Information Systems Security in Shipping, according to ISO 27001

Stergios OIKONOMOU
Dept. of Biochemistry and Biotechnology (DBB)
University of Thessaly (UTH)
Volos, Greece
stergios.oikonomou@gmail.com

Alexandros VOLIOTIS
Dept. of Biochemistry and Biotechnology (DBB)
University of Thessaly (UTH)
Larissa, Greece
abwasp2000@yahoo.gr

***Abstract*—Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of the utmost importance for the success of the organization. The maritime industry is no different than any other organization. This document introduces the information security role in shipping companies as well as the analysis for the standard ISO 27001.2013 and its implementation to them.**

Keywords—Information Systems, Shipping, Security, ISO 27001.2013.

I. SHIPPING

A. Concept of Shipping

Maritime is defined as "all the methods, processes, and actions that are applied in such a way that a vessel can travel from one part of the earth to another safely and as soon as possible" (Theotokas, 2011).

Shipping is defined as "all of the systemic actions of any kind, which are intended to provide services and which are related to maritime transport, satisfying human needs, for some benefit".

B. Shipping Company

1) Shipping company structure

The pattern of past management that relied heavily on experience and tradition tends to be eliminated. Modern ways of organizing, administering and operating are naturally adopted with the necessary adjustments to meet the specificities of the industry.
A typical management structure of a shipping company consists of the following departments:

THE LEGAL DEPARTMENT

Covers a large field. Among the main functions can be mentioned Board matters, contracts for new buildings, company law, national/international taxes, and purchase/sale of ships. The company lawyer is also often on the Managing Director's staff, and/or secretary to the Board of Directors. Frequently, this department will often also handle marine and other insurance matters that may arise of a legal nature.

THE ADMINISTRATIVE DEPARTMENT

Is responsible for the main organization, for personnel, internal services and internal control. Within all these fields a new development has taken place during the last few years. The importance of a sensible employment policy combined with systematic training has been given increased emphasis. Internal control covers the traditional auditing as well as the more detailed control work required to ensure that the organization works according to the policies laid down and within the working instructions given.

THE FINANCE AND ACCOUNTING DEPARTMENTS

Cover budgets, accounting, EDP and finance. Regular reports are prepared for each operational department, each ship and for the company as a whole. The management needs to keep the Accounting Department up to date with operational proceedings at all times, with changes and corrections when necessary. Computers have been used for a long time in modern shipping companies and for different purposes. Computers are indispensable as an advanced technical aid in the office, also for complicated techno/ economic calculations and for budgeting in the operational and liquidity area. During the last few years long range planning has also been taken up as a subject of business administration. The reporting of the economic results should follow the organization chart and will, if correctly done, be of prime importance to the management, for the organization's mode of operations and for the control of the results. Financial questions will always be vital to any shipping company. To arrange finance when building new vessels and to find the highest interest for liquid working capital are main activities together with follow-up of

the unstable currency markets and protection against currency losses.

THE TECHNICAL AND MARINE DEPARTMENTS

Take care of fleet management, including ship operations, manning, storing, repair and maintenance and dockings. The departments are also usually responsible for building of new ships, often organized in a new-building section. Project development with optimization studies and operational analysis is done in cooperation with other departments, mainly the shipping departments. For Project developments EDP is increasingly becoming a useful tool.

THE MARINE INSURANCE AND CLAIMS DEPARTMENT

Handles ship insurance, statistics of damage and makes preparations for adjustments of claims. All claims relating to damage of the cargo are handled in this department. These claim adjustments cause considerable work, particularly within the liner trade.

THE LINER DEPARTMENT.

From an organizational point of view it is of interest to observe that the liner trade seldom operates under the supervision of one company alone. There are many different types of cooperation. In some cases the owners put their ships at the disposal of a separate joint venture company which manages the operations. In other cases they may participate as partners in a co-sailing agreement, possibly also with a pool agreement. Usually this takes place within the framework of a liner conference, where all the shipping companies serving the trade in question participate. No matter how the cooperation is arranged, it includes marketing and booking of cargo, allocation of space, responsibility for routing, documents, port facilities, loading/discharging, control of port expenses, stevedore contracts, etc.

TANKER AND DRY CARGO DEPARTMENT

Arrange employment for the vessels and are also responsible for their operation. These departments are frequently referred to as Chartering Departments. The tanker department will usually handle bunker contracts for the company fleet. In the organization chart the interaction between the main department and the sub departments is shown by the lines of authority. This authority goes down from the ship-owners, through the main departments and down into the organization. The lines show how the instructions for the company are transmitted from the ship-owners through the different links. All department heads are fully responsible for their own activities and they must therefore be fully familiar with all matters concerning their departments so as to be capable of managing and making decisions. Information, messages, tasks, proposals, etc. follow the formal lines of communication. This is the main principle, but modifications occur.

THE ICT DEPARTMENTS

Develops, manages and maintains a shipping company's technology-related assets (hardware, software, systems, etc.), policies, procedures and systems. This includes, but is not limited to, the administration of company email systems, business intelligence and enterprise resource planning [ERP] platforms, network setup, data backup and retrieval and document storage. The group also provides employees with day-to-day technology support to ensure that technology-related problems do not interfere with their work.

OTHER DEPARTMENTS.

Department for other activities reflects the fact that many shipping companies have assumed other shipping related activities within their organization, such as agencies activities, forwarding, travel agency, and in recent years, offshore activities. Shipping companies will frequently build their organization around key personnel and the dividing lines between the departments might therefore be very different from those mentioned above. Shipping companies should also be aiming at flexibility in their organizational development, as changing conditions in the world market might make it necessary to reorganize or set up new departments to cater for new trades or ventures.

2) Operating enviroment

Shipping by its nature is a very competitive and a very complex industry. Shipping companies have to operate on a global scale and manage offices all around the world and work with a diverse work force.

Maritime transportation is one of the most global industries so that, in order to operate efficiently and effectively, its regulations and standards are must be generated and implemented on an international basis. International Maritime Organization (IMO), which is authorized agency that responsible for the safety and security of ships and prevention of pollutions from ships, is international regulatory forum for maritime transportation. The most important IMO conventions are Standards of Training Certification and Watchkeeping (STCW); International Ship and Port Facility Security Code (ISPS Code); International Convention for the Prevention of Pollution from Ships (MARPOL); International Convention for the Safety of Life at Sea (SOLAS). It has been aimed to establishing acceptable quality level, determines minimum requirements, set a general framework etc. in an international basis by entering into force such conventions. However, to become an excellence mode of transportation, maritime organizations should do more than just compliance their organizations, and operations with international rules.

