JAPAN P&I CLUB Vol.42 May 2018

P&I Loss Prevention Bulletin

The Japan Ship Owners' Mutual Protection & Indemnity Association Loss Prevention and Ship Inspection Department

Cyber risk and Cyber security countermeasures

JAPAN P&I CLUB
P&I Loss Prevention Bulletin

Contents

Text and forms provided by ORCA CO., LTD.

§1 Introduction

The threat of cyber attacks at sea have increased recently and our Club issues a circular entitled “Cyber risk and cyber security” accordingly. The necessity of cyber security countermeasures and guidelines have been set forth by the IMO (MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management) and each shipping organization.

1－1 Cyber risk and P&I insurance

Cyber risks have not been specified in the Japan P&I Club rules, however, a claim regarding the coverage of a cyber attack or cyber breach would be examined in the usual way with reference to the Rules. When the cyber attack would not fall under the definition of "war" or "act of terrorism" under rule 35, a member will be subject to cover along with his normal P&I insurance.

Sponsored by FURUNO
New Generated Bridge System　Voyager

For example, the following case would normally be subject to P&I insurance: The ship’s system gets infected with a virus via the onboard LAN system via the e-mail PC used for work or a crew member’s personal PC. The onboard PC’s software for work use is updated without permission or, as a result that particular crew member changed connection to the onboard LAN cable without permission. The electronic aid for navigation and propulsion breaks down, which causes damage to harbour facilities at the time of departure.

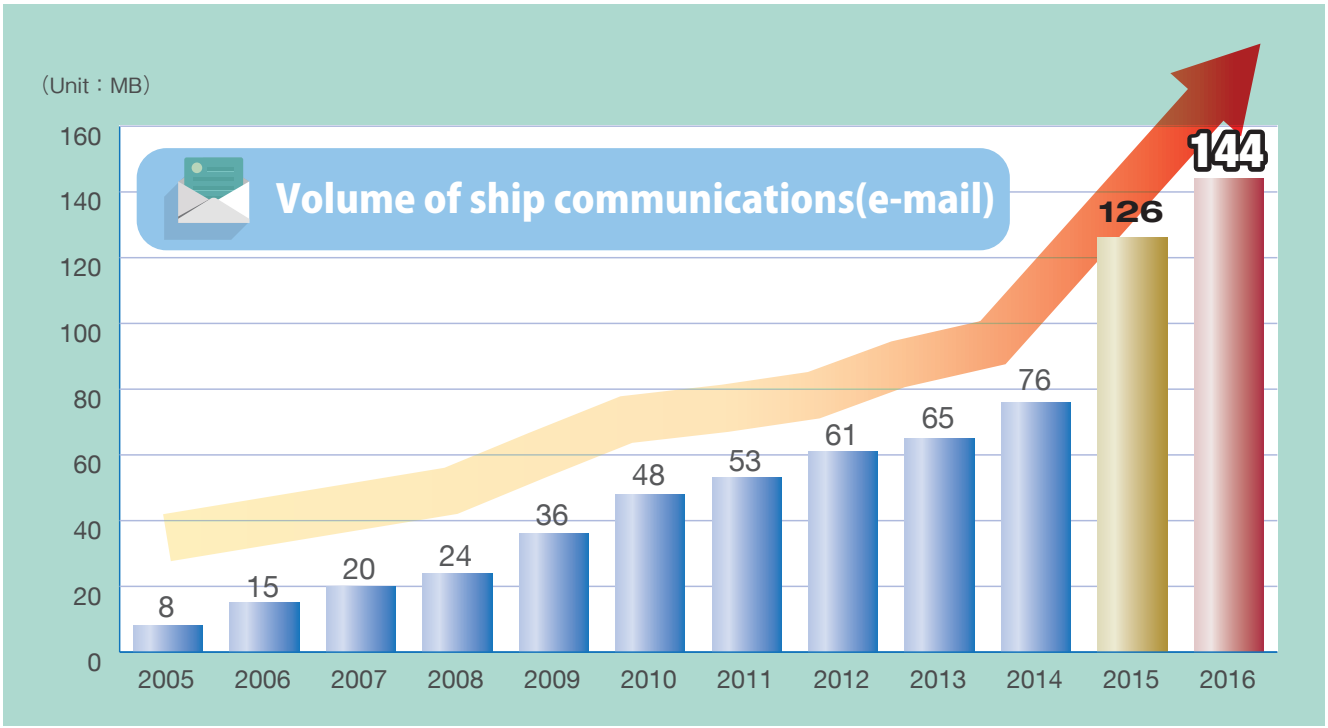
The following examples will not be covered by P&I insurance: For instance, there was a case whereby a certain amount of the ship’s store was transmitted mistakenly due to a hacked e-mail. In another case, the ship’s schedule was delayed because the crew was investigated by the authorities, because the uploaded video which was found in his personal PC appeared to be associated with terrorism. Further, a threatening email was sent to the ship as a fake money demand meaning that the ship might have been arrested. Such cases which do not develop into P&I accidents were reported.

§2 Example of a ship communications system that has been infected with a virus

2-1 Ship communications

Except for GMDSS (Global Maritime Distress and Safety System, which is equipment that is installed on a ship depending on the sea area that is to be sailed), V-SAT, Fleet Xpress, FBB, Iridium, internet using 4G, e-mail, telephones and Faxes are frequently used on the ship. This ship communication equipment is not only a communication tool between ship and shore, but also essential equipment for current navigation, such as weather routing, chart correction and PMS (Planned Maintenance System).

The volume of ship communications via e-mail have increased due to this. Graph 1 shows the volume of ship communications via e-mail by month over the last 12 years. Compared with 2005, the volume of communications in 2016 has increased by 18 times.



Graph 1 Volume of ship communications via e-mail by month over the last 12 years

2-2 Example of a system infected with a virus

On the other hand, along with the volume increase in ship communications, the number of ship systems that are prone to being infected with a virus are also occurring more frequently, and the way in which viruses infect systems are now more varied.

By around the year 2000, ship viral infection was blocked by the e-mail provider. When it came to ship's local network, because most vessels were not initially connected to an external network, there were many cases whereby people or crew who boarded the ship brought viruses on board with them physically.

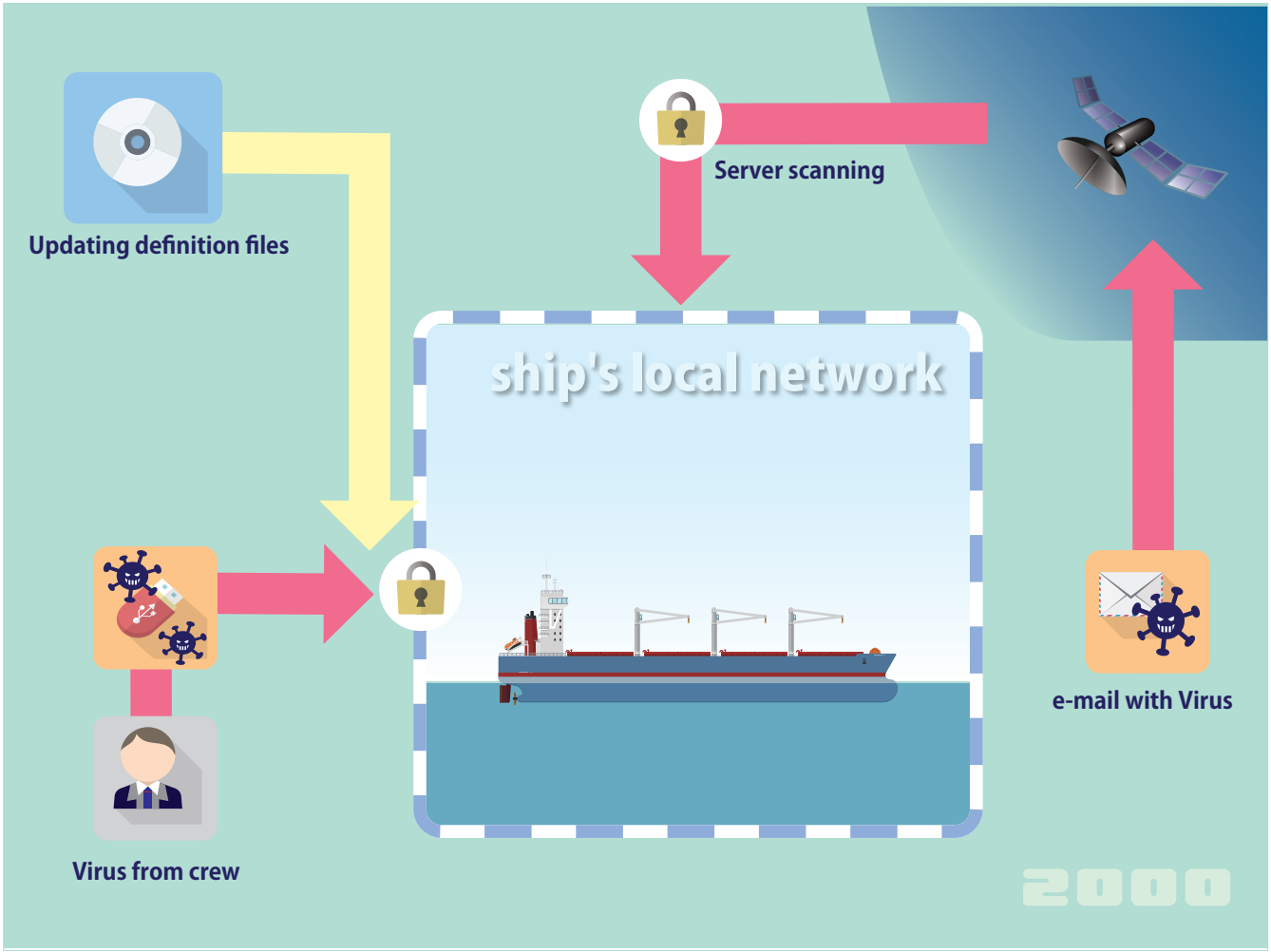


Fig. 2 Around 2000

However, since around 2010, there have been some cases whereby an intrusion of the latest virus caused the ship to be infected and, as a result, disrupted the e-mail system. This came about as a result of a member of crew using 3G/4G when calling at port.

