system are communicated to the ship's officers and crew and satisfied.

Such communication and discussion of important health, safety and environmental

Protection issues take place during any suitable circumstances (such as Safety & Environmental Meetings, Safety drills etc.) And shall also be left in writing, when and if deemed necessary. Furthermore, all newly joining seafarers shall be familiarized to critical health and safety (refer to Marine Personnel procedure CP03).

The Company in order to provide a link between the Company and those on board, has designated the designated person ashore as the person responsible for monitoring the Health, Safety and Pollution Prevention aspects of the operation of the managed ships. The DPA shall review, sign and reply to all "Safety & Environmental Committee meeting minutes" with comments and communicate with Shipmasters and senior Company personnel as necessary to maintain required levels of health and safety management. Furthermore, the Company's Management shall meet at prescribed periods in order to review its Management System.

During that meeting the Company's Health Safety & Environmental Protection Policy & Procedure shall also be evaluated in order to ensure its suitability & effectiveness. Furthermore the SQE Manager shall trigger safety & environmental meetings in the office at any other intervals he might consider necessary.

The Master, to satisfy the need of review of Company's Management System (see Policy Manual), reviews the system together with the Officers or Crew concerned and presents his review (at least once before his signing-off), with or without findings, to the Company. The Company (DPA) after evaluating the Master's Review, shall forward his remarks to the vessel. The Master shall chair a Safety & Environmental Committee Meeting (SECM) at least every month. The meeting is attended by the Master together with all officers and crew except those in watch or in rest. Safety & Environmental Meeting Agenda shall be posted in mess rooms, 4 days prior to the meeting so that all crew can have access to the subjects to be discussed. During the meeting important topics related to the health and safety and environmental management on board the vessel are discussed. The SECM always include in the Agenda the following: a) the Inspection of safety and environmental equipment and appliances b) Analysis of accidents and near misses, if any, unsafe acts and unsafe practices since last SECM.

Furthermore, in order to assess and review the effectiveness of health, safety and environmental policy, working systems and activities on board, the following are periodically reviewed and can form part of the agenda: the health, safety and environmental protection requirements and training, the performance during safety

drills and suggested improvements, the condition of health and safety equipment, the safety of working practices and conditions on board, the cargo operations (especially if dangerous cargo on board), the port state control requirements of next port, the suggestions for improvements and action decided.

The minutes of the Safety & Environmental Committee Meeting are signed by the Master and all attendees and kept in file. One copy of the minutes is posted on the vessels' notice board and another copy is forwarded to the SQE Dept. The DPA shall view and initial the meetings minutes, noting any aspects that need further attention and provides to the vessel his comments/responses in writing. The SQE Manager is responsible to communicate with

Masters and Chief Engineers and with other shore based Managers in order to ensure that required levels of health and safety are maintained on board managed vessels.

Emergency Preparedness:

The Company's Management System includes procedures necessary to ensure that the Company is prepared at all times to respond effectively and efficiently to hazardous situations, accidents or emergencies involving its managed ships and or the environment. The Management (Shore based) Emergency Response Plan is a stand-alone manual, and appropriate parts of it are reproduced in the Shipboard Emergency Manual.

The Shipboard Emergency Manual provides instructions and guidance from the Company to the Masters on how best they may deal with certain incidents, such as: The Shipboard Oil Pollution Emergency Plan (SOPEP) for each managed vessel is in accordance with the requirements of MARPOL 73/78 Annex I / Regulation 37.

The Vessels' Response Plan (VRP) for each managed vessel, eligible to trade in U.S.A. is in accordance with the Oil Pollution Act (OPA 90) of USA, as revised.

The SOPEP and VRP of each vessel cover the emergencies, which involve pollution or substantial threat of pollution, i.e. operational oil spills and non-operational oil spills (resulting from casualties). The Ship's Security Plan of each vessel covers the security emergencies that may arise. Specific scenario-based contingency plans and standard operating procedures are developed to address identified threats. The Company has issued instructions for the Masters in the Navigation Manual (NAM) to carry out emergency drills at least as frequent, as specified by the respective Flag Administration

of the vessel. The purpose of emergency drills is to develop and maintain a well-trained, confident and efficient shipboard team to deal with emergencies.