At that point, organizational, operational, proprietary process becomes more critical for maritime organizations, since operational reliability, safety, cost etc. is concern for companies' executives.

II. INFORMATION SYSTEMS

A. What is an "Information System"?

"Information systems are interrelated components working together to collect, process, store, and disseminate information to support decision making, coordination, control, analysis, and visualization in an organization.

B. Components of information systems

The six components that must come together in order to produce an information system are:

1) Hardware.

The term hardware refers to machinery. This category includes the computer itself, which is often referred to as the central processing unit (CPU), and all of its support equipment. Among the support, equipment are input and output devices, storage devices and communications devices.

2) Software.

The term software refers to computer programs and the manuals (if any) that support them. Computer programs are machine-readable instructions that direct the circuitry within the hardware parts of the system to function in ways that produce useful information from data. Programs are generally stored on some input/output medium, often a disk or tape.

3) Data.

Data are facts that are used by programs to produce useful information. Like programs, data are generally stored in machine-readable form on disk or tape until the computer needs them.

4) Procedures.

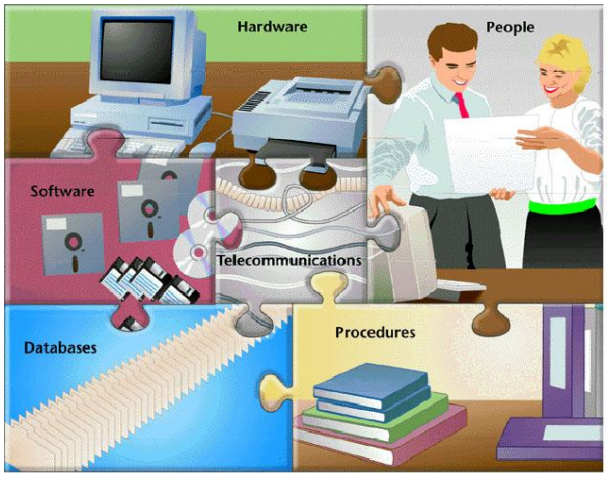
Procedures are the policies that govern the operation of a computer system. "Procedures are to people what software is to hardware" is a common analogy that is used to illustrate the role of procedures in a system.

5) People.

Every system needs people if it is to be useful. Often the most overlooked element of the system are the people, probably the component that most influence the success or failure of information systems. This includes "not only the users, but those who operate and service the computers, those who maintain the data, and those who support the network of computers."

6) Network – Communication

Telecommunications are used to connect, or network, computer systems and portable and wearable devices and to transmit information. Connections are established via wired or wireless media. Wired technologies include coaxial cable and fiber optics. Wireless technologies, predominantly based on the transmission of microwaves and radio waves, support mobile computing.
Various computer network configurations are possible, depending on the needs of an organization. Local area networks (LANs) join computers at a particular site, such as an office building or an academic campus. Metropolitan area networks (MANs) cover a limited densely populated area and are the electronic infrastructure of “smart cities.” Wide area networks (WANs) connect widely distributed data centers, frequently run by different organizations. Peer-to-peer networks, without a centralized control, enable broad sharing of content. The Internet is a network of networks, connecting billions of computers located on every continent. Through networking, users gain access to information resources, such as large databases, and to other individuals, such as coworkers, clients, friends, or people who share their professional or private interests. Internet-type services can be provided within an organization and for its exclusive use by various intranets that are accessible through a browser; for example, an intranet may be deployed as an access portal to a shared corporate document base. To connect with business partners over the Internet in a private and secure manner, extranets are established as so-called virtual private networks (VPNs) by encrypting the messages.
Extensive networking infrastructure supports the growing move to cloud computing, with the information-system resources shared among multiple companies, leading to utilization efficiencies and freedom in localization of the data centers. Software-defined networking affords flexible control of telecommunications networks with algorithms that are responsive to real-time demands and resource availabilities.



C. Types of Information Systems

- KMS (Knowledge Management Systems)

A knowledge Management system (KMS) is a specialized system built to promote the creation of knowledge and to make sure that knowledge and technical skills are proper integrated into business. It helps the knowledge workers in creating and propagating new information and knowledge by providing them the graphics, analytical, communications, and document management tools.
The knowledge workers also need to search for knowledge outside the organization. Thus, knowledge work system must give easy access to external databases. In addition, knowledge work systems should have user-friendly interface to help users to get the required information quickly and easily.
Some examples of knowledge work systems are computer-aided design (CAD) systems, virtual reality systems, and financial workstations.
Computer-aided design (CAD) systems: These systems are used for automating the creation and revision of designs using computers and graphics software. The CAD software has the capability to provide design specifications for tooling and

manufacturing process. This saves much time and money while making a manufacturing process.
Virtual Reality System: These systems have more capabilities than CAD systems for visualization, rendering and simulation. They make use of interactive graphics software to build computer-generated simulations which almost look like real. They can be used in educational, scientific and business work.
Financial Workstations: They are used to combine a wide range of data from internal as well as external sources. This data includes contact management data, market data and research reports. Financial workstations help in analyzing trading situations and large amount of financial data within no time. It is also used for portfolio management.

- OAS (Office Automation Systems)

An office automation system (OAS) is a collection of communication technology, computers and persons to perform official tasks. It executes office transactions and supports official activities at every organizational level. These activities can be divided into clerical and managerial activities.

Clerical activities performed with the help of office automation system include preparing written communication, typesetting, printing, mailing, scheduling meetings, calendar keeping, etc. Under managerial activities, office automation system helps in conferencing, creating reports and messages, and controlling performance of organization. Many applications like word processing, electronic filing and e-mail are integrated in office automation system.

Word processing is used for the preparation of documents like letters, reports, memos, or any type of printable material by electronic means. The text is entered by keyboard and displayed on the computer's display unit. This text can be edited, stored, and reproduced with the help of commands present in the word processor. Word processors have facilities for spell checking, grammar checking, counting (character, lines, pages, etc.), automatic page numbering, index creation, header and footer, etc.