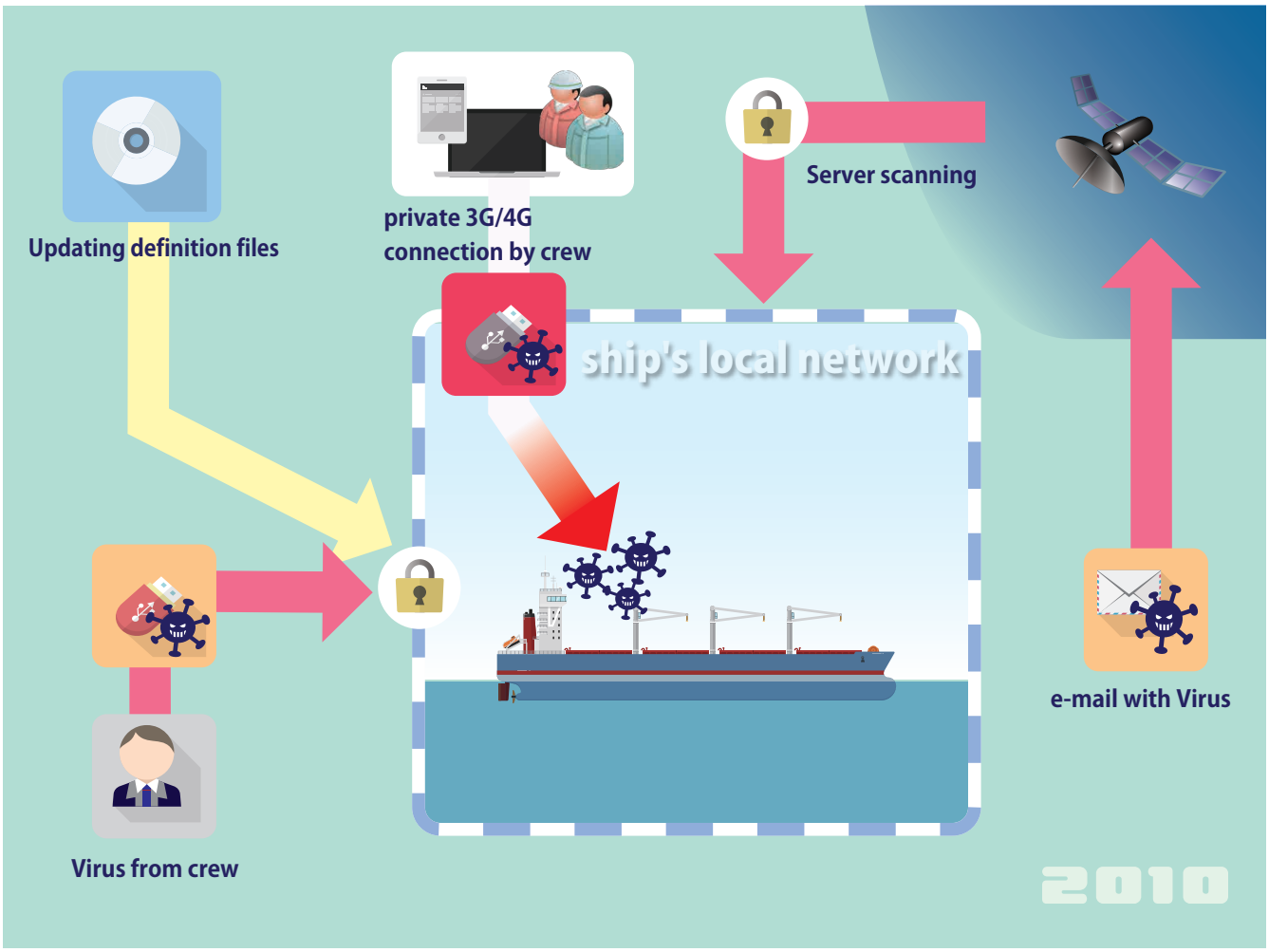


Fig. 3　Around 2010

Actions such as the use of illegally copied software and illegally downloaded sites, as a result, are some of the causing circumstances whereby a system may be easily infected by the latest virus.

It is needless to say that these ship communications devices and their connected onboard PCs, navigation electronics and propulsion equipment etc. are essential when it comes to examining cyber security countermeasures. However, there seems to be little known when it comes to taking a specific approach concerning the examination of risk assessment, revisions to the SMS (Safety Management System) or SSP (Ship Security Plan).

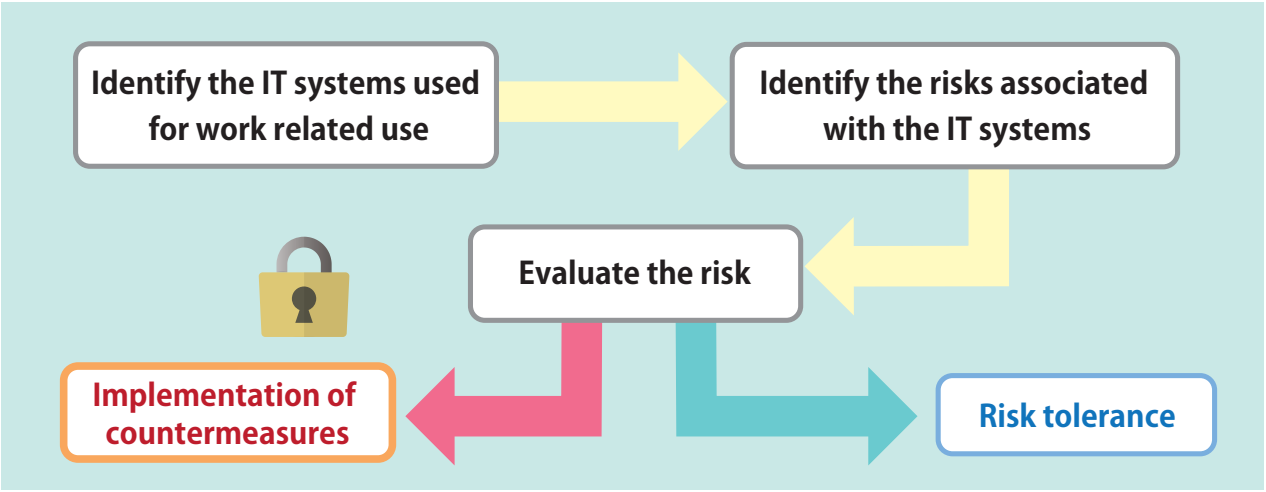
In the last part of this bulletin, we will take a look at ORCA CO., LTD., which has practical accomplishments in the shipping IT field, and introduce a SMS template that simulates the MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management, using the risk assessment approach method for cyber security countermeasures.

§3 Preparation needed to manage cyber security countermeasures

3－1 How to prevent cyber risk

Here, we would like to define cyber risk as potential factors which may cause problems or affect the IT system which may even also cause disorder in the carrying out of duties and lead to economic loss.

IT system This can be defined as anything to do with a ship's computer's software, hardware, system, equipment and appliances, namely, Information Technology.



3－2 Explanation of Class NK technical information (No. TEC-1145)

Regarding IACS, the importance of security countermeasures of a computer system are to be considered. In order to specify the requirements related to a person's role in a computer system used on board, security countermeasures of both software and hardware to be used in the computer system and the quality of management, such as the procedure of software changes etc., the Unified Requirement of IACS E22(Rev.2) was adopted in June, 2016.

Following this, a notice of revised related rules and inspection procedures in the Class NK technical information

guideline (No. TEC-1145) was issued on February 28, 2018.

In the Class NK technical information guideline (No. TEC-1145), regarding each piece of software and hardware that performs automatic control or remote control installed on board, they were classified according to the extent of influence they exert by disorder. Further, responsibilities and duties were distinguished according to shipyard, system integrator, supplier and shipowner.

Table 2.1 System categories in Annex D18.1.1, Part D of the Guidance for the Survey and Construction for Steel Ships

Category	Effects Typical	system functionality
Ⅰ	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Monitoring function for informational or administrative tasks
Ⅱ	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Alarm and monitoring functions - Control functions which are necessary to maintain the vessel in its normal operational and habitable conditions
Ⅲ	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Control functions for maintaining the vessel's propulsion and steering - Vessel safety functions

(Quoted from No. TEC-1145)

Category Ⅲ

System	Examples of detailed machinery and system
Main propulsion systems	Engine control system, Engine remote control system, Main boiler control system, CPP control system, Electric propulsion control system
Steering system control systems	Steering system, Azimuth thruster
Electric power systems	Generator engine control system, Electric power converter (for electric propulsion ship, etc.)
Safety systems	Fire detection and fighting system, Flooding detection and fighting system, Internal communication system, System involved in operation of life saving appliances equipment
Other systems	Dynamic positioning system, Drilling system

(Quoted from No. TEC-1145)

Category Ⅱ

Liquid cargo transfer control systems	Cargo control system (e.g. cargo control console, cargo valve remote control system, cargo machinery emergency shut-down system), Reliquefaction system, Inert gas generator (including nitrogen generator), Oil discharge monitoring and control system
Fuel oil treatment systems	Viscosity control system, Fuel oil purifier
Stabilization and ride control systems	Fin stabilizer, Jetfoil
Alarm and monitoring systems for propulsion systems	Engine alarm and monitoring system (including data logger)
Other systems	Ballast transfer valve remote control system, Oily water separator, Oil content meter, Waste oil incinerator, Sewage treatment plant, Aux. boiler control system, Ballast water treatment system, SOx/NOx scrubber, NOx exhaust gas recirculation system

(Quoted from No. TEC-1145)

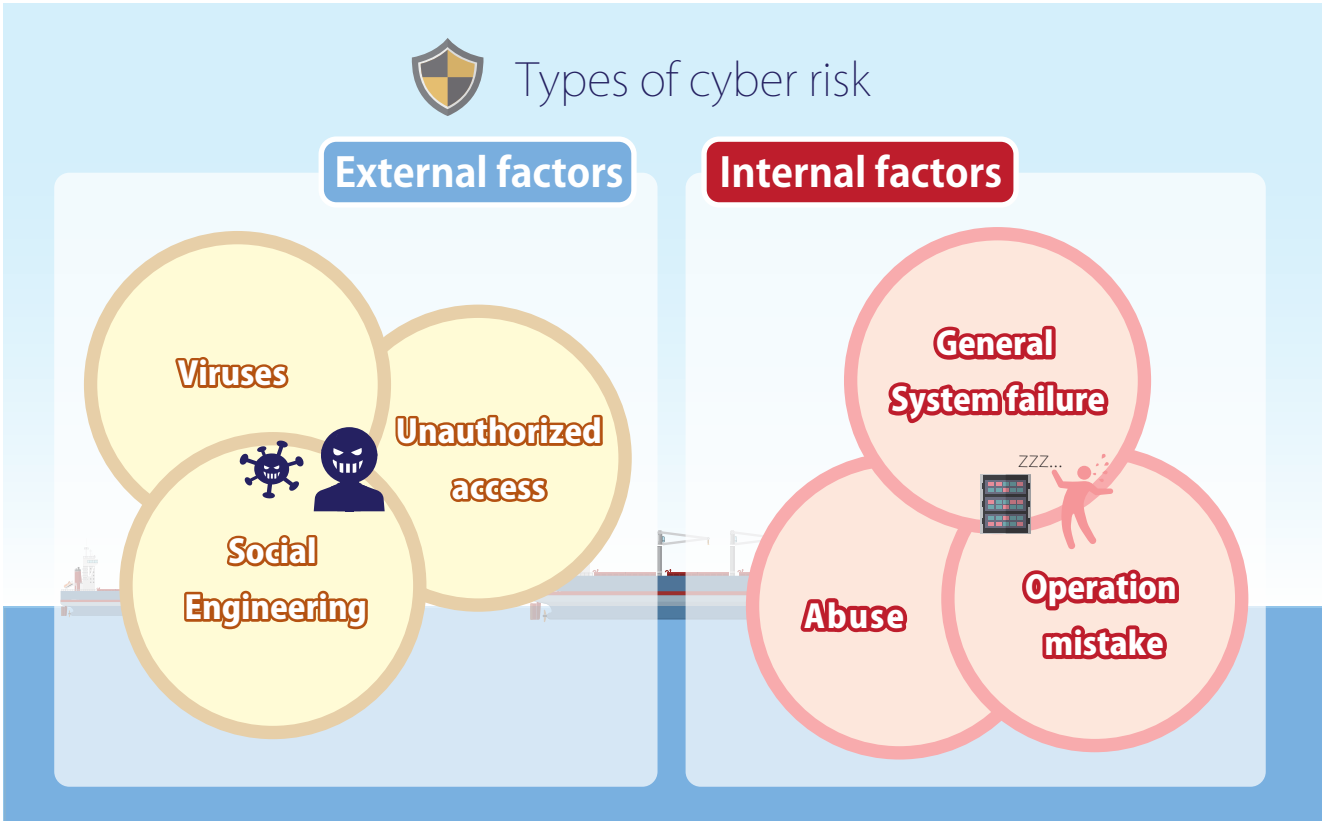
It is defined that the responsibility for cyber security countermeasures of each computer system is down to the supplier of each computer system. However, in the event of networking systems, the system integrator will be responsible because there will be new risks, which were not taken into account when operating a system as a single unit.