At least one drill per year, per vessel, will include the participation of the Company for verifying the efficiency of ship-to-shore communications. The Company has identified and has provided guidance to the Masters on such emergency drills, which deal with the emergencies.

All emergency drills are recorded in the vessel's log and on appropriate Company's Forms, which are checked by shore personnel during internal audits. The Company is advised in writing every month on the drills conducted and whether their performance was satisfactory. At the beginning of each year, a summary report is prepared by the Master and is submitted to the Company for all the drills conducted during the previous year. All monthly and yearly reports are reviewed by the DPA in charge. The Master has ultimate responsibility for deciding the frequency of drills and this will depend upon his assessment of the effectiveness, confidence, and motivation of his crew. However, the number of drills cannot be less than those set by the Company. Security drills / exercises are conducted at least once every three months to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and to identify security related deficiencies, if any, which need to be addressed. Various types of exercises, which may include participation of the CSO, Port Facility Security Officers, relevant authorities of contracting governments, as well as SSOs, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises.

The Management Emergency Response Plan is exercised at least once per year by simulation, as per exercise scenario prepared by the SQE Manager in liaison with the DPAs. Records and findings of such drills, as well as their effectiveness, are discussed among the Managing Director., Operations Manager, SQE Manager and the DPAs, and any raised non-conformities are corrected. The managed vessels are informed on the Company's exercise and the lessons to be learnt, if any.

Critical Operations:

Shipboard controlled operations concerning safety and the prevention of pollution have been identified and defined in the Instructions Manuals as Critical Operations and their performance has been assigned to qualified personnel. The Company, where appropriate, has implemented the use of checklists to ensure that critical shipboard

operations are covered and performed in a controlled manner. The following operations are considered ‘critical’, and relevant instructions are provided in the corresponding Company manual.

Critical Equipment:

The Company has identified equipment and technical systems, the sudden operational failure of which may result in hazardous situations. Such equipment and systems are clearly identified and defined as Safety Critical Equipment by creating comprehensive lists of all vessel systems and equipment and:

- a) Identify failure modes (i.e. loss of function, structural failure, leak, rupture)
- b) Identify the end effect of the failure, with respect to each applicable functional failure consequence category, from the following: propulsion, directional control, explosion/fire, loss of containment, safety
- c) Carry out risk characterization of the identified failure and effect, using Risk Matrix.

If risk ranking is “High” the equipment is defined as CRITICAL. As critical equipment are considered the following:

- a) Main and Generator Engine’s alarms, shut down and slow down protective devices,
- b) Emergency generator,
- c) Steering Gear and control systems and alarms,
- d) Gyro Compasses,
- e) ECDIS, Radars, ARPA and Echo sounder,
- f) GMDSS equipment,
- g) Main and emergency fire pumps,
- h) Cargo pump protection systems, alarms and emergency shutdown systems (for tankers only),
- i) Bow loading equipment emergency shutdown system (for tankers only),
- j) Crankcase mist detectors,
- k) Fire detection systems and fire alarms,
- l) Fixed fire extinguishing systems,
- m) ODME (for tankers only),
- n) OWS and monitor,
- o) Pump room fixed gas detection systems and alarms (for tankers only),
- p) Inert gas systems and alarms (for tankers only),
- q) Lifeboat and life raft systems,
- r) Engineers alarm,
- s) De-watering system (for bulk carriers only),
- t) Cargo tank overfill alarm (for tankers only),
- u) Water ingress system (for bulk carriers only).

The company has also identified equipment and technical system whose sudden operational failure may result in loss of hire or disturbance of commercial obligations towards its customers (charterers, receivers). Such systems are: the Cargo Loading and Discharging equipment and systems for dry cargo ships and the Cargo Discharging equipment and systems for oil tankers

Although the above equipment and systems do not impair safety, they are treated as business critical. Therefore, they are thoroughly maintained and a safety stock of spare parts is always kept onboard.