E-mail or electronic mail facilitates the transfer of messages or documents with the help of computer and communication lines. This helps in speedy delivery of mails and also reduces time and cost of sending a paper mail. E-mail supports not only the transfer of text messages but it also has options for sending images, audio, video, and many other types of data.

Voice mail, an important call service, allows recording and storing of telephone messages into the computer's memory. The intended person can retrieve these messages any time.

- MIS (Management Information Systems)

Management information systems are especially developed to support planning, controlling, and decision-making functions of middle managers. A management information system (MIS) extracts transaction data from underlying TPSs, compiles them, and produces information products in the form of reports, displays or responses.
These information products provide information that conforms to decision-making needs of managers and supervisors. Management information systems use simple routines like summaries and comparisons which enable managers to take decisions for which the procedure of reaching at a solution has been specified in advance.
Generally, the format of reports produced by MIS is pre-specified. A typical MIS report is a summary report, such as a report on the quarterly sales made by each sales representative of the organization. Another type of management information system report is an; for example, exception report that specifies the exception conditions the sales made by some sales representative is far below than expected.
Usually, management information systems are used to produce reports on monthly, quarterly, or yearly basis. However, if managers want to view the daily or hourly data, MIS enables them to do so. In addition, they provide managers online access to the current performance as well as past records of the organization.

- TPS (Transaction Processing Systems)

Every firm needs to process transactions in order to perform their daily business operations. A transaction refers to any event or activity that affects the organization. Depending on the organization's business, transactions may differ from one organization to another. In a manufacturing unit, for example, transactions include order entry, receipt of goods, shipping, etc., while in a bank, transactions include deposits and withdrawals, cashing of cheques etc.
However, some transactions, including placing orders, billing customers, hiring employees, employee record keeping, etc., are common to all organizations. To support the processing of business transactions, the transaction processing systems (TPS) are used in the organizations.

- ESS (Executive Support Systems)

An executive support system (ESS) – an extension of MIS – is a computer based information system that helps into decision making at the top-level of an organization. The decisions taken with the help of executive support system are non-routine decisions that affect the entire organization and, thus, require judgement and sight.
As compared to DSSs, ESSs offer more general computing capabilities, better telecommunications and efficient display options. They use the advanced graphics software to display the critical information in the form of charts or graphs that help senior executives to solve a wide range of problems. To make effective decisions, they use summarized internal data from MIS and DSS as well as data from external sources about events like new tax laws, new competitors, etc. They filter, compress, and track data of high importance and make it available to the strategic-level managers.
Executive support systems help to monitor performance, track activities of competitors, identify opportunities, and forecast trends. They also assist senior managers in answering the following question:
• What business should we do?
• How are our competitors doing the business?
• Which units can be sold and which new units are to be bought?

- DSS (Decision Support Systems)

A decision support system (DSS) is an interactive computer-based information system that, like MIS, also serves at the management level of an organization. However, in contrast to MIS, it processes information to support the decision making process of managers. It provides middle managers with the information that enables them to make intelligent decisions. A decision support system in a bank, for example, enable a manager to analyze the changing trends in deposits and loans in order to ascertain the yearly targets.

Decision support systems are designed for every manager to execute a specific managerial task or problem. Generally, they help managers to make semi-structured decisions, the solution to which can be arrived at logically. However, sometimes, they can also help in taking complex decisions. To support such decisions, they use information generated by OASs and TPSs.

Decision support systems have more analytical power as compared to other information systems. They employ a wide variety of decision models to analyze data or summarize vast amount of data into a form (usually form of tables or charts) that make the comparison and analysis of data easier for managers. They provide interactive environment so that the users could work with them directly, add or change data as per their requirements, and ask new questions.

D. Use of Information Systems

Some examples of KMS

- Universities
- Scientific research
- Stock market

Some examples of OAS

- Document management
- Teleconference
- Electronic publishment
- Storage &Archiving file system

Some examples of MIS

- Sales management systems
- Inventory control systems
- Budgeting systems
- Management Reporting Systems (MRS)
- Personnel (HRM) systems

Some examples of TPS

- Payroll systems
- Order processing systems
- Reservation systems
- Stock control systems
- Systems for payments and funds transfers

Some examples of ESS

- Executive Support Systems tend to be highly individualized and are often custom made for a particular client group; however, a number of off-the-shelf ESS packages do exist and many enterprise level systems offer a customizable ESS module.

Some examples of DSS

- Group Decision Support Systems (GDSS)
- Computer Supported Co-operative work (CSCW)
- Logistics systems
- Financial Planning systems
- Spreadsheet Models?

E. Information systems in shipping

Information systems play a very important role in the management of the shipping company.

Given the increase of international maritime traffic and port capacity, shipping sector actors need to become more reactive. The adoption of information systems has become a major factor in improving companies' performance and flexibility. Shipping information systems are emerging as essential to the proper functioning of logistic operations involving multiple complex supply chains actors.

Benefits of Information system

Lower Cost: The e-sourcing system assisted them to procure products from a list of suppliers and they were benefited from competitive pricing which resulted in procurement costs. Cost saving per customer was increased due to increased efficiency.

Improved Communication: As the data was consolidated into a single system, hence staff gained an integrated view of operations.

Improved Management Control: ERP systems and re-engineering process helped in improved business management. This gave the managers a complete view of the company's operations and also equipped the staff with detailed information they required to plan, execute and evaluate complex initiatives. The managers were also able to make decisions and ensure problems were addressed immediately. Performance evaluation was easier and could be easily done on a global basis and medium and long term strategy planning could be done due to data availability.

New Capability: An HR platform can help to improve the efficiency of the department. The managers has complete history of the staff and also discard applications. This resulted in increased efficiency of HR staff which could focus more on attracting and retaining skilled employees and also train them.

Improved Customer Service: Due to its service network it could respond faster to customers' demands. Detailed sales and marketing plans could be developed.

III. INFORMATION SYSTEMS SECURITY

A. Intoduction

Information systems security is responsible for the integrity and safety of system resources and activities. Most organizations in developed countries are dependent on the secure operation of their information systems. In fact, the very fabric of societies often depends on this security. Multiple infrastructural grids—including power, water supply, and health care—rely on it. Information systems are at the heart of intensive care units and air traffic control systems. Financial institutions could not survive a total failure of their information systems for longer than a day or two. Electronic Funds Transfer Systems (EFTS) handle immense amounts of money that exist only as electronic signals sent over the

networks or as spots on storage disks. Information systems are vulnerable to a number of threats and require strict controls, such as continuing countermeasures and regular audits to ensure that the system remains secure.
Although instances of computer crime and abuse receive extensive media attention, human error is estimated to cause greater losses in information systems operation. Disasters such as earthquakes, floods, and fires are the particular concern of disaster recovery planning, which is a part of a corporate business continuity plan. A contingency scheme is also necessary to cover the failure of servers, telecommunications networks, or software.