The role of the shipowner and ship management company is to keep receiving necessary information, such as a list of equipment that uses computers and risk assessment results etc. from the shipyard and system integrator; this is all that is required of them.

However, with respect to the revision of the SMS in the future (cyber security countermeasures), the concept "System integrator bears a certain amount of the responsibility" will play a key role. Regarding the onboard PC for duty use, loading computer, V-SAT, FBB and so on, which are classified into Class Category I, it will be necessary for a shipowner or ship management company to implement a risk assessment as a cyber security countermeasure.

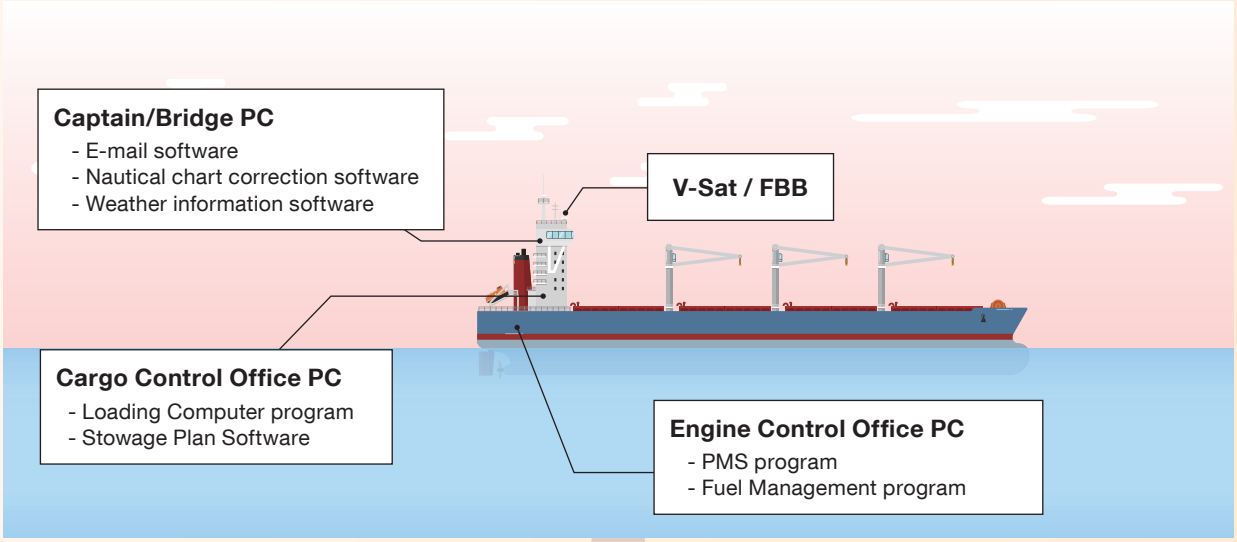
3－3　Types of cyber risk

Although external factors such as unauthorized access and system hacking are mainly the focus when it comes to cyber risk, it will be important to consider reviewing internal factors, such as the existence of operation mistakes and general system failure.



3－4 How to make a plan for cyber security countermeasures

1 To identify the IT systems After identifying the IT systems installed on the ship, list them up.



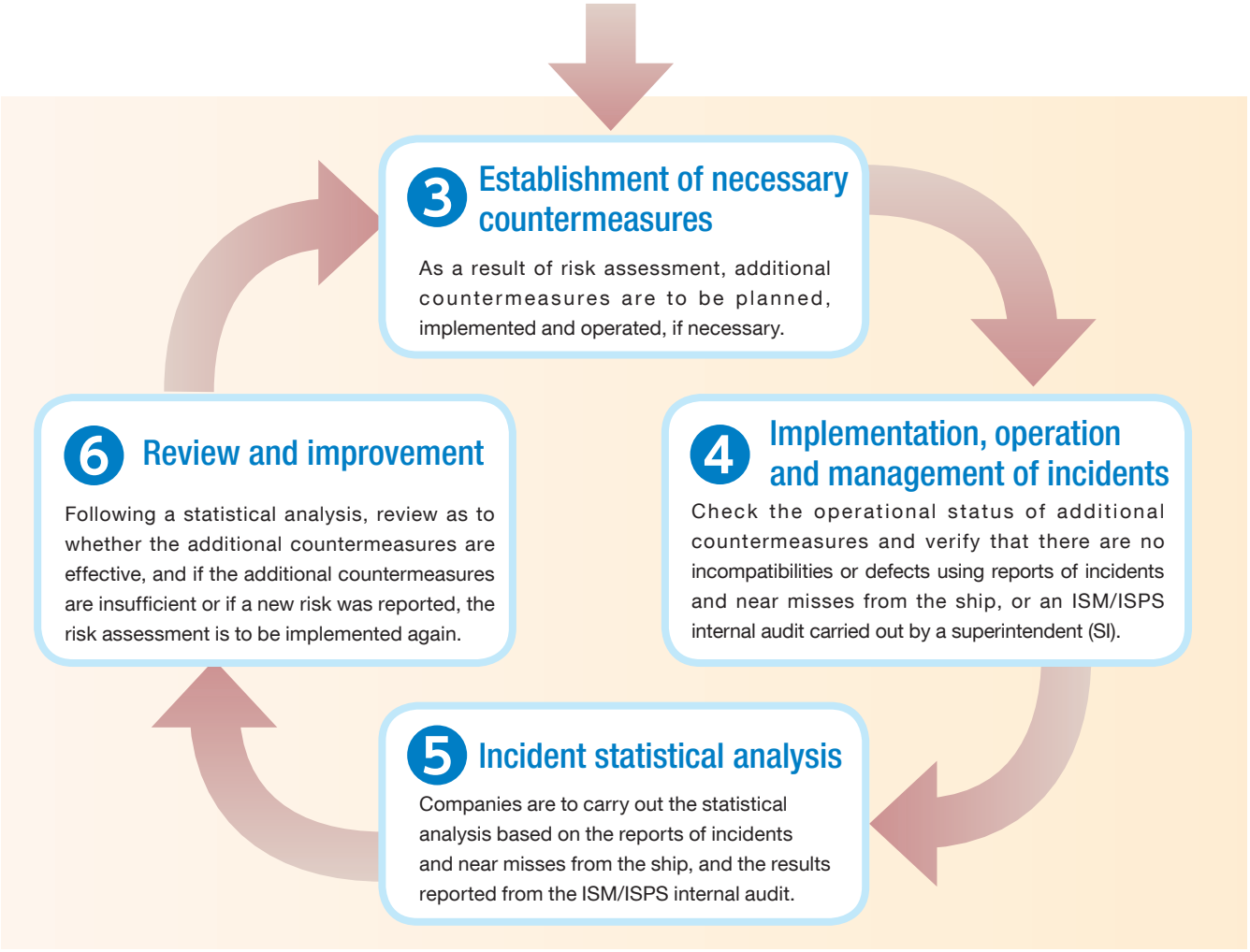
2 Implementation of risk assessment For each listed-up IT system, risk assessment is to be implemented by examining the possible outcomes of a cyber attack (damage), frequency and current management method.

Table 4 Examples of risk assessment

E-mail communication

No.	Scenario	Possibility	Frequency	Damage	Evaluation	Countermeasures	Due date
1	Malfunction of e-mail software infected by a virus from a crew member's personal USB	**Middle**	**Middle**	**Middle**	Additional countermeasure is required	① Additional SMS training ② Arrangement of a back-up PC	Dec., 2018
2	High cost of communications fee because firewall is not installed	**Middle**	**High**	**Middle**	Additional countermeasure is required	Dispatch a technician to the next port of call and install the FW and set up a filter in the FBB	Dec., 2018
3	Crew's personal PC that has been directly connected for the use of sending emails etc.	**Low**	**Low**	**Middle**	Risk tolerance	Although a certain amount of risk may be tolerated, this can be further mitigated by setting up the FBB filter	N/A
4	Malfunction of satellite and land earth station	**Low**	**Low**	**Middle**	Risk tolerance	N/A	N/A
5	Continued...						

The above is one example, because risk assessment and the SMS can differ depending on the crew structure, sea area for shipping operation, ship type and management company.



1 ····· Identify the IT systems on the ship in order to list them up.

2 3 ··· In the same way that dangerous work and hazardous areas designated on the ship are operated using the current SMS, identify the onboard IT systems and implement a risk assessment while examining the possible outcome of a cyber attack (damage), frequency of and current management method, and carry out a countermeasure, if necessary. When confronted with a cyber risk, it is also necessary to consider trends in the IT field, types and versions of systems and equipment, and so on.

4 ····· Check the operational status of additional countermeasures and verify as to whether there were no incompatibilities or defects using reports of incidents and near misses from the ship, or an ISM internal audit carried out by a SI.

