ISM
Cyber Security

Berufsgenossenschaft Verkehrswirtschaft Post-Logistik Telekommunikation
Dienststelle Schiffssicherheit

BSH - Bundesamt für Seeschifffahrt und Hydrographie

Co-Editors:

Hamburg, August 2020

Legal note

Editor:
Deutsche Flagge

German Social Accident Insurance Institution for Commercial Transport, Postal Logistics and Telecommunication (BG Verkehr)
Ship Safety Division
Brandstwiete 1
20457 Hamburg
Internet: https://www.deutsche-flagge.de

Federal Maritime and Hydrographic Agency (BSH)
Postfach 30 12 20
20359 Hamburg
Internet: https://www.deutsche-flagge.de

Co-Editor:
Federal Office for Information Security (BSI)
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Content

Introduction

Modules

Appendices

I BSI IT-Grundschutz Profiles
II Glossary
III Rules & Guidelines
IV Owners-Masters

Hamburg, August 2020

Introduction

Increasing digitization, intensified interactivity, an increasing degree of interconnectedness of networks and progressively less and less network boundaries on board of ships provide added potential for threats by internal and external cyber risks.

Third parties as well as crew members can intentionally or unintentionally introduce malware to an interconnected and unprotected IT/OT-system. Technical failures and an accompanying exposure of the ship operations would be a potential consequence.

In crisis areas, GNSS signals (e.g. GPS) may be disturbed in a way that makes them inoperable on board.

If the ship remains unprotected, the hazard can increase exponentially.

It is necessary to support the operation of the ship with individual measures and a Cyber Risk Management (CRM).

The information listed in this document is based on Circular 04/2018 (ISM), has a recommendatory character and describes approaches for creating a Cyber Risk Management System for integration into the company's existing SMS. The document also shows the interfaces to

- the BSI IT-Grundschutz,
- the ISPS Code

and is intended to provide support for a holistic maritime Cyber Risk Management.

This circular is not intended to be exhaustive and is not an interpretation of international or national rules.

Cyber Risk Management

According to IMO Resolution MSC.428(98), cyber risks must be addressed appropriately in the Safety Management System (**SMS**) at the latest from the first annual verification of the **ISM DOC** after **1 January 2021**. For this, the IMO GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/Circ.3) have to be considered.

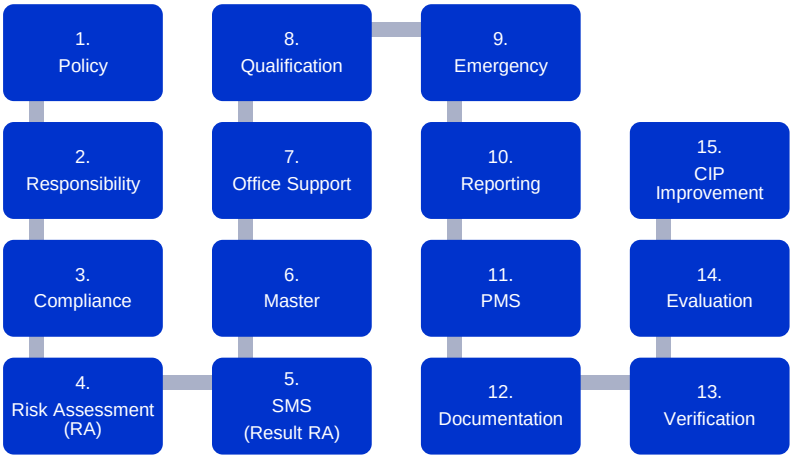
ISM Code

The ultimate aim of all measures to be taken is to ensure safe operation of the ship and pollution prevention in all circumstances.

The ISM Code stipulates required measures for the safety management of a ship. Since the Code has a modular structure, safety measures that have become necessary due to cyber threats can be integrated into the existing ISM Safety Management System (SMS) of the shipping company, or they can be described in a self-developed Information Security Management System (ISMS) in reference to the ISM SMS. In any case, the IMO requirements must be considered.

Process

Following the elements of the ISM Code, the content of the modules below are to be considered appropriately when developing a management system.