B. *Implementation*

Bellow there are some of implementation principles for a global information security strategy:

- Create list of informational assets.
- Define security classifications of databases.
- Define security classifications for other assets.
- Define security levels for classified assets.
- Analyze need for security zones.
- Add security modules to specification of informational assets.
- Create list of security measures.
- Create implementation plan for security measures and implement it.
- Check security situation, evaluate risks, and implement additional measures (when needed).

IV. ISO 27001.2013

A. *What is an ISO*

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 162 national standards bodies.
Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.
The ISO story began in 1946 when delegates from 25 countries met at the Institute of Civil Engineers in London and decided to create a new international organization 'to facilitate the international coordination and unification of industrial standards'. On 23 February 1947 the new organization, ISO, officially began operations.
Since then, they have published over 21991 International Standards covering almost all aspects of technology and manufacturing.
ISO is derived from the Greek *isos*, meaning equal.
It's based in Geneva, Switzerland.

B. *ISO 27000 family*

The ISO/IEC 27000 family of standards helps organizations keep information assets secure.
Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.
ISO/IEC 27001 is the best-known standard in the family providing requirements for an Information Security Management System (ISMS).

C. *Introduction of ISO 27001.2013*

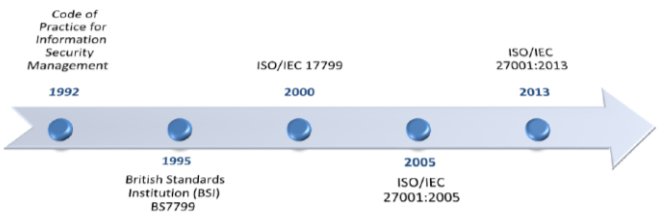
ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
ISO 27001 is an internationally recognized standard that ensures the information security of an enterprise. An Information Security Management System maintains the requirements that result to the effective management and gate keeping of information security in and out of the company/organization.
Its purpose is to ensure that access to information is authorized and controlled, but also to guarantee the accuracy and completeness of information and processing methods.
ISO 27001:2013 is the standard for Information Security Management; it is part of the ISO 27000 family of standards which helps organizations keep information assets secure. Adopted by thousands of organizations across the world, its implementation puts in place a systematic approach to managing sensitive organizational information, ensuring it remains both secure and available. It is a broad standard covering process, personnel, physical and technical security.
ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). There are three key issues to note about the standard:

1) Its generic requirements mean that it is applicable to all organisations, regardless of size, type or nature. However, you tailor it to the exact needs of your organisation through the information security controls that you select to implement within your Information Security Management System.

2) It takes a flexible, risk-driven approach.

3) It is dynamic – it focuses on continual improvement and helps the organisation keep ahead of changes both within and outside the organisation.

D. *Historical evolution*



- 1992

The Department of Trade and Industry (DTI), which is part of the UK Government, publish a 'Code of Practice for Information Security Management'.

- 1995

This document is amended and re-published by the British Standards Institute (BSI) as BS7799.

- 2000

In December, BS7799 is again re-published, this time as a fast tracked ISO standard. It becomes ISO/IEC 17799

- 2005

ISO/IEC 27001:2005 is published, this is a specification for an ISMS (information security management system), which aligns with ISO 17799 and is compatible with ISO 9001 and ISO 14001.

- 2013

ISO/IEC 27001:2013 A New information security standard published on the 25/09/2013. It cancels and replaces ISO 27001:2005

E. Structure of ISO 27001.2013

1) Context of the Organization (company)

External and internal issues shall be determined that are relevant to the organization's purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

a) Understanding The Needs And Expectations Of Interested Parties

The organization shall determine interested parties that are relevant to the information security management system and the requirements of these interested parties relevant to information security.

b) Determining The Scope Of The Information Security Management System

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

c) Information Security Management System

Based on the monitoring results, the organization needs to implement the identified improvements, communicate them to all the interested parties with sufficient details, and ensure that the improvements achieve their intended objectives.
To establish an ISMS the organization needs to define the ISMS which includes the following steps:

Important stages	Issues to consider when establishing an ISMS
Scope	Based on business characteristics, location, assets and technology, and justifications for any exclusion from scope
Risk assessment approach	1. Risk assessment methodology, and business information security, legal and regulatory requirements 2. Criteria for accepting risks, and acceptable risks levels
Risk identification	1. Asset identification and asset owner identification 2. Threats to those assets 3. Vulnerabilities 4. Impact of loss of confidentiality , integrity and availability
Risk analysis and evaluation	1. Business impacts assessment 2. Realistic likelihood assessment considering the threats and vulnerabilities 3. Risk level estimation 4. Risk acceptability or treatment, depending on the risk acceptance criteria
Risk treatment option	1. Application of appropriate controls 2. Objective risk acceptance in accordance with the organization's policies 3. Risk avoidance 4. Risk transfer to other parties (insures, suppliers)
Control objectives and controls for the treatment of risks	1. Selection and implementation of controls based on the requirements identified by the risk assessment and treatment process. 2. Selection of controls from Annex A of ISO 27001 when appropriate, to cover the risk assessment and treatment process. 3. Additional controls may be selected outside of Annex A

2) Leadership

a) leadership and commitment:

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

• Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

• Ensuring the integration of the information security management system requirements into the organization's processes;

• Ensuring that the resources needed for the information security management system are available;

• Communicating the importance of effective information security management and of conforming to the information security management system requirements;

• Ensuring that the information security management system achieves its intended outcome(s);

• Directing and supporting persons to contribute to the effectiveness of the information security management systems;

• Promoting continual improvement; and

• Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

b) Policy:

Top management shall establish an information security policy that:

• Is appropriate to the purpose of the organization;

• Includes information security objectives or provides the framework for setting information security objectives;

• Includes a commitment to satisfy applicable requirements related to information security; and

• Includes a commitment to continual improvement of the information security management system.