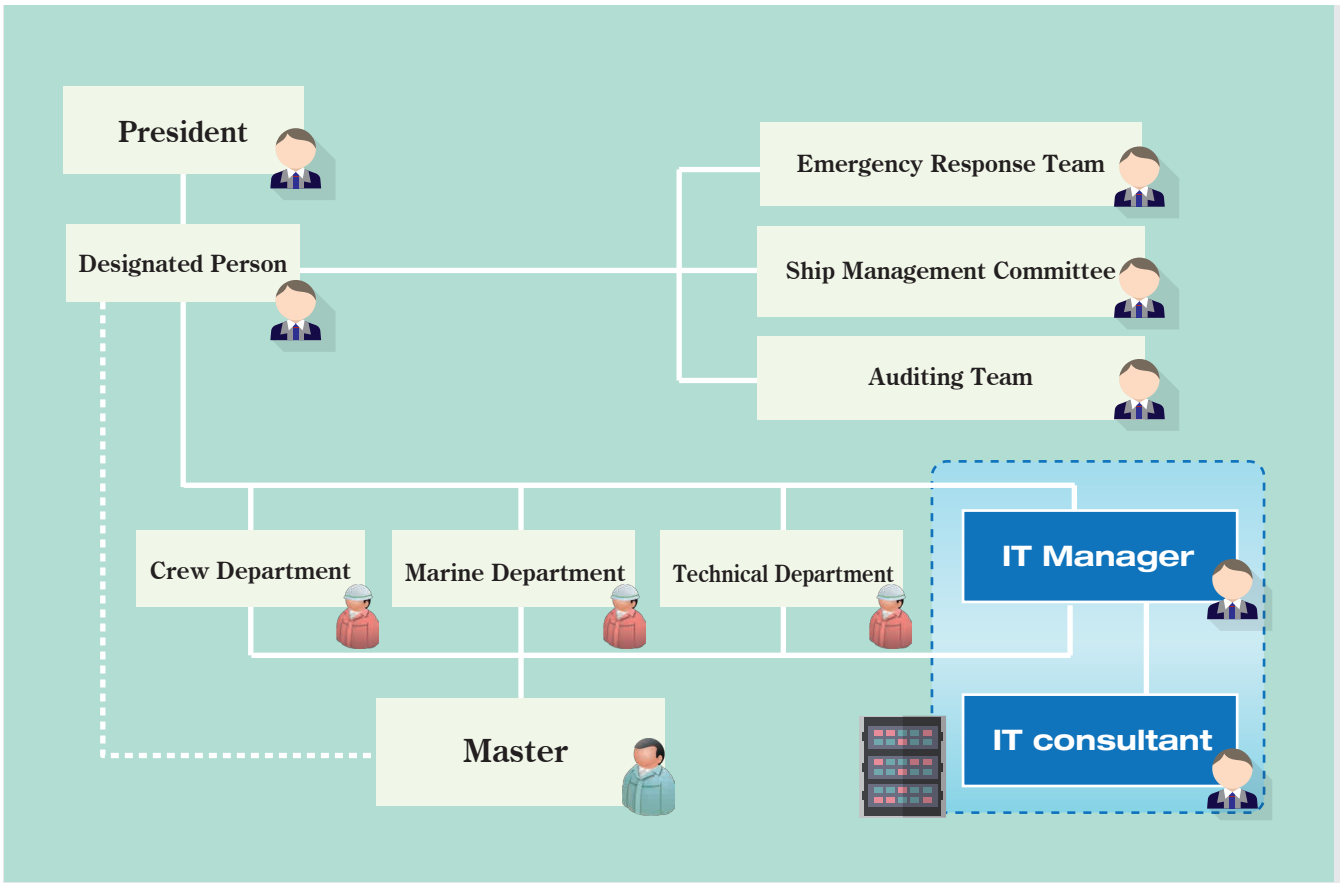
5 6 ··· Companies are to implement the statistical analysis based on the reports of incidents and near misses from the ship, and the results reported from the ISM internal audit. Following the results of the statistical analysis, review (management review) as to whether the additional countermeasures were effective, and if the additional countermeasures were insufficient or if any new risks were reported, a risk assessment is to be implemented again, in the same way that the operation would be carried out with the existing SMS, and the necessary countermeasures are to be examined.

Regarding the reporting of incidents and near misses, the following examples can be said to be occurring recently: A crew member inserted a USB memory stick which is not permitted by the company, into their work PC, or he/she downloaded non-permitted software or a programme onto the onboard PC.

In addition, in order to receive visitors (external factors of cyber risk), not dissimilar to that of the SMS, it could be necessary to review the SSP, also, as an unspecified number of visitors and dock workers will get on board, especially at the port of call, and multi-purpose offshore support vessels and research vessels carrying a large number of researchers and workers may embark.

§4 Selecting designated IT personnel

We believe that it will be desirable to appoint an IT designated person when it comes to drawing up and implementing cyber security countermeasures that can be incorporated into the SMS. In the future, when countermeasures in a state of emergency and the introduction of systems maintenance on board a ship are required, the role of the IT Manager and the importance of this role will become more essential. In addition, it will be important to have a system in place that allows for consultation to be carried out with an external ship IT system expert.



§5 Establish an IT standard in your organization

The establishment of an IT standard will allow for the smooth integration of operation and management (maintenance etc.) if your organization is managing a large fleet of ships. With an IT standard in place, it will be much easier to deal with any problems that arise, compared to not having established one.

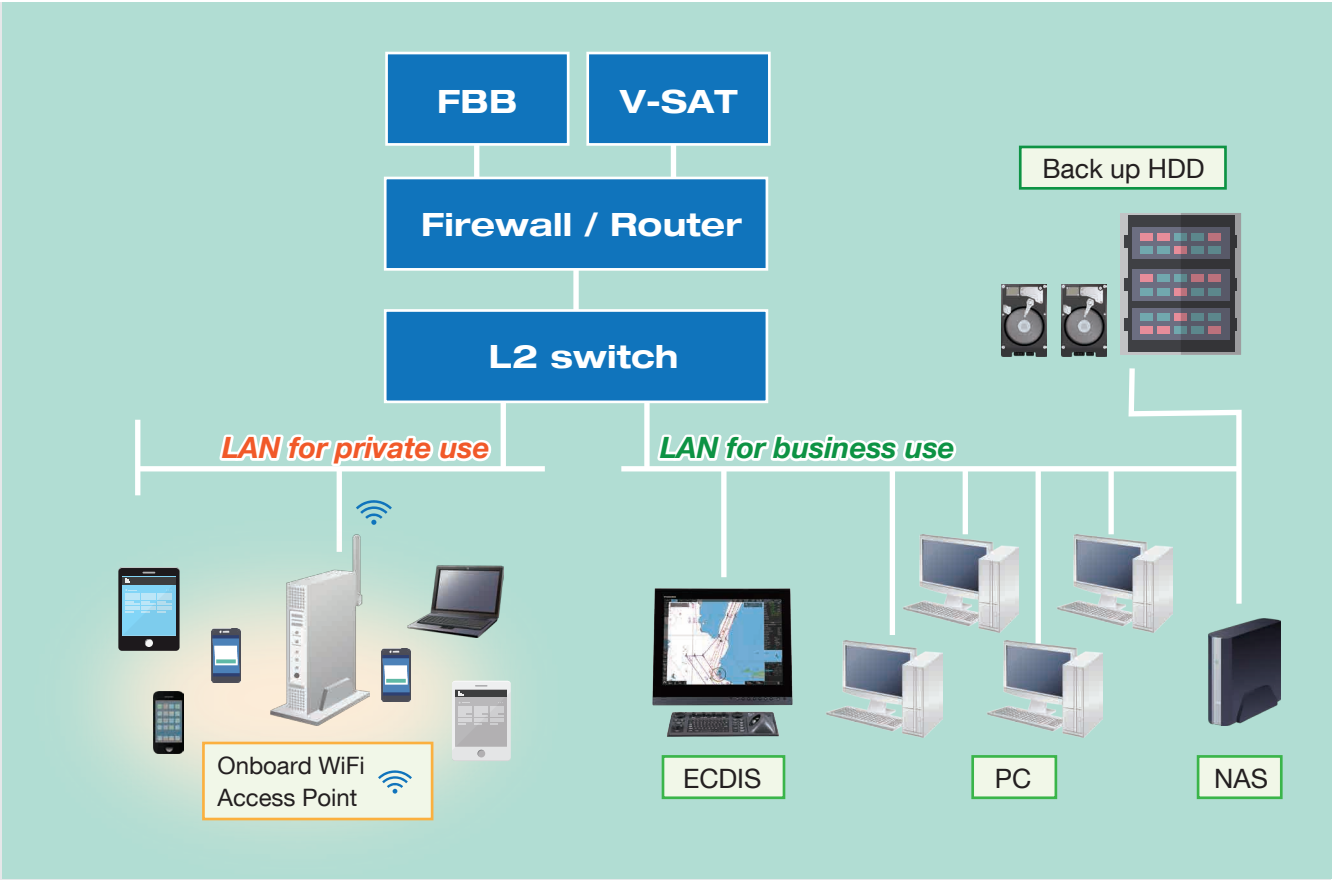


Fig. 5 Construction example of ship's LAN

It is important to organize the specification, software and purpose of each onboard PC. For reference, it will be useful if a substitute PC is available in case a PC breaks down or new software is added.

Record standard design of onboard PC!

Record for IT Standard Design

Standard type:
Date of Record:
IT Manager:
Designated Person:

This IT Standard will be value from :

I. Client PC Conditions				Remark
(1) Hardware				
	Number of PCs			
	Type (Laptop PC/Desktop PC)			
	CPU			
	Memory			
	HDD			
(2) Software	**Basic Software**			
	OS			
	MS-OFFICE (version)			
	MS-OFFICE (Applications)			
	Acrobat Reader			
	AntiVirus Software			
(3) Software	**Application Software**	**Applications**	**Suppliers**	
(4) Network Diagram	**Detail of PC setting**			
	Detail of PC setting	**(Refer to the second sheet)**		
II. Peripheral Device				
(1) Printer				
	Laser Printer			
	* Number of them			
	* Single or Multiple function			
	* Black/White or Color			
	Inkjet Printer			
	* Number of them			
	* Single or Multiple Function			
	* Black/White or Color			
(2) Scanner				
	* Number of them			
	* Flatbed/Stand			
(3) NAS set				
	* Model			
III. Network				
(1) Router				
	Type of Router			
	Supplier			
(2) Sub Network				
	Purpose of Sub Network			
(3) Wifi Access Point				
	Number of Wifi Access Point			
(4) Network Diagram				
	Network Diagram	**(Refer to the third sheet)**		

Table 6 Record for IT Standard Design

§6 Implementing an IT standard risk assessment

Regarding the IT standard (ship's LAN/onboard PC specification), risk assessment is to be implemented following the procedure that was established in the introduction of this guide “3-4 How to make a plan for cyber security countermeasures”.

Please note that systems that have already been risk assessed, IT systems that do not directly interfere with work being carried out even when a system failure occurs, stand-alone use computers etc. in Class Category II and III can be excluded from the risk assessment.

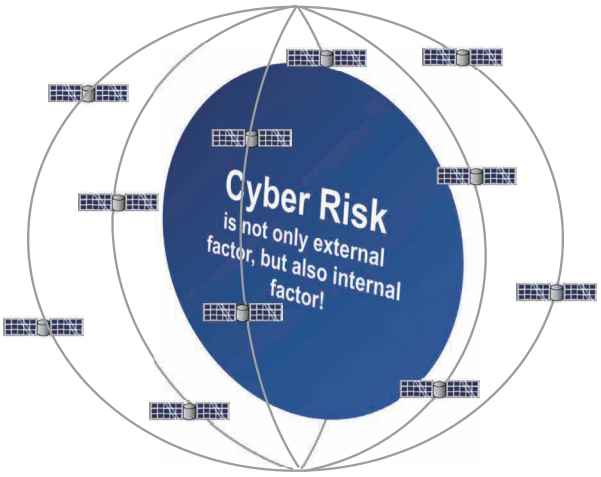
§7 SMS manual to include IT control documents

Having implemented a risk assessment and incorporation of the IT control documents into SMS manual, it is recommendable that a ship and shore joint drill that simulates a severe IT incident be implemented, even if only once. It would be a good opportunity to review as to whether the manual and instructions for cyber security countermeasures which were established in the SMS manual work effectively, and as to whether both personnel on shore and crew on the ship are familiar with the new manual and so on.