Specific measures are provided at promoting the reliability of all these equipment and systems considered as critical by appropriate monitoring, checking, testing and preventive maintenance. Relevant procedures and instructions are provided in the Company's Planned Maintenance System (PMS). No critical systems, alarms, control or shut down may be by-passed, inhibited or taken out of service without the authority of the Company. Only those personnel authorized by the Ch. Engineer are to work on any such critical systems. The Company must approve any changes to critical alarms, control or shut down set points and risk assessment shall be conducted by ship and Company before any changes are effected.

The Ch. Engineer is responsible for communicating any deactivation of critical alarm or system to the duty personnel. Risk assessment shall be conducted and forwarded to the office for approval prior any shut down of critical equipment for routine planned maintenance. Any operational failure in critical equipment or any significant safety deficiency should be immediately reported to the Company. Both Company and ship's Master shall make a full assessment of the situation before the affected operation is resumed.

For operational failure following procedures should be followed: The Officers on duty are aware of critical equipment, the Master and Chief Engineer to be notified by the officer on duty immediately. It is very important to try to rectify the problem in a reasonable time depending on the circumstances. The Master and the Chief Engineer will assess the situation and will estimate the time required for rectification. If it is not possible to rectify the problem, they will proceed with temporary measures to reduce risk. In case that the problem was not rectified, inform the office (all involved departments) by phone or email. In case immediate assistance from office is necessary then the office must be notified by phone. Moreover, in cooperation with office, agree on action plan to rectify the problem. If a deficiency was not permanently rectified, the Master and the Chief Engineer will submit Risk Assessment which will be reviewed by the departments involved and will conclude if control measures are adequate in order to resume operation. In case deficiency was not rectified, the company shall notify all the involved parties (flag state, classification society, port authorities, charterers, oil majors,

P&I club and/or other), as applicable. They will agree with the office schedule for closing out the deficiency, and finally they will inform the office when normal operation is resumed.

A safety stock of spare parts for critical equipment and systems are identified and maintained onboard. These spare parts are associated with the maintenance and repair of critical equipment and they may be used either proactively during planned maintenance of critical equipment or reactively during unplanned maintenance to repair damaged critical equipment.

Except spare parts, special and ordinary tools, lubricant oils, materials and consumables needed to execute the maintenance and repair, such as pipes, steel plates, bolts and nuts, clamps, welding consumables, gaskets must be maintained onboard. The critical spare parts and their quantity are identified based on equipment manufacturer advice, industry experience and company's fleet experience. The quantity should cover the requirements in case of unplanned maintenance and repair of critical equipment so that to avoid some periods when those spares are not carried out onboard. The safety stock of spare parts for critical equipment is incorporated in the computerized planned maintenance inventory system and maintained onboard at all times. The Company has adopted, implements and maintains "safe working practices" to minimize injuries/accidents. These cover areas such as: protective clothing (shoes, gloves, overalls, goggles, hard hats, etc.) the use of machinery and equipment (precautions during maintenance, training, etc.), the work permit system (entry into enclosed spaces, hot work) and to provide safety posters

The Health & Safety Manual describes the use of the Company's permit to work system. Permit to work will be used where an operation involves a particular hazard and step by step actions are considered necessary to ensure the safety of the personnel on board. Such permits include permit to entry in dangerous spaces and hot work permit. Management ensures that adequate resources are available to care for the welfare of the ships' crew, whether they are employed directly or through a manning agency. Well-being covers diverse aspects of the crew's quality of life including factors such as quality of food, accommodation, rest and recreation facilities, hygiene, air conditioning, access to ship and shore medical facilities. The Company actively promotes high standards of housekeeping and hygiene, particularly in food storage and preparation. Additional information regarding health is provided in the Health & Safety Manual. Health and safety of all Company employees is also promoted in the office. All health and safety aspects and impacts have been identified and risk assessment carried out to assess and minimize the risks, if any. To maintain a safe working environment, minimize negative health effects and promote personnel safety, monthly safety checks

are carried out by the office safety officer. According to OHSAS 18001 requirements, the Company has set health and safety objectives and targets as referred in Appendix II of this procedure. Appendix II should be placed onboard (in Master's cabin and both mess rooms) as a guidance regarding subject.