The information security policy shall:

- Be available as documented information.
- Be communicated within the organization; and
- Be available to interested parties, as appropriate

c) Organizational Roles, Responsibilities And Authorities:

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.
Top management shall assign the responsibility and authority for:

• Ensuring that the information security management system conforms to the requirements of this International Standard; and

• Reporting on the performance of the information security management system to top management.

3) Planning

When planning for the information security management system, the organization shall consider the issues and the requirements referred in the standard and determine the risks and opportunities that need to be addressed to:

• Ensure the information security management system can achieve its intended outcome(s);

• Prevent, or reduce, undesired effects; and

• Achieve continual improvement.

The organization shall plan:

• Actions to address these risks and opportunities; and

• How to:

• Integrate and implement the actions into its information security management system processes;

• Evaluate the effectiveness of these actions.

4) Support

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system, such as:

• Competence,

• Awareness,

• Communication, and

• Documented information.

5) Operation

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in the standard. The organization shall perform information security risk assessments at planned intervals, and shall also implement the information security risk treatment plan.

6) Performance Evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organization's own requirements and to the International Standard requirements.

7) Improvement

Improvement of ISMS consists of corrective actions. They should fulfill the requirements as listed in the table below:

Corrective action Requirements
Identifying
Determing the causes of nonconformities
Evaluating the need for actions to ensure that the nonconformities are not repeated
Determining and implementing the corrective action needed
Recording results of the action taken
Reviewing of the corrective action taken

F. Benefits of ISO 27001.2013.

There are a number of clear business benefits in adopting ISO 27001, either as best practice or by formally certifying against it. Those benefits and outlines the steps towards achieving certification.

1) Key benefits.

a) It improves enterprise security.

Whether the organization using ISO 27001 decides to go for full certification or not, ISO 27001 brings with it a systematic examination of the organization's information security risks, taking account of the threats, vulnerabilities and impacts that are unique to that organization.
It provides a framework for the selection and implementation of a coherent suite of information security controls and/or other forms of risk treatment to address those risks that are deemed unacceptable to that individual organization.
It also brings with it a continual improvement ethos to ensure that the risk treatments continue to meet the organization's individual information security needs on an on-going basis.

b) It is an independent, unbiased measurement of the actual information security state.

One of the major drivers for organizations to work towards certification is that the standard provides an internationally recognized, externally assured, quality mark for Information Security Management. ISO 27001 is the industry yard stick that most Information Security Management activity is measured against.
External assurance is provided to both the customer and the organization's management on the actual state of the organization's Information Security Management System.

External, qualified ISO 27001 auditors impartially review and assess the organization's Information Security Practices, policy procedures and their operation against the standard.
This provides a clear, unbiased, scientific view of the actual state of the present Information Security Practices.

c) It increases customer confidence

ISO 27001 certification gives service consumers and customers an easily recognizable security hallmark.
Using the ISO 27001 logo on company literature is a continual reminder to potential and existing customers that demonstrates commitment to information security at all levels of the organization. The certification demonstrates credibility and trust.

d) It reduces customer and supply chain audit

ISO 27001 certification reduces third party scrutiny of your Information Security Management by customers and the wider supply chain. It provides assurance to customers that their information is appropriately protected and, as such, reduces the need to undertake time consuming and costly onsite security audits reducing time and cost for both parties.

e) It provides market differentiation

Holding an ISO 27001 certification is an increasing requirement to do business in many different verticals, especially when processing any type of personal or sensitive data. The achievement of ISO 27001 will differentiate two competing organizations in the market place, providing a valuable competitive advantage.

f) Increased legislative and regulatory compliance

ISO 27001 supports compliance with relevant laws such as the Data Protection Act 1998 and software copyright legislation. This in turn reduces the risk of facing prosecution and fines.
An organization's liability in security incidents may be reduced if it is certified ISO 27001 compliant. Under the Data Protection Act 1998, organizations are obliged to have an institutional framework designed to ensure the security of all personal data. As ISO 27001 is the current international benchmark for Information Security Management, it is increasingly recognized that compliance with the standard is supportive evidence of adequate security.

g) Considerations and outcomes

To achieve ISO 27001 certification, an organization must produce documentation that demonstrates that it has developed an Information Security Management System that complies with the standard. Organizations should consider producing most of this documentation even if they are not going for certification as it provides a best practice approach for compliance as well.

2) The process of creating the documentation takes the organisation through a number of vital steps, including:

a) Understanding the organisation's security landscape and practices.

b) Identifying the business drivers for implementing and maintaining an effective Information Security Management System and the benefits of achieving ISO 27001 certification.

c) Defining the scope of the Information Security Management System and the risk management approach you will take.

d) Selecting the appropriate information security controls from the standard in order to create a Statement of Applicability (SoA).

e) Using the Statement of Applicability (SoA) to create a risk treatment plan, which describes your information security objectives and how you will achieve them.

f) Putting in place effective information security awareness and training programmes.

3) Whether or not you choose to apply for certification, these steps will provide your organisation with:

a) A clear strategic approach and management commitment to information security with defined information security objectives.

b) Specific information security responsibilities defined.

c) Established Information Security Management System processes that are repeatable and that drive continual improvement.

d) A clear approach to risk assessment and management.

e) Effective information security awareness programme(s)

V. INFORMATION SYSTEMS SECURITY IN SHIPPING, ACCORDING TO ISO 27001.2013

A. ISO 27001.2013 Objects and Controls

As previously discussed, the adoption of the ISMS seems to be a very important decision for every company.
As per the ISO 27001, at least a minimum of set prerequisites need to be followed, 14 domains and 114 individual control points which define the framework need to unremittingly followed.
Of course, it is possible to adopt more control points, based on the needs and structure of every company.
The 114 control points are as follows:

1) (A5) Information Security Policies

a) (A5.1) Management direction for information security

Objective: to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

(A.5.1.1) POLICIES FOR INFORMATION SECURITY

Control – a set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

(A.5.1.2) REVIEW OF THE POLICIES FOR INFORMATION SECURITY.

Control – – the policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and, effectiveness.

2) (A6) Organization of Information Security

a) (A6.1) Internal organization.

Objective: to establish a management framework to initiate and control the implementation and operation of information security within the organization.

(A6.1.1) INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Control – all information security responsibilities shall be defined and allocated.

(A6.1.2) SEGREGATION OF DUTIES

Control – conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organizations assets.

(A6.1.3) CONTACT WITH AUTHORITIES

Control – appropriate contacts with relevant authorities shall be maintained.