§8 Conclusion

It is hoped that if this Loss Prevention Bulletin will be put to good use and that it may assist you in your establishment of cyber security countermeasures.

<Remarks> The documents and contents in this bulletin were compiled with the co-operation of ORCA CO., LTD. (Http://www.orcajpn.co.jp/index.html).



Text and forms provided by ORCA CO., LTD.

Following test and forms are available on our Club website

Text and forms provided by ORCA CO., LTD.

Reference ICS Bridge Procedure Guide Fifth Edition

1. Regulation for the Organization of the Safety Management System MN-02-00

SMS Document No.: ORCA-MN-02-00 **Chapter: 2**
Issued by: The Designated Person **Approved by: The President**
Title: Regulation for the Organization of the Safety Management System

1. Purpose

This regulation is to define the responsibilities and authorities of Departments and personnel implementing the SMS. It also clarifies the reciprocal relationship between them in order to ensure that the Company's management activities comply with the regulations of safety operation and environmental protection.

(snipped)

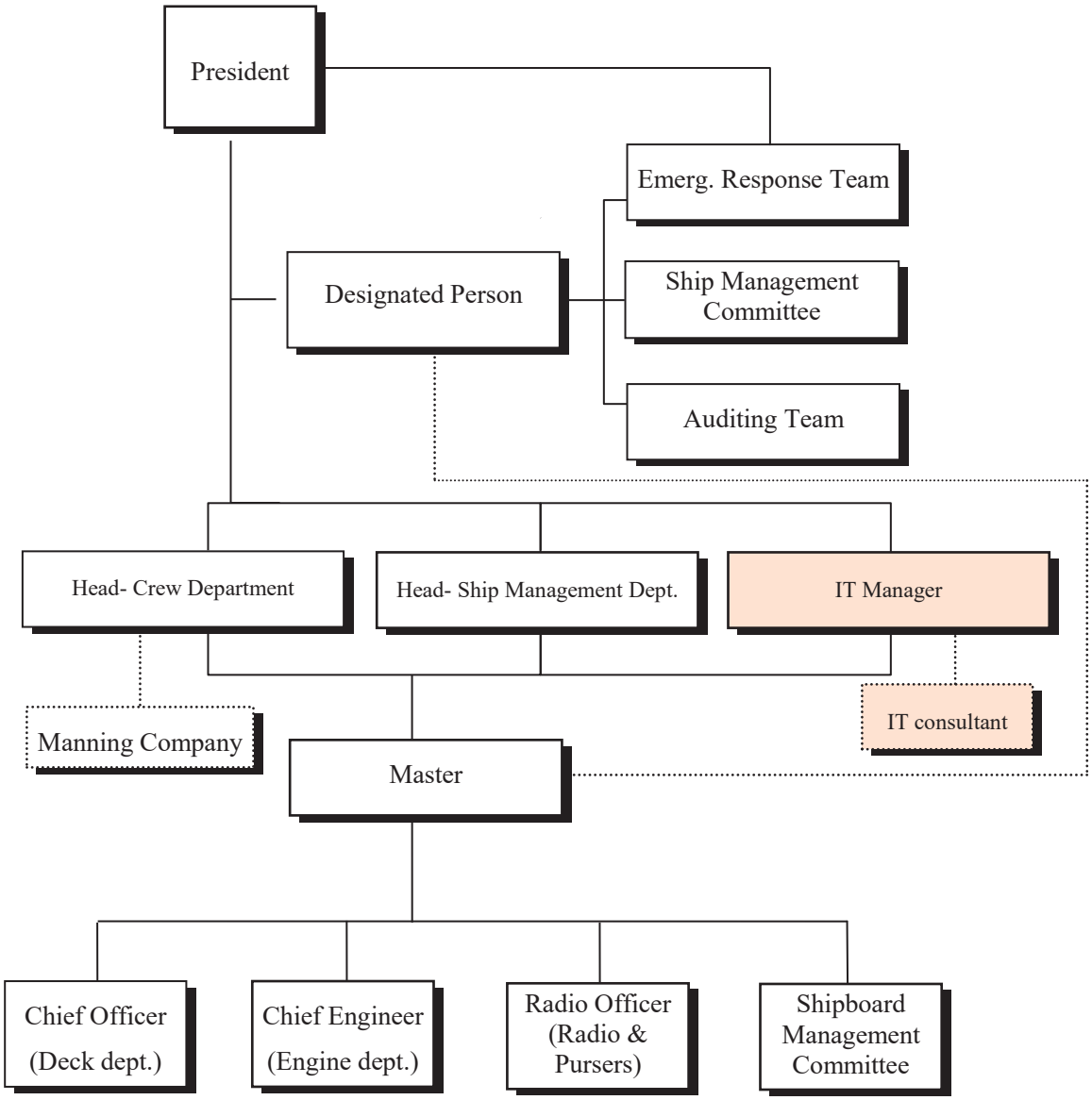
4.5 The IT Manager
4.5.1 The IT Manager is responsible for the following jobs;
(1) To ensure the proper operations of IT systems onboard ships and ashore;
(2) To watch, assess, and assist to response to IT related incidents;
(3) To proceed necessary training and education related to IT systems;
(4) To control data related to IT systems;
(5) To catch up cyber risks in IT fields;
4.5.2 The Company may contract with outside IT expert or consultant to support IT matters, if so required.

(snipped)

2. Chart of Organization for the Safety Management System MN-02-00A

ORCA-MN-02-00A
Revision: 0
Page: 1 of 1
Date: 01 Feb,2018

SMS Document No.: ORCA-MN-02-00A **Chapter: 2**
Issued by: The Designated Person **Approved by: The President**
Title: Chart of Organization for the Safety Management System



ORCA CO., LTD.

3. Regulation for management of IT systems MN-20-00

SMS Document No.: ORCA-MN-20-00 **Chapter: 20**
Issued by: The Designated Person **Approved by: The President**
Title: Regulation for management of IT systems

1. Purpose

This regulation is prepared to specify the arrangement and management of IT systems in the Company and onboard ships for the proper implementation of SMS, including to response to possible cyber risks.

2. Application

This regulation is applicable to the Company and all vessels under management of the Company.

3. Reference regulations

SOLAS XI-2
MSC-FAL-1/Circ. 3

4. Definition

4.1 IT system
"IT system" is a computer-based system used for all kind of operations. The system can be total packaged equipment or install based software for PC. Any device, equipment or services based on computer are defined as a part of "IT System".

4.2 Cyber-risk
"Cyber-risk" is a potential risk to lead operation failure of the IT systems, which will cause financial loss, disruption or damage to the reputation of an organization. Cyber-risk includes external factors (such as computer virus, Trojans, or attack over network, etc.) and internal factors (malfunction, miss-operation, or system bug, etc.).

4.3 IT incident
"IT incident" is an occurrence, which actually or potentially results in adverse consequences to IT systems, includes all deficiencies and non-conformities involving to the IT systems.

4.4 Cyber risk management

"Cyber risk management" is the process of identifying, analyzing, assessing, and communicating a cyber related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level; taking into consideration the costs and benefits taken by the Company.

5. Requirements

5.1 Design of IT standard

For a smooth and effective implementation of the SMS, the Company shall set-up an IT Standard, and, accordingly, construct IT Systems in the Company and on-board ships under management of the Company. IT Standard is to be recorded on the "Records for IT Standard Design" (ORCA-SM-07-50), and to be annually reviewed for any improvement by the IT Manager. For details, refer to the "Procedure for Management of IT Systems" (ORCA-MN-20-01).

5.2 Operation of IT systems

Under the direction of the Designated Person and the Head of the Shipmanagement Department, the IT Manager must integrate the specified IT Systems and network systems properly and supervise and direct the relevant personnel to operate IT systems in accordance with IT Standard or makers" instructions.

5.3 Identification of IT systems

5.3.1 The IT manager should identify all IT systems onboard and ashore using the "List of IT Systems" (ORCA-SM-07-51).

5.3.2 The IT manager should process the risk assessment regarding cyber-risk for each IT systems and prepare for countermeasure if so required.

5.3.3 During the risk assessment, if a part of the IT systems had already assessed in the IT standard, the part of risk assessment can be omitted.

5.3.4 In case of addition, replacement, or abolition of the IT system had been taken, the IT manager must re-process risk assessment to the part of modification.

5.4 Maintenance of IT systems

In order to ensure the proper operation of IT systems, the IT Manager shall set up a maintenance plan (on the OMPS software) for the periodic maintenance of IT systems, including its important elements as well as associated software. The maintenance plan should include the following factors:

(1) Maintenance operation designated by each IT system vender.
(2) Minor software update.
(3) Backup operation of data.
(4) Condition check of each IT systems.

Maintenance of the IT systems should be processed in reference to the "Regulation for Maintenance of Hull, Machinery and Equipment"

5.5 Hardware Replacement of IT systems

5.5.1 Due to service life, hardware of the IT systems required replacement.

5.5.2 The IT manager should plan the hardware replacement considering following factor;

(1) Recommendation of the hardware vender
(2) Condition report of the IT systems
(3) Improvement of new hardware tolerance for cyber-risk

5.5.3 Plan for replacement should include following operation;

(1) Replacement of the client PC due to deterioration
(2) Replacement of the peripherals due to deterioration
(3) Replacement of the hardware which has newer countermeasure to handle cyber-risks.
(4) Replacement of the hardware which considered being required for appropriate operation of the IT systems.

5.6 Version control for firmware or software of IT Systems.

5.6.1 The IT manager should control version tables of firmware or software of the IT systems.

5.6.2 If any update version has been released, the update should be applied as possible.

5.6.3 However, major update might affect to compatibility or connectivity among other IT systems. In this case, sufficient verification and risk assessment must be done by the IT manager before applying the update.

5.6.4 The IT manager should judge if the update is major or minor appropriately.

5.7 Handling of incidents of IT systems

5.7.1 The IT manager should handle and solve incidents in relation to the IT system onboard and ashore.

5.7.2 The IT manager should record the incidents for future analyzing, to improve tolerance for cyber-risk.

5.7.3 If the incident is considered as critical, the IT manager must report this to the Designated person according to “Regulation for emergency preparedness” .

5.7.4 After solution of the critical incident, the IT manager must proceed risk investigation for recurrence prevention.

5.7.5 The “Procedure for Cyber Risk Management” (ORCA-MN-20-02) must also be referred to.

5.8 Education and training regarding to the operation of IT systems.

5.8.1 The IT manager should ensure that all personnel involved in the Company's SMS have an adequate understanding of the IT systems and cyber-risks.