Training and Familiarization:

The Company has issued instructions in the Health & Safety Manual for the shipboard training Program which includes the following: They are given by senior officers and cover health, safety and environmental protection matters. Such training sessions are conducted at least monthly and subjects are selected by the Master or Chief Engineer according to the identified training needs of the crew. The Video Training which are available on managed vessels are shown to the shipboard personnel, with subsequent training on the same topic by the appropriate senior officer. Another way of training, is the Training by Company's Superintendents

Company's Superintendents who stay onboard during a short voyage may conduct safety training lectures and emergency drills to fit with the vessels operational commitments. In addition, personal supervision and training may be given to selected staff where necessary. There are also hired consultants executive for the Training. In addition to the previously mentioned training, the Company, if necessary, provides additional training onboard and audits on safety/navigational matters by external consultants.

All tankers are supplied with Interactive Computer Based Training (CBT) modules, which are used individually by all officers and cadets to complete the relevant with their job CBT courses (see Appendix III - On board Training Program). Training of Deck and Engine Cadets is a systematic training program is available to ensure that the cadets will be ready to assume junior officer's responsibilities upon completion of their practical training and experience at sea (sea service). This program is described in Health & Safety Manual. The training of junior officers and pump men is conducted via a training program for junior officers to ensure that junior officers and pump men are familiar with the vessel's cargo operations.

For the ashore training, the training courses (over and above STCW requirements) are organized by the Marine Personnel Department in cooperation with the SQE, at various training centers ashore, for all Masters and Officers.

Familiarization of new personnel:

The Company has issued instructions in HSM for the Master to ensure that each new crew member is fully familiar with the vessel and his duties before taking over. The familiarization process includes also procedures for passengers and supernumeraries to be familiarized with the basic health, safety and environmental equipment/procedures. The familiarization procedure is composed of: the initial training with safety equipment and procedures onboard, the proper hand over either from the relieved person or from another responsible officer to ensure that the new crew member is fully familiar with the equipment of the vessel relevant to his job. The relieved officers have to provide brief hand-over notes in writing to their reliever for important issues. The general ship familiarization training which ensures that all personnel have familiarized themselves fully with the vessel's equipment, arrangements and emergency procedures. The extensive familiarization of Master and Chief Engineer prior taking over the command.

Management leadership and commitment:

The Company's top management is dynamically involved to all the issues related to the Company's functions. Through constant and active participation to the Company's every day activities, they demonstrate leadership and commitment to the development and proper implementation of the Company's Management System. Top management's commitment is also effected / passed to the Company's personnel by communicating to them the importance of meeting customers, as well as, statutory and regulatory requirements, by ensuring that appropriate quality, safety and environmental protection policies and objectives are established, by conducting management meetings for reviewing the System's effectiveness, and by ensuring availability of required resources.

The top management shall ensure the integration of the quality management system requirement into the organization's business procedures and shall promote the use of the process approach and risk-based thinking. The Managing Director (MD) is ultimately responsible for the effectiveness of the Company's Management System & Organization and for ensuring that those within it are supported to contribute to the effectiveness of the quality management system. Where individuals hold specified responsibilities, the MD authorizes those individuals to take such actions to ensure fulfillment of those responsibilities promoting improvement.