(A6.1.4) CONTACT WITH SPECIAL INTEREST GROUPS

Control – appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

(A6.1.5) INFORMATION SECURITY IN PROJECT MANAGEMENT

Control – information security shall be addressed in project management, regardless of the type of the project.

b) (A6.2) Mobile devices and teleworking

Objective – to ensure the security of teleworking and use of mobile devices.

(A6.2.1) MOBILE DEVICE POLICY

Control – a policy and supporting security measures shall be adopted to manage risks introduced by using mobile devices.

(A6.2.2) TELEWORKING

Control – a policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

3) (A7) Human resource security

a) (A7.1) Prior to employment

(A7.1.1) SCREENING

Control – background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to business requirements, the classification of the information to be accessed, and the perceived risks.

(A7.1.2) TERMS AND CONDITIONS OF EMPLOYMENT

Control – the contractual agreements with employees and contractors shall their and the organization's responsibility for information security.

b) (A7.2) During employment

Objective – to ensure that all employees and contractors are aware of and fulfil their information security responsibilities.

(A7.2.1) MANAGEMENT RESPONSIBILITIES

Control – management shall require employees and contractors to apply security in accordance with established policies and procedures of the organization.

(A7.2.2) INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

Control – all employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in the organizations policies and procedures, as relevant to their job function.

(A7.2.3) DISCIPLINARY PROCESS

Control – there shall be a formal and communicated disciplinary process to take action against employees who have committed an information security breach.

c) (A7.3) Termination and change of employment

Objective – to protect the organizations interests as part of the process of changing or terminating employment.

(A7.3.1) TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES

Control – information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

4) (A8) Asset Management

a) (A8.1) Responsibility for Assets

Objective – to identify organizational assets and define appropriate protection responsibilities.

(A8.1.1) INVENTORY OF ASSETS

Control – assets associated with information security and information processing facilities shall be identified and an inventory of these assets shall drawn up and maintained.

(A8.1.2) OWNERSHIP OF ASSETS

Control –assets maintained in the inventory shall be owned.

(A8.1.3) ACCEPTABLE USE OF ASSETS

Control – rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented and implemented.

(A8.1.4) RETURN OF ASSETS

Control – all employees and external party users shall return all of the organizations assets in their possession upon termination of their employment, contract or assignment.

b) (A8.2) Information Classification

Objective – to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

(A8.2.1) CLASSIFICATION OF INFORMATION

Control – information shall be classified in terms of its legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

(A8.2.2) LABELLING OF INFORMATION

Control – an appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

(A8.2.3) HANDLING OF ASSETS

Control – procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

c) (A8.3) Media handling

(A8.3.1) MANAGEMENT OF REMOVABLE MEDIA

Control - procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

(A8.3.2) DISPOSAL OF MEDIA

Control - Media shall be disposed of securely when no longer required, using formal procedures.

(A8.3.3) PHYSICAL MEDIA IN TRANSIT

Control - Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

5) (A9) Access control

a) (A9.1.) Business requirements of access control

Objective – to limit access to information and information processing facilities.

(A9.1.1) ACCESS CONTROL POLICY

Control - An access control policy shall be established, documented, and reviewed based on business and security requirements.

(A9.1.2) ACCESS TO NETWORKS AND NETWORK SERVICES

Control – Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

b) (A9.2) User access management

Objective – to ensure authorized user access and to prevent unauthorized access to systems and services.

(A9.2.1) USER REGISTRATION AND DEREGISTRATION

Control - a formal user registration and de-registration procedure in implemented to enable assignment of access rights.

(A9.2.2) USER ACCESS PROVISIONING

Control – a formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

(A9.2.3) MANAGEMENT OF PRIVILEGED ACCESS RIGHTS

Control – the allocation and use of privileged access rights shall be restricted and controlled.

(A9.2.4) MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS

Control - The allocation of secrete authentication information shall be controlled through a formal management process.

(A9.2.5) REVIEW OF USER ACCESS RIGHTS

Control – Asset owners shall review users' access rights at regular intervals.

(A9.2.6) REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS

Control – The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

c) (A9.3) User Responsibilities

Objective – to make users accountable for safeguarding their authentication information.

(A9.3.1) USE OF SECRET AUTHENTICATION INFORMATION.

Control - Users shall be required to follow the organization's practices in the use of secrete authentication information.

d) (A9.4) System and application access control.

Objective – to prevent unauthorized access to systems and applications.

(A9.4.1) INFORMATION ACCESS RESTRICTION

Control - Access to information and application system functions shall be restricted in accordance with the access control policy.

(A9.4.2) SECURE LOG-ON PROCEDURES

Control – where required by the access control policy, access to systems and applications shall be controlled by secure log-on procedures.

(A9.4.3) PASSWORD MANAGEMENT SYSTEM

Control – password management systems shall be interactive and shall ensure quality passwords.

(A9.4.4) USE OF PRIVILEGED UTILITY PROGRAMS.

Control - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

(A9.4.5) ACCESS CONTROL TO PROGRAM SOURCE CODE

Control - Access to program source code shall be restricted.

6) (A10)Cryptography

a) (A10.1) Cryptographic Controls

Objective - To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

(A10.1.1) POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

Control - A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

(A10.1.2) KEY MANAGEMENT

Control – a policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented throughout their whole lifetime.

7) (A11) Physical and Environmental Security

a) (A11.1) Secure areas

Objective – to prevent unauthorized physical access, damage and interference to the organizations information and information processing facilities

(A11.1.1) PHYSICAL SECURITY PERIMETER

Control – security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

(A11.1.2) PHYSICAL ENTRY CONTROLS

Control – secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

(A11.1.3) SECURING OFFICES, ROOMS AND FACILITIES

Control – physical security for offices, rooms and facilities shall be designed and applied.

(A11.1.4) PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

Control – physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

(A11.1.5) WORKING IN SECURE AREAS

Control – procedures for working in secure areas shall be designed and applied.

(A11.1.6) DELIVERY AND LOADING AREAS.

Control – access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

b) (A11.2) Equipment

Objective – to prevent loss, damage, theft or compromise of assets and interruption to the organizations operations.

(A11.2.1) EQUIPMENT SITING AND PROTECTION

Control – equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

(A11.2.2) SUPPORTING UTILITIES

Control – equipment shall be protected from power failures or other disruptions caused by failures in supporting utilities.