5.8.2 The IT manager should plan appropriate education or training in relation to the operation of the IT systems.

5.8.3 The education or training plan should be processed in reference to “Regulation for Education and Training” .

5.8.4 The IT manager should timely release a newly appeared cyber-risk to the relevant departments and vessels for prevention purpose.

5.9 Data Management of IT systems.

5.9.1 The IT manager should properly manage the data which is operated in the IT systems.

5.9.2 Regarding the data management, following factor should be considered;

(1) Availability the data can be used in proper timing.

(2) Integrity to prevent data loss or falsification

(3) Confidentiality the data will not be leaked to any unauthorized party.

5.9.3 The IT manager should clarify about ownership of intellectual property for the data.

5.9.4 In case of transfer of management of a ship, the IT manager should correct or delete the data in reference to “List of the IT systems” (ORCA-SM-07-51).

5.10 Monitoring of unknown cyber-risks.

5.10.1 The IT manager should try to find out new unknown cyber-risks.

5.10.2 Master or each Department of the Company must inform the IT manager for any newly identified cyber-risk.

5.11 Management review regarding to IT systems

5.11.1 The IT manager should provide following information to the safety management committee during management review;

(1) Analyze report of the IT incidents
(2) Newly found cyber-risk and risk assessment report
(3) Trend information of IT fields
(4) Update information of software and hardware.
(5) Revision plan of IT standard with risk assessment
(6) Revision plan of IT systems list with risk assessment.

5.11.2 The Designated Person should investigate this information and review the IT management in reference to "Regulation for Internal Audits and Management Reviews" (ORCA-MN-11-00).

5.12 Contract with IT consultant or IT expert

5.12.1 Operation of IT system which connected to Internet using TCP/IP, requires high knowledge and experience regarding IT.

5.12.2 In order to support the IT manager, the Company may contract with external IT consultant or IT expert.

6. Applicable procedures

Procedure for Management of IT Systems (ORCA-MN-20-01)
Procedure for Cyber Risk Management (ORCA-MN-20-02)

7. Applicable records:

The Company and the ship:

Records for IT Standard Design (ORCA-SM-07-50)
List of IT Systems (ORCA-SM-07-51)
Records for Risk Assessment of IT Systems (ORCA-SM-07-52)
Maintenance Plan for Hull, Machinery and Equipment

4. Procedure for management of IT systems MN-20-01

SMS Document No.: ORCA-MN-20-01 **Section: 20-1**
Issued by: The Designated Person **Approved by: The President**
Title: Procedure for Management of IT Systems

1. Area of application

This procedure defines the guidance for the management of IT systems onboard and ashore and apply to the Company and vessels under the management of the Company

2. References

ORCA-MN-20-00 Regulation for Management of IT systems

3. Procedure to setup IT Standard

3.1 The IT manager should design IT Standard using "Record for IT Standard Design" (ORCA-SM-07-50) to standardize the IT system integration.

3.2 In order to prevent any problem in connection of software and hardware, following factor should be verified;
(1) Compatibility
(2) Convertibility
(3) Conflict
(4) System response speed

3.3 The IT manager should prepare IT Standard for vessel and company.

3.4 The IT manager should categorize the IT system as following;

Company Category	Effects
A	Those systems, failure of which will not directly affect to commercial shipping operation.
B	Those systems, failure of which could eventually impact to commercial shipping operation.
C	Those systems, failure of which could immediately cause an impact to commercial shipping operation.

3.5 Regarding Category B and C, The IT manager should prepare a specific measure to ensure those systems working continuously.

3.6 The ship manager should also categorize the IT system defined by NK TEC-1145 as followings;

Class Category	Effects
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

3.7 The ship manager should process risk assessment regarding IT standard.

4. Procedure for risk assessment of IT SYSTEM

4.1 The IT manager should process risk assessment regarding identified risks on IT systems using the “Record for Risk Assessment of IT Systems” (ORCA-SM-07-52).

4.2 If any connection had made among multiple IT systems, risk of the connection should be also verified.

4.3 Following factors should be assessed for each risk;
(1) Possibility
(2) Frequency
(3) Damage

4.4 In conclusion of the assessment, following option should be selected;
(1) Accept the risk
(2) Measures required
(3) To be re-evaluate later

4.5 If any countermeasure required, the IT manager should plan a measure and process it with approval of the Designated Person.

4.6 As risk assessment requires highly knowledge and experience of IT, it is preferable to have an advice from IT consultant or IT expert.

5. Procedure for review of IT Standard

5.1 The IT manager should review the IT standard annually.

5.2 If any modification such as revision, addition, deletion has been made in IT standard, the IT manager must process risk assessment on such modification.

5.3 Even if no modification had been made, the IT manager still has to process risk assessment considering following factor;

(1) Change of shipping operation environment and requirement

(2) Improvement of IT technology

(3) Trend of new cyber-risks

5.4 Update of IT Standard must be submitted to the Designated Person for approval.

5.5 If update of the IT Standard had been approved, the IT manager should prepare a plan to update each IT system of vessel and shore side.

6. Preparation of IT systems in newly management vessels.

6.1 The IT manager shall refer to the IT standard and integrate IT systems onboard the ship with reference to the "Guideline for IT System Integration" (ORCA-MN-20-01A) and record the same on the "list of IT Systems" (ORCA-SM-07-51).

6.2 The IT manager should process risk assessment for each IT systems using "Record for Risk Assessment of IT Systems" (ORCA-SM-07-52).

6.3 In this assessment, if the IT system is already assessed in IT Standard, assessment of this part can be omitted.

6.4 Also, if the IT system is categorized as Category II or III in NK TEC-1145, and the system is operated as standalone, assessment of this part can be omitted. These systems should be assessed by the system vender.

6.5 The IT manager should prepare a maintenance plan including following tasks;

(1) Maintenance operation which instructed by the system vender.

(2) Minor update of software/firmware which approved by the IT manager

(3) Backup of the data

(4) Condition check

6.6 These preparations should be approved by the Designated Person.

7. Procedure for handling of IT systems by the termination of vessel management.

7.1 The IT manager should correct or delete the data of every IT systems onboard, referring “List of IT Systems” (ORCA-SM-07-51).

8. Procedure for modification of IT system

8.1 In case of IT system modification such as addition, replacement, or abolition is planned, the IT manager should verify following factors;
(1) Compatibility
(2) Convertibility
(3) Conflict

8.2 The IT manager should also process risk assessment for the new connection of IT systems.

8.3 If any risk or problem has been found the IT manager should prepare a countermeasure to operate new system integration or postpone the modification.

8.4 The conclusion should be approved by the Designated Person.

9. Procedure for handling IT incident

9.1 The IT manager should handle IT incident occurred both onboard and ashore.

9.2 In case of following situation, the IT manager must report the occurrence to the Designated Person as critical incident.
(1) The incident can directly affect to the vessel’s safety navigation.
(2) Or, the incident can lead to commercial damage to outside of the company.
(3) Or, delay of the solution may lead to situation (1) or (2).

9.3 In case of critical incident, the Designated Person must setup Emergency Response Team to handle the situation in reference of “Regulation of Emergency Preparedness” (ORCA-MN-10-00).

9.4 The Designated Person can contact IT consultant or IT expert for advice, if so required.

9.5 The “Procedure for Cyber Risk Management” (ORCA-MN-20-02) must also to be referred to.

10. Relevant forms and information

Guideline for IT System Integration (ORCA-MN-20-01A)
Procedure for Cyber Risk Management (ORCA-MN-20-02)

Records for IT Standard Design (ORCA-SM-07-50)
List of IT Systems (ORCA-SM-07-51)
Records for Risk Assessment of IT Systems (ORCA-SM-07-52)
Maintenance Plan for Hull, Machinery and Equipment (the OMPS)

5. Guideline for IT system integration MN-20-01A

Appendix
Guideline for IT system integration

Client PC

(1) Following points should be considered for selection of client PC model.
  (a) Sufficient CPU power, memory, HDD space to operate the IT systems. Especially, security software requires these resources.
  (b) PC model which has enough reliability to operate onboard.

(2) Language model might affect to the IT systems. The IT manager must verify it if PCs are supplied from different countries.

OS

(1) In order to apply necessary security update, “auto update function” should be ON as possible.

(2) However, major updating of OS might affect to the other IT systems or peripherals. If the IT manager decides to update the OS’s version, sufficient verification and risk assessment must be taken.

Basic software

(1) “Basic software” is software which acts as system requirements of each IT systems, such as MS-Office, PDF reader, etc.

(2) Major update of basic software might affect to related IT systems. So if the IT manager decides to update the version of basic software, sufficient verification and risk assessment must be taken.

Application software

(1) All application software should be verified in IT standard environment by the IT manager before installation.

(2) If the application software has a communication function, detail of the function (communication port, destination IP, etc.) must be clarified. If communication detail of the software is not disclosed, the software shall not be adopted.

(3) Application software might have conflict to the other applications. In order to prevent conflicts, the IT manager must proceed sufficient verification before adoption.

Anti-virus software

(1) Anti-virus software (or any kind of security software) must be installed to all operational official PCs.
(2) The IT manager should prepare an appropriate method to update definition files (or pattern files) to keep Anti-virus software operational.
(3) Especially, in the vessel which has an ability to access to the Internet in the ocean, "online updating function" is required.

Communication infrastructure

(1) In order to ensure communication reliability, it is preferred to have more than two different kinds of communication infrastructure.
(2) The IT systems onboard are preferred to operate as "Open system" which will not be affected by any specific communication infrastructure. The IT systems onboard should be independent from communication.
(3) To control the latest cyber-risks, maintaining the version of OS and applications by auto is very crucial. If the vessel has no ability to apply "auto updating" via satellite, shore side communication such as 4G should be adapted.

Vessel Local Network (LAN)

(1) Vessel LAN should be designed to suit each IT systems can be operate appropriately.
(2) Vessel LAN can be separated to multiple sub-network to control packet traffics.
(3) Following IT systems are preferred to be separated into sub-network due to their traffic volume.
    (a) Internet connection for crew welfare
    (b) CCD monitoring camera system
(4) For any IT system identified its importance, the system should be placed into independent sub-network to ensure traffic reliability.
(5) For crew welfare network, it is preferred to have Wi-Fi access points. So, crew can connect his private device to them. In order to avoid network conflict, Ethernet connection should not be provided to crew network.

Peripheral equipment

(1) The IT manager must clarify the detail of communication function of all LAN connected peripheral equipment on board (port, destination IP, etc.). If the

communication details are not disclosed, the equipment shall not be adopted.

Crew private device and private internet connection

(1) Most of cyber-risks are coming from crew private device and private connection such as “rental 4G in port”.

(2) To bring this kind of situation under control, the IT manager must prepare appropriate countermeasure such as;

  (a) Train and educate crew to have adequate IT literacy.

  (b) Identify the difference of management policy between official IT systems and private devices.