The Fleet Safety & Security Officers (one for Tankers, one for Dry Cargo Vessels and one for Containers) are the Designated Persons Ashore (DPAs), responsible to the Managing Director for the implementation, monitoring and control of the Management System onboard the managed vessels. They report any deficiencies or improvement directly to the highest level of Management, control and maintain any changes necessary thereby, and provide the vital link between the Company and those onboard the managed vessels. In the absence of the

DPAs their duties are performed by the appointed alternate DPAs. The Master of the vessel is the ultimate authority on matters affecting the health and safety of the crew, the ship and its cargo, own and third party property and the protection of the environment. The Master is responsible for: the implementation of the Health, Safety, Environmental and Energy Efficiency, the Management policy and all other policies issued by the Company. He is also responsible to motivate his crew in the observation of those policies, and to issue appropriate orders and instructions in a clear and simple manner. The Master of the vessel also verifies that specific requirements of the Company's Management System are observed. Moreover, he conducts the reviewing of the Management System and reporting in writing its deficiency to the shore based management through the responsible DPA.

The Superintendent Engineers and Marine Superintendents are responsible for the maintenance of the safety, quality and environmental standards in the vessels under their Supervision as per Company's Management System. The Marine Personnel Manager, in liaison with DPAs/Superintendents/ Operators in Charge and the Manning Agents involved, is responsible for: ensuring the managed vessels are manned with qualified, medically fit and suitably experienced seafarers in accordance with the relevant national and international manning requirements. Marine Personnel Manager, also keeps appropriate records of qualifications, medical fitness and training and he is allowing to Senior Officers reasonable handover periods of time to ensure their appropriate familiarization with the vessel. He also ensures that shipboard personnel is able to communicate effectively in the execution of their duties in the official working language on board which is the

English language and that the new recruits are all made aware of the Company's Management System.

Internal Auditor:

The internal auditor is responsible to report to the Managing Director. He is an independent person of the areas to be audited, who has the following duties/responsibilities: He or She is conducting scheduled, random or following up office internal audits, as instructed by the managing director and/or the Management Representative. He also reviews the relevant audit checklists and Company's procedures to familiarize himself/herself with procedures of the areas to be audited. An Internal Auditor is also responsible to conduct the audits assigned to him/her to ensure that the relevant Company's procedures are duly followed and to verify implementation of corrective actions to previously issued Non-Conformities and observations. Finally he also prepares and submits the audit checklists and/or summary reports, duly completed, to the MD and the Company's responsible personnel.

Sqe Representative:

Reports to the SQE Manager and has the following duties/responsibilities:

He/ she is planning and organizing external class (ISM/ISPS/MLC and ISO) audits for the vessels and relevant certification for the company, he/she is planning, organizing and performing internal audits for the Company's departments (office). He/ she is also coordinating the management review and TMSA audits by external parties and reviewing and analyzing Company's audit reports/Non-Conformities, as submitted by the external and internal auditors, proposing appropriate corrective actions, and ensuring their implementation and effectiveness, in cooperation with responsible manager(s). The SQE Representative is also responsible for the issuance, revision and update of all Company's Management system documentation in liaison with responsible managers. This person is authorizing the issuance, revision and update of Company's Policy and Procedures and Manuals.

Moreover, he collects information from the IMO, classification societies, USCG, flag states,

INTERTANKO, INTERCARGO, MOUs and other sources of information, preparing and

Updating file(s) with Rules and Regulations (international, national, flag state) and industry guidelines that may affect the Company, in cooperation with SQE Manager,

DPA's and responsible managers. He also prepares Management Review Meetings agenda and following up, in cooperation with SQE Manager, the findings of the Management Review Meetings. He also is responsible that the familiarization of SQE new personnel is carried out as appropriate, and ensures that the training of SQE new personnel is carried out according to plan and their personal training needs. The SQE Representative, is keeping the records of the company KPIs as these are set and reviewed during the Management review meetings. He is also processing requests of Change proposed by SQE Manager, DPA and Marine Superintendents as well as those proposed by other departments until they are incorporated in Company's Management System. One more responsibility of the SQE Representative is reviewing Masters' Reviews in order to identify any constructive proposals for the improvement of the Company Management System. In such cases, the identified proposals will be discussed with SQE Manager and/or DPA and/or managers of the other departments as appropriate for the purpose of agreeing if the proposed improvements will be adopted. He is also issuing the quarterly and annual safety, quality and environmental statistics on the basis of the data collected in SQE department, identifying gaps and weaknesses and proposing corrective actions (procedures, training, KPIs etc.). In liaison with the training officer, reviewing the progress of training of SQE personnel and proposing improvements and upgrading of existing training plan. On the basis of the information provided by DPA from the results of Management Review carried out by majors at other shipping companies (recommendations and observations), performing gap analysis and proposing improvements as appropriate. SQE Representative is also responsible to check the invoices issued by the classification societies related to the ISM, ISPS, MLC and ISO certification of the vessels and the company. In cooperation with Training Officer, the SQE Representative is organizing courses by external trainers for the in-house seminars in head-office, negotiating prices and checking relevant invoices. Finally he is organizing the in-house seminars for shore personnel or make arrangements for attendance at a training center, negotiating prices and checking relevant invoices.