(A11.2.3) CABLING SECURITY

Control – power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

(A11.2.4) EQUIPMENT MAINTENANCE

Control – equipment shall be correctly maintained to ensure its continued availability and integrity.

(A11.2.5) REMOVAL OF ASSETS

Control – equipment, information or software shall not be taken offsite without prior authorization.

(A11.2.6) SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES.

Control – security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

(A11.2.7) SECURE DISPOSAL OR RE-USE OF EQUIPMENT

Control – all items of equipment containing storage media shall verified be to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

(A11.2.8) UNATTENDED USER EQUIPMENT

Control - Users shall ensure that unattended equipment has appropriate protection.

(A11.2.9) CLEAR DESK AND CLEAR SCREEN POLICY

Control - A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

8) (A12) Operations Security

a) (A12.1) Operational procedures and responsibilities

Objective – to ensure the correct and secure operation of information processing facilities.

(A12.1.1) DOCUMENTED OPERATING PROCEDURES

Control – operating procedures shall be documented, maintained and made available to all users who need them.

(A12.1.2) CHANGE MANAGEMENT

Control – changes to the organization, business processes and information processing facilities and systems shall be controlled.

(A12.1.3) CAPACITY MANAGEMENT

Control – the use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

(A12.1.4) SEPARATION OF DEVELOPMENT, TEST AND OPERATIONAL ENVIRONMENTS

Control – development, test and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

b) (A12.2) Protection from malware

Objective – to ensure that information and information processing facilities are protected against malware.

(A12.2.1) CONTROLS AGAINST MALWARE

Control – detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

c) (A12.3) Back up

Objective – protect against the loss of data.

(A12.3.1) INFORMATION BACK-UP

Control – back-up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed back-up policy.

d) (A12.4) Logging and Monitoring

Objectives – to record events and generate evidence.

(A12.4.1) EVENT LOGGING

Control – event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

(A12.4.2) PROTECTION OF LOG INFORMATION

Control - Logging facilities and log information shall be protected against tampering and unauthorized access.

(A12.4.3) ADMINISTRATOR AND OPERATOR LOGS

Control - System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

(A12.4.4) CLOCK SYNCHRONIZATION

Control - The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

e) (A12.5) Control of operational software

Objective – to ensure the integrity of operational systems.

(A12.5.1) INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS

Control - procedures shall be in place to control the installation of software on operational systems.

f) (A12.6) Technical vulnerability management

Objective – to prevent exploitation of technical vulnerabilities.

(A12.6.1) MANAGEMENT OF TECHNICAL VULNERABILITIES

Control - information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

(A12.6.2) RESTRICTIONS ON SOFTWARE INSTALLATION

Control – rules governing the installation of software by users shall be established and implemented.

g) (A12.7) Information system audit considerations

Objective – to minimize the impact of audit activities on operational systems.

(A12.7.1) INFORMATION SYSTEMS AUDIT CONTROLS

Control - Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.

9) (A13) Communications Security

a) (A13.1) Network security management

Objective – to ensure the protection of information in networks and its supporting information processing facilities.

(A13.1.1) NETWORK CONTROLS

Control - Networks shall be managed and controlled, in order to be protected information in systems and applications.

(A13.1.2) SECURITY OF NETWORK SERVICES

Control – Security mechanisms, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

(A13.1.3) SEGREGATION IN NETWORKS

Control - Groups of information services, users and information systems shall be segregated on networks.

b) (A13.2) Information transfer

Objective – to maintain the security of information and software transferred within an organization and with any external entity.

(A13.2.1) INFORMATION TRANSFER POLICIES AND PROCEDURES

Control - Formal transfer policies, procedures, and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

(A13.2.2) AGREEMENTS ON INFORMATION TRANSFER

Control - Agreements shall be established for the secure transfer of business information and software between the organization and external parties.

(A13.2.3) ELECTRONIC MESSAGING

Control - Information involved in electronic messaging shall be appropriately protected.

(A13.2.4) CONFIDENTIALITY OR NONDISCLOSURE AGREEMENTS

Control – requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

10) (A14) System acquisition, Development and Maintenance

a) (A14.1) Security requirements of information systems

Objective - To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

(A14.1.1) INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION

Control – the information security related requirements shall be included in the requirements for new information systems or enhancements to existing information's systems.

(A14.1.2) SECURING APPLICATION SERVICES ON PUBLIC NETWORKS

Control – information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

(A14.1.3) PROTECTING APPLICATION SERVICES TRANSACTIONS

Control - Information involved in service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

b) (A14.2) Security in development and support processes

Objective - To ensure that information security is designed and implemented within the development lifecycle of information systems.

(A14.2.1) SECURE DEVELOPMENT POLICY

Control – rules for the development of software and systems shall be established and applied to developments within the organization.

(A14.2.2) SYSTEM CHANGE CONTROL PROCEDURES

Control – changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

(A14.2.3) TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES

Control - When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

(A14.2.4) RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES

Control - Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

(A14.2.5) SECURE SYSTEM ENGINEERING PRINCIPLES

Control – principles for engineering secure systems shall be established, documented, maintained and applied to any information systems implementation efforts.

(A14.2.6) SECURE DEVELOPMENT ENVIRONMENT

Control – organizations shall establish and appropriately protect sure development environments for system development and integration efforts that cover the entire system development lifecycle.

(A14.2.7) OUTSOURCED DEVELOPMENT

Control – the organization shall supervise and monitor the activity of out-sourced systems development.

(A14.2.8) SYSTEM SECURITY TESTING

Control – testing of security functionality shall be carried out during development.

(A14.2.9) SYSTEM ACCEPTANCE TESTING

Control – acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

c) (A14.3) Test data

Objective – To ensure the protection of data used for testing.

(A14.3.1) PROTECTION OF TEST DATA

Control - Test data shall be selected carefully, and protected and controlled.

11) (A15) Supplier Relationships

a) (A15.1) Information security in supplier relationships

Objective – to maintain an agreed level of information security and service delivery in-line with supplier agreements.

(A15.1.1) INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS

Control – information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the suppliers and documented.

(A15.1.2) ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS

Control – all relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

(A15.1.3) INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN

Control – agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

b) (A15.2.) Supplier service delivery management

Objective – to maintain an agreed level of information security and service delivery in line with supplier agreements.