  (c) Prepare specific method to block this kind of cyber-risks which come from crew private devices and Internet connections.

(3) One of the better solutions is to supply controlled Internet connection for crew officially. Then, IT manager can arrange appropriate filters and sub-network settings to prevent this kind of cyber-risks.

SNS or private E-mail access

(1) SNS or private E-mail access of crew might have security-risks.

(2) The IT manager should identify which onboard-information should be secured.

(3) The IT manager should train the crew for handling of secured information.

License compliance

(1) The IT manager must ensure that all software and hardware have appropriate license.

(2) In order to avoid unknown cyber risks, following systems are prohibited.

  (a) Illegal copy

  (b) Pirated edition

  (c) A hardware which have unauthorized modification.

  (d) Any illegal network devices.

Network router

(1) It is preferred to have a network router independent from communication infrastructure. So, the vessel LAN can be operated without dependency.

(2) Network router should have an ability to switch multiple communication infrastructures.

(3) Network router should have a function to control internal network traffic.
(4) In order to avoid un-controlled traffic or cyber-attack from outside, un-necessary port must be closed in filter settings.

ORCA CO., LTD.

6. Procedure for Cyber Risk Management MN-20-02

SMS Document No.: ORCA-MN-20-02 **Section: 20-2**
Issued by: The Designated Person **Approved by: The President**
Title: Procedure for Cyber Risk Management

1. Area of application

This procedure defines the guidance for taking necessary measures to response to cyber security incidents of IT systems apply to the Company and all ships under the management of the Company.

2. References

ORCA-MN-20-00 Regulation for Management of IT systems

3. Authorities and responsibilities

3.1 The Head of the Shipmanagement Department, under the direction of the Designated Person, is responsible for cyber risks management, including IT systems, onboard ships and the shore-based Company.

3.2 The IT Manager is responsible for the smooth operation of IT systems and, supervise, monitoring, and timely response to cyber incidents.

3.3 The Master onboard is responsible for the smooth operation of IT systems and, supervise, monitoring, and report any deficiency, non-conformity or cyber incident to the Company in accordance with the “Procedure for Management of Deficiencies and Non-conformities” (ORCA-MN-13-01).

4. Procedure

4.1 Identify threats- The IT Manager, under the direction of the Head of the Shipmanagement Department, and the Designated Person, is to take measures to make all relevant personnel understand the external cyber security threats to the ship and the Company and to understand the internal cyber security threat posed by inappropriate use and lack of awareness.

4..2 Identify vulnerability- The IT Manager is to develop inventories the Company and shipboard systems with direct or indirect communication links with referring to the “List of IT Systems” (ORCA-SM-07-51) and understand the consequences of a cyber security threat on these systems also understand the capabilities and limitations of existing protection measures.

4..3 Assess risk exposure- The IT Manager is to assess and determine the likelihood of vulnerabilities being exploited by external threats, by inappropriate use, and the security and safety impact of any individual or combination of vulnerabilities being exploited. The form “Records for Risk Assessment of IT Systems” (ORCA-SM-07-52) is to be applied.

4.4 Develop protection and detection measures- The IT Manager, under the direction of the Head of the Shipmanagement Department, and the Designated Person, is to take measures to the likelihood of vulnerabilities being exploited through protection measures also to reduce the potential impact of a vulnerability being exploited.

4.5 Establish contingency plans- The IT Manager shall develop a response plan to reduce the impact of the treats under the approval and direction by the Designated person in accordance with the “Procedure for Management of Deficiencies and Non-conformities” (ORCA-MN-13-01).

4.6 Response to and recover from cyber security incidents- After recover cyber security incidents by using the response plan, the IT Manager shall assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

4.7 Investigating cyber incidents- The IT Manager, under the direction of the Head of the Shipmanagement Department, and the Designated Person, is to investigate cyber incidents in order to archive a better understanding of the potential cyber risks, identification of lessons learned also updates to technical and procedural measures to prevent a recurrence.

4.8 Response to cyber incidents of IT systems - The IT manager shall assess its vulnerability and impact and give a response in accordance with the “Procedure for Management of Deficiencies and Non-conformities” (ORCA-MN-13-01), and coordinate with the makers of the operational technology system to ensure its safety and security.

5. Relevant forms and information

Records for IT Standard Design (ORCA-SM-07-50)
List of IT Systems (ORCA-SM-07-51)
Records for Risk Assessment of IT Systems (ORCA-SM-07-52)

7. Record for IT Standard design SM0750

Record for IT Standard Design

Standard type:
Date of Record:
IT Manager:
Designated Person:

This IT Standard will be value from :

I. Client PC Conditions				Remark
(1) Hardware				
	Number of PCs			
	Type (Laptop PC/Desktop PC)			
	CPU			
	Memory			
	HDD			
(2) Software	**Basic Software**			
	OS			
	MS-OFFICE (version)			
	MS-OFFICE (Applications)			
	Acrobat Reader			
	AntiVirus Software			
(3) Software	**Application Software**	**Applications**	**Suppliers**	
(4) Network Diagram	**Detail of PC setting**			
	Detail of PC setting	**(Refer to the second sheet)**		
II. Peripheral Device				
(1) Printer				
	Laser Printer			
	* Number of them			
	* Single or Multiple function			
	* Black/White or Color			
	Inkjet Printer			
	* Number of them			
	* Single or Multiple Function			
	* Black/White or Color			
(2) Scanner				
	* Number of them			
	* Flatbed/Stand			
(3) NAS set				
	* Model			
III. Network				
(1) Router				
	Type of Router			
	Supplier			
(2) Sub Network				
	Purpose of Sub Network			
(3) Wifi Access Point				
	Number of Wifi Access Point			
(4) Network Diagram				
	Network Diagram	**(Refer to the third sheet)**		

PC setting detail

	PC01	PC02	PC03	PC04	PC05	PC06
Location or Main Usage						
Location(Bridge, Master, etc.)						
Type (Desktop, Laptop)						
Main Usage(Mail, SMS-MAIN, SMS-SUB, Office Work)						
E-mail Function(MAIN/SUB/NO)						
Use LAN? (Y/N)						
Softwares						
ORCA SMS SYSTEM(MAIN/SUB/StandAlone/NO)						
MS-OFFICE						
Peripherals						
Laser Printer						
Single or Multipul function, B/W or Color						
Inkjet Printer						
Single or Multipul function, B/W or Color						
Scanner install						
Install Driver/standard soft/quality adjust						
Printer						
Scanner						

Network Diagram Plan

(Free Form)

Vessel Computer Systems List

Vessel Name: _____

Date Report: _____

Reported by: _____ Designated Person _____

1. Application Software

Category		System Name	Supplier	Version		Data			Remark
Class	Company			No.	Update	Property	Backup	Action	

2. Network

Category		System Name	Supplier	Version		Data			Remark
Class	Company			No.	Update	Property	Backup	Action	

3. Navigational Equipment

Category		System Name	Supplier	Version		Data			Remark
Class	Company			No.	Update	Property	Backup	Action	

Vessel IT Risk Assessment Report

Vessel Name _____

Date Report _____

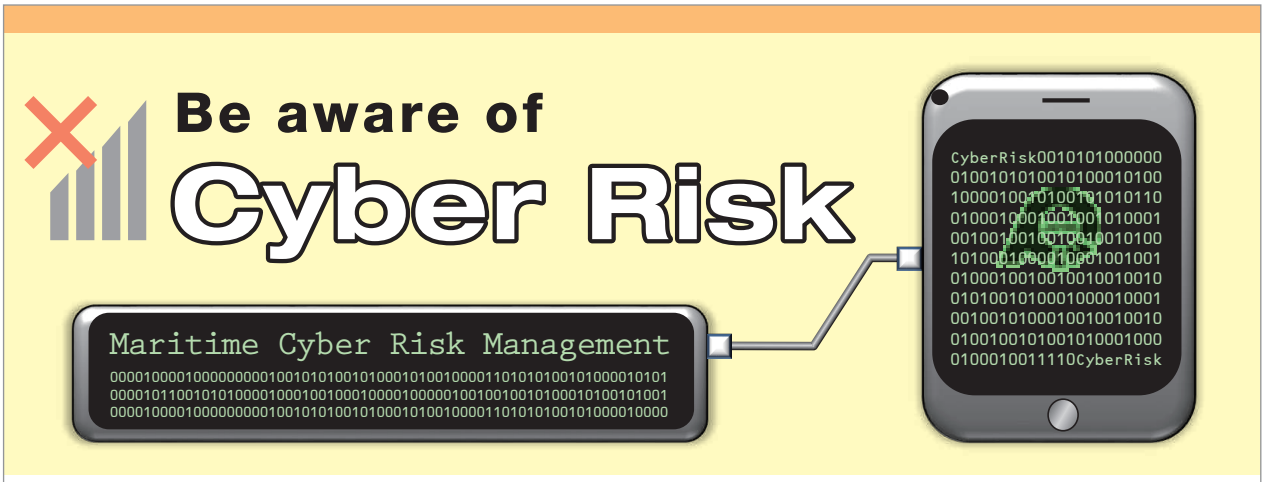
Report by _____ Designated Person _____

ISSUE								
Date Found	Description	Assessment			Evaluation	Countermeasures	Due Date	Status
		Possibility	Frequency	Damage				

ISSUE								
Date Found	Description	Assessment			Evaluation	Countermeasures	Due Date	Status
		Possibility	Frequency	Damage				

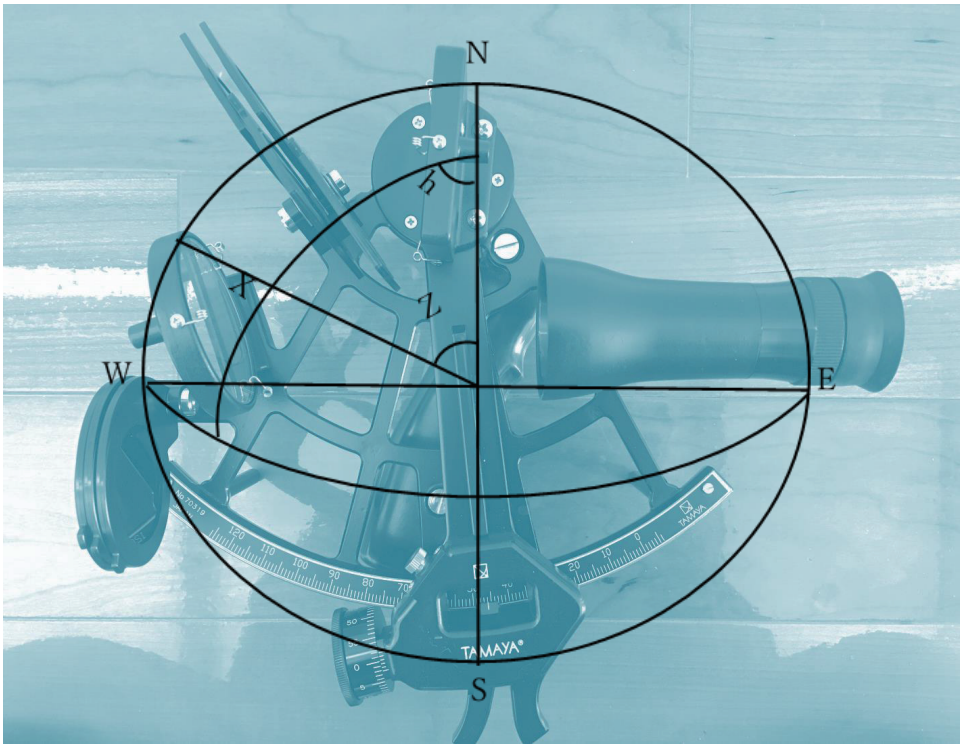
ISSUE								
Date Found	Description	Assessment			Evaluation	Countermeasures	Date Start	Status
		Possibility	Frequency	Damage				