Vessel Risk Assessment:

The purpose of this procedure is to define when Hazard identification & Risk Assessment is to be conducted on board, the process to be followed and the control actions to be taken. This procedure applies to the process of Hazard Identification and Risk Assessment to be followed on board. The Company implements a fleet wide Risk Assessment process for the operations undertaken. Such Risk Assessment shall be utilized on board to ensure that shipboard operations are risk controlled and any residual risk involved is within acceptable limits (risk level medium or lower).

The Master in coordination with Chief Engineer, Chief Officer and/or other ship officers is responsible to ensure that risk assessment is used for identifying and managing hazards on board and that adequate risk control measures are implemented on board.

Identification of hazards and level of risk is to be assessed prior to undertaking the relevant operation / activity and should be integral part of the work planning process on board. Any shipboard operation/activity involving risk at a level above 'Medium Risk' is to be immediately addressed as follows: Any action and risk control measures are to be agreed and implemented prior to initiating the operation / activity. Such action and measures are to adequately mitigate and control the risk within acceptable levels. Risk Assessment form is to be used for documenting the agreed control actions. If the operation / activity is already under progress, the control measures are to be implemented as soon as possible. In this case the office is to be immediately notified.

Risk Assessment form is to be used for documenting the agreed control actions. If the resources available and/or circumstances are such that the risk cannot be lowered to an acceptable level, the operation must be discontinued and the office is to be immediately notified and further advice is to be provided. The Risk Assessments undertaken on board for critical operations are to be submitted to the office for approval prior commencement of the intended work, except in cases of emergency. Risk assessments for routine operations are filed onboard and are subject to review during internal and external audits. When a risk assessment is to be carried out on board. The Company's Management System has been developed taking into consideration all the risks identified in the initial Risk Assessment process conducted on all routine operations of the Company. However in order to further identify potential hazards and manage operational risks fleet-wide the Company has an active shipboard program, requiring a risk assessment to be conducted on board on a number of cases as shown here below.

Hazards associated with non-routine repairs (following critical equipment breakdown or arising from the potential for breakdown) are identified (C/O + MASTER + C/E)

Routine planned or unplanned maintenance of critical equipment or immobilization of main engine is to take place. The Risk Assessment shall be submitted to the office requesting approval prior shutting down of the equipment. The assessment must include: the alternate back-up equipment/systems, the necessary modification in operational procedures as a result, the additional safety procedures (emergency) (C/O + MASTER + C/E). A planned temporary or permanent change to procedure or equipment is to be implemented on board.

The operation will be carried out under exceptional circumstances, which may include hazards not identified in the FSA or unsafe conditions/acts are identified which related to the operation. For hot works, risk assessment shall be conducted and submitted to the office together with the hot work permit. The assessment must include the following: the alternate back-up equipment/systems, the necessary modification in operational procedures as a result of the additional safety procedures (emergency).