(A15.2.1) MONITORING AND REVIEW OF SUPPLIER SERVICES.

Control – organizations shall regularly monitor, review and audit supplier delivery.

(A15.2.2) MANAGING CHANGES TO SUPPLIER SERVICES.

Control – changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls shall be managed, taking account of the criticality of the business information and processes involved and the re-assessment of the risks.

12) (A16) Information Security Incident Management

a) (A16.1) Management of information security incidents and improvements

(A16.1.1) RESPONSIBILITIES AND PROCEDURES

Control - Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

(A16.1.2) REPORTING INFORMATION SECURITY EVENTS

Control - Information security events shall be reported through appropriate management channels as quickly as possible.

(A16.1.3) REPORTING INFORMATION SECURITY WEAKNESSES

Control – employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

(A16.1.4) ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS

Control – information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

(A16.1.5) RESPONSE TO INFORMATION SECURITY INCIDENTS

Control – information security incidents shall be responded to in accordance with documented procedures.

(A16.1.6) LEARNING FROM INFORMATION SECURITY INCIDENTS

Control – knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

(A16.1.7) COLLECTION OF EVIDENCE

Control – the organization shall define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence.

13) (A17) Information Security Aspects of Business Continuity Management

a) (A17.1) Information security continuity.

Objective – information security continuity shall be embedded in the organization's business continuity management systems.

(A17.1.1) PLANNING INFORMATION SECURITY CONTINUITY.

Control – the organization shall determine its requirements for information security and continuity of information security management in adverse situations, e.g. a crisis or disaster.

(A17.1.2) IMPLEMENTING INFORMATION SECURITY CONTINUITY.

Control – the organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

(A17.1.3) VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY.

Control – the organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

b) (A17.2) Redundancies

Objective – to ensure availability of information processing facilities.

(A17.2.1) AVAILABILITY OF INFORMATION PROCESSING FACILITIES

Control – information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

14) (A18) Compliance

a) (A18.1) Compliance with legal and contractual requirements.

Objective - To avoid breaches of any legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

(A18.1.1) IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL REQUIREMENTS.

Control - All relevant legislative, statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

(A18.1.2) INTELLECTUAL PROPERTY RIGHTS.

Control - Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and on the use of proprietary software products.

(A18.1.3) PROTECTION OF RECORDS.

Control - records shall be protected from loss, destruction and falsification, in accordance with legislatory, regulatory, contractual, and business requirements.

(A18.1.4) PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

Control - privacy and protection of personally identifiable information shall be ensured as required in relevant legislation, regulations where applicable.

(A18.1.5) REGULATION OF CRYPTOGRAPHIC CONTROLS

Control - Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations.

b) (A18.2) Information security reviews.

Objective – to ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.

(A18.2.1) INDEPENDENT REVIEW OF INFORMATION SECURITY

Control – the organizations approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes occur.

(A18.2.2) COMPLIANCE WITH SECURITY POLICIES AND STANDARDS

Control - Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security polices, standards and any other security requirements.

(A18.2.3) TECHNICAL COMPLIANCE REVIEW.

Control - Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

VI. CONCLUSIONS

Shipping Industry is increasingly using systems that rely on digitization, integration, and automation, which calls for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet.

This brings the greater risk of unauthorized access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media.

The security of information and related technology is vital. The goal of every company is to work to reduce the number of security incidents and to enable organizations to be better prepared for attacks and to react more effectively.

A well-structured information security management system (ISMS) designed in accordance with international standards provides an ideal foundation for efficient, effective implementation of a comprehensive security strategy, particularly in an era where cyber threats and cyber security are prevalent issues.

The ISO 27001:2013 is the most acclaimed standard for information security management.

VII. REFERENCES

[1] International Organization for Standardization (www.iso.org/home.html)

[2] PwC_AT&C Information Security webinar presentation 6 June 2017.pdf (www.pwc.com.au)

[3] PECB Whitepaper ISO 27001.pdf (www.pecb.com)

[4] ROSSI_DNV_GL_Cyber_Security.pdf (www.dnvgl.com)

[5] Alan_Calder,_Steve_Watkins]_IT_Governance_A_Mana(b-ok.org).pdf (https://www.itgovernance.co.uk)

[6] Schemes for Auditing Security Measures.pdf (www.enisa.europa.eu)

[7] 2011_ENISA_Analysis_of_cyber_security_aspects_in_the_maritime_sector_1 0.pdf (www.enisa.europa.eu)

[8] ESC-White-paper-on-Maritime-Cyber-Security-2016_02.pdf (https://www.escgs.com/)

[9] aspida_cyber_pres.pdf (https://cyber.aspida.org/)

[10] benefits-of-iso27001-white-paper.pdf (www.capita.co.uk/itprofessionalservices)

[11] Overview of Maritime Cybersecurity_Final.pdf (https://www.theseus.fi)

[12] NIST.SP.800-12r1.pdf (https://doi.org/10.6028/NIST.SP.800-12r1)

[13] Information Security Management System (ISMS) Overview.pdf (https://chapters.theiia.org/)

[14] SEC1210CL_ISO27K_PH_r2.0.0_ITp_Demo.pdf (www.itpreneurs.com)

[15] an introduction to iso 27001 2013.pdf (https://shop.bsigroup.com)

[16] An_Overview_of_ISO_27000_Family_EN.pdf (http://www.infocloud.gov.hk/home/)

[17] Best-practice-Studie-2013.pdf (www.dnvgl.com)

[18] GlobalMarineTrends2030Report.pdf (www.futurenautics.com/)

[19] ics-annual-review-2017.pdf (www.ics-shipping.org)

[20] Information management for container line - case study for the co.pdf (https://commons.wmu.se/)

[21] ioannides.pdf (http://forums.capitallink.com/)

[22] ISMS Checklist.pdf (http://nwm.gov.in/)

[23] ISO27k_ISMS_implementation_and_certification_process_overview_v2.pptx (https://www.scribd.com/)

[24] ISO27k_ISMS_Mandatory_documentation_checklist_release_1.docx (http://www.iso27001security.com/)

[25] shipping-world-trade-and-the-reduction-of-co2-emissions.pdf (www.ics-shipping.org)

[26] notification_draft_2014_426_L_EN.DOC (http://www.eco.public.lu)

[27] Unit01a-Internationalshippingindustry_003.doc (www.marisec.org)