◆ Our club's original poster



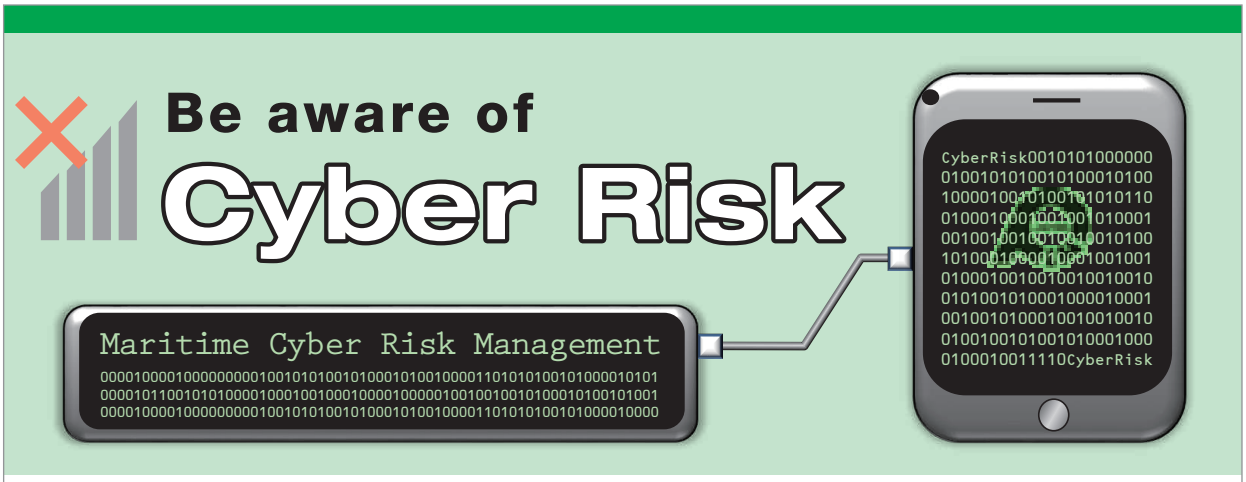
Remember Celestial Navigation?

In case of GPS (Global Positioning System) failure under navigation with ECDIS, are you able to navigate by Celestial Navigation?



Over reliance on ECDIS should be avoided particularly if detrimental to the keeping of a proper look-out

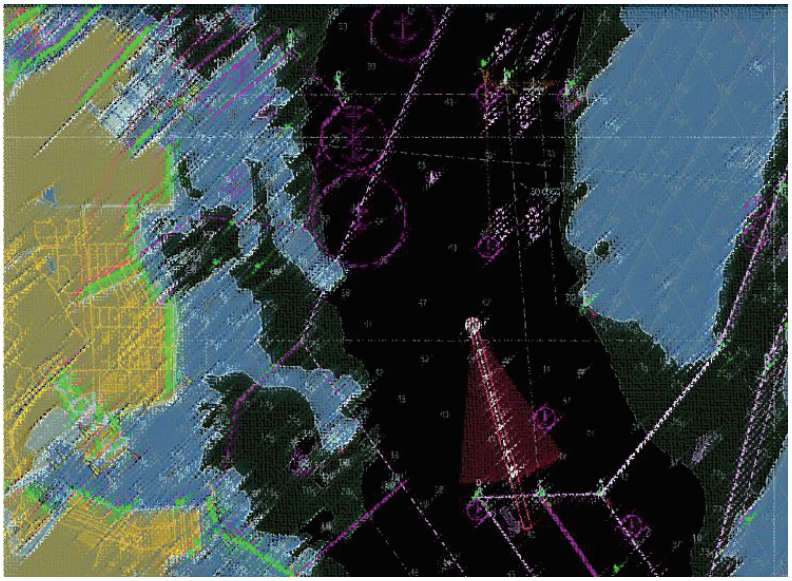
JAPAN P&I CLUB



Is your GPS position data of ECDIS truly correct?

All deck officers should be aware of importance of that;

- there's a possibility that GPS data does not tell the correct position due to jamming devices.
- periodical check of cross track (XT) by visual, radar and radar overlay on ECDIS.
- re-check your Bridge Procedure.



ICS Bridge Procedure Guide say; ECDIS is an aid to safe navigation. ECDIS does not conduct safe navigation or relieve the Master or OOW of their responsibilities for conducting safe navigation.

To be posted on Bridge

JAPAN P&I CLUB

Crew is not a System Integrator, is it?

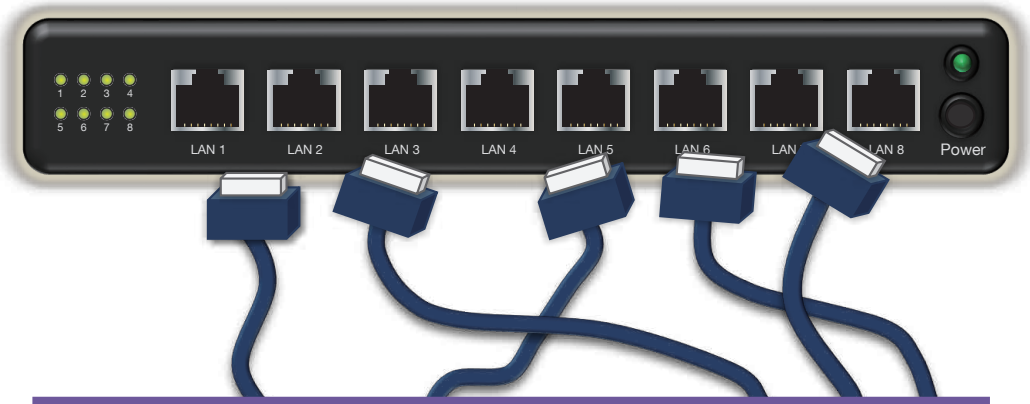
Exchanging of LAN cables by onboard crew without owner's permission, caused **malfunction** of onboard computer based systems.

malfunction

IACS UR E22(Rev.1) specifies requirements related to composition and function of computer based systems used for machinery systems such as monitoring systems.

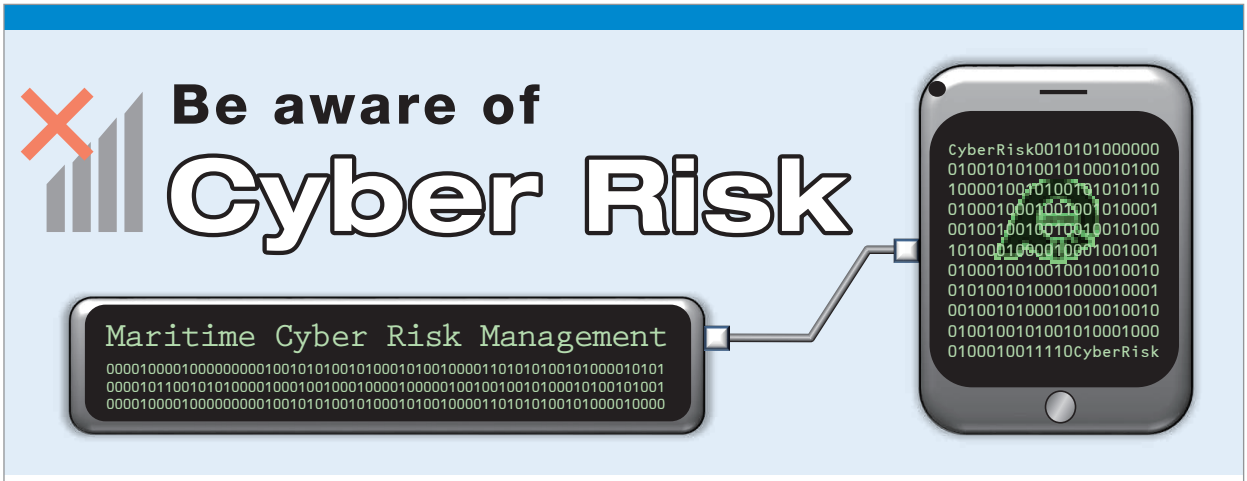
3.3.2 Change management

The owner shall ensure that necessary procedures for software and hardware change management exist on board, and that any software modification/upgrade are performed according to the procedure. All changes to computer based systems in the operational phase shall be recorded and be traceable.



All crew and visitors onboard shall strictly follow the system security procedure.

JAPAN P&I CLUB



Do (U)you (S)can and (B)lock your ship's PC ?

U Used only by authorised persons, in conjunction with the periodical update of anti-virus software.

S Scan devices is to be activated whenever a USB is used.

B Block ship's PC access at port and consider the risks involved when using a USB.

- **It is a common root cause of infection of virus ship's PCs by USB connection.**
- **All crew members should be fully aware of the risk.**

To be posted on Public space, Bridge, Officers Office, Engine Control Room

JAPAN P&I CLUB

The author

Takehiko Hino / Manager

Loss Prevention and Ship Inspection Dept.

The Japan Ship Owners' Mutual Protection & Indemnity Association

JAPAN P&I CLUB
日本船主責任相互保険組合

Website http://www.piclub.or.jp

● Principal Office（Tokyo） 2-15-14, Nihonbashi-Ningyocho Chuoh-ku, Tokyo 103-0013, Japan
Tel：03-3662-7229 Fax：03-3662-7107

● Kobe Branch 6th Floor Shosen-Mitsui Bldg. 5, Kaigandori Chuoh-ku, Kobe, Hyogo 650-0024, Japan
Tel：078-321-6886 Fax：078-332-6519

● Fukuoka Branch 6th Floor Meiji-Dori Business Center 1-1, Shimokawabata-machi, Hakata-ku, Fukuoka 812-0027, Japan
Tel：092-272-1215 Fax：092-281-3317

● Imabari Branch 2-2-1, Kitahorai-cho, Imabari, Ehime 794-0028, Japan
Tel：0898-33-1117 Fax：0898-33-1251

● Singapore Branch 80 Robinson Road #14-01B SINGAPORE 068898
Tel：65-6224-6451 Fax：65-6224-1476

● Japan P&I Club (UK) Services Ltd 5th Floor, 38 Lombard Street, London EC3V 9BS U.K.
Tel：44-20-7929-3633 Fax：44-20-7929-7557