A ship is added to the fleet. The initial Risk Assessment is to ensure that all anticipated mooring arrangements and equipment ensure the safety of shipboard personnel. Any changes to mooring arrangements and equipment shall necessitate a new Risk Assessment. In case of changes in the conditions of an already made Risk Assessment. The person (or team) undertaking the Risk Assessment shall analyze the operational characteristics of the process / activity to be undertaken and shall identify any hazards associated with the process to be undertaken. Particular attention is to be given to unsafe practices that could be followed (due to lack of experience, lack of training, lack of time, lack of resources, crew fatigue, new operation / activity / equipment / procedure) and/or any unsafe conditions that may prevail during the operation / activity (such as extreme weather conditions, explosive atmosphere, lack of maintenance, breakdown of equipment etc.)

For any hazards identified, the related level of risk is to be evaluated by assigning the corresponding LIKELIHOOD and SEVERITY and by filling the relevant boxes indicating

“HAZARDS IDENTIFIED” in Risk Assessment form. For any hazards identified with a risk level above ‘High Risk’, risk control action must be taken in order to mitigate the risk. Any action to be taken should be sufficient to lower the related risk to at least within ‘Medium Risk’. Any action decided and the period for which it will remain

effective is to be recorded in Risk Assessment form by completing the section “DESCRIPTION OF CONTROL MEASURES”. In order to ensure that the agreed action is effective in reducing the related level of risk the section indicating “FURTHER ACTION TO CONTROL RISK”. For each hazard and its associated potential accident identified in the previous step, the likelihood of that hazard leading to an accident are rated. It will be decided how frequently each of the hazards and undesirable events listed in the previous step could become reality and cause harm. For each hazard and its associated potential accident identified in the previous step, the severity of that hazard leading to an accident will be rated. The risk is evaluated without any control measures in place.

Likelihood x Severity = Risk factor or Risk rating. The output from this step is the identification of the hazards which have to be addressed to reduce the risk.

The General Risk Assessment Matrix framework for risk criteria divides risk into 3 regions:

Intolerable (High Risk) - risks regarded as intolerable except in extraordinary circumstances (such as wartime), whatever their benefits. Activities causing such risks would be prohibited, or would have to reduce the risks whatever the cost.

Tolerable (Medium Risk) - risks that are tolerated in order to secure benefits. In this region, risks are kept as low as reasonably practicable (ALARP), by adopting risk reduction measures unless their burden (in terms of cost, effort or time) is grossly disproportionate to the reduction in risk that they achieve.

Broadly acceptable (Low Risk) - risks that most people regard as insignificant, negligible.

Office Risk Assessment:

The purpose of this procedure is to define when Hazard identification & Risk Assessment is to be conducted, the process to be followed and the control actions to be taken. This procedure applies to the process of Hazard Identification and Risk Assessment to be followed in the office. The SQE Manager of a company, is responsible to ensure that the Company implements a fleet wide Risk Assessment process for the operations undertaken. Such Risk Assessment shall include

health and hygiene and shall be utilized for reviewing, amending and improving Company's procedures, processes and practices so that the risk involved in Company operations is at the level of Medium Risk and lower. The Company shall maintain a Risk Assessment database, providing the details of Risk Assessment sessions together with the follow up action. Records of risk assessments and follow up meetings shall be reviewed by an appropriate Company's representative. The Risk Assessment database shall be also available on board and reviewed at least on a yearly basis or at any shorter intervals that may be considered necessary.

References:

1. ISM Code , a practical guide to the legal and insurance implications, Dr. Phil Anderson, second edition, Taylor & Francis, 2015
2. The International Ship and Port Facility Code (ISPS) and SOLAS Amendments, IMO, 2003
3. "An empirical assessment of ISM Code effectiveness on performance: the role of ISO certification", Angelos Pantouvakis & Maria Karakasnaki
4. "The impact of ISO 9001 effectiveness on the performance service companies", Evangelos L. Psomas, Angelos Pantouvakis, Dimitrios P. Kafetzopoulos
5. "ISM Code implementation: an investigation of safety issues in the shipping industry", Angelos Pantouvakis, Periklis Vlachopoulos, Nancy Bouranta
6. "The impact of internal service quality and learning organization on clinical leaders' job satisfaction in hospital care services", Angelos Pantouvakis, Panagiotis Mpogiatzidis