Application notes

The following pages tabulate the ISM modules (the information is non-binding.):

Description	Possible measures	Reference to
The requirement	▪ [measure 1] ▪ [measure 2]	ISM ISPS BSI

ISM — Reference to elements of the ISM Code

ISPS — Reference to chapters of the ISPS Code or notes relating to ISPS

BSI — Reference to BSI IT-Grundschutz or the IT-Grundschutz profiles for shipping companies

BSI IT-Grundschutz

The IT-Grundschutz of the Federal Office for Information Security (BSI) is a proven methodology for more than 25 years to increase the level of information security in institutions of all sizes. Its compatibility in the standard assurance with ISO 27001 has earned it international recognition. The modular and structured approach enables a tailored entry into the security process:

- **BSI-Standards:** The BSI Standard 200-1 defines general requirements for an information security management system (ISMS). With the help of the BSI Standard 200-2 on IT-Grundschutz methodology, this can be built up solidly. The BSI Standard 200-3 on risk management includes all risk-related work steps for the implementation of IT-Grundschutz.

- **IT-Grundschutz Compendium:** The IT-Grundschutz modules offer concrete requirements for about 100 top topics of information security. They already contain risk analyses for almost 50 potential threats. The Basic Requirements, together with the Standard Requirements, reflect the state of the art and are continuously developed further by the BSI.

The modules in the IT-Grundschutz Compendium are divided into process and system modules, each of which is subdivided into a total of 10 layers. In this document, a reference is made in particular to modules from the following layers:

- ISMS (Basis for all further activities in the security process)
- ORP (Organisation and personnel safety aspects)
- CON (Concepts and Approaches)
- DER (Detection and Reaction)

In addition, the use of the two "IT-Grundschutz Profiles for shipping companies", shore operation (2018) and ship operation (early 2020) is recommended. They were developed within the scope of the cooperation between the Verein Hanseatischer Transportversicherer (VHT) and the BSI. Within the framework of a structural analysis, experts from the shipping sector identified which processes in their view are particularly in need of protection. Based on these processes, the relevant modules from the IT-Grundschutz Compendium were determined. This resulted in a model security concept for shipping companies which can help to meet the requirements of the IMO.

ISPS Code

This document refers to provisions of the ISPS Code. This is because SOLAS Chapter XI-2 and the ISPS Code contain requirements for handling "security related incidents" (SOLAS XI-2/1.1.13). According to the relevant IMO requirements regarding Cyber Risk Management (MSC-FAL.1/Circ.3, Resolution MSC.428(98)), these include incidents that have a digital origin.

A Ship Security Assessment (SSA) required by Section 8 ISPS/A should also cover radio and telecommunication systems, including computer systems and networks (Section 8.3.5 ISPS/B). This requirement is binding for EU Member States in accordance with Section 8.3.5 ISPS/B in conjunction with Article 3(5) of Regulation (EC) No. 725/2004. The flag state administrations of the EU Member States must ensure that this requirement is implemented. This means that a SSA, which forms the basis for the Ship Security Plan (SSP), must also cover cyber risks.

The following options are available for the sensible implementation of this requirement:

1. cyber risks shall be considered in the SSA for the SSP in accordance with section 8 ISPS/A

or

2. the risk assessment to be prepared within the framework of the Safety Management System (SMS) or the relevant aspects of cyber risks shall be submitted to the BSH as the competent "ISPS authority" together with the SSP to be approved. This requires that the contents of Section 8 ISPS/A are covered in that risk assessment.

The basis for the SSP is the assessment of the cyber risks according to the ISPS Code. The SSP shall address the measures resulting from that risk assessment. Depending on the measure, it can either be anchored directly within the SSP or a reference to the SMS may be used. The symbol (ISPS) in the modules section helps to identify where the provisions of the ISPS Code must be observed with regard to cyber risks.

Modules

1. Policy

Cyber Risk Management (CRM) is an issue that involves the company's top management directly. The top management recognizes the fundamental risks of cyber threats for the operation of the ship and expands the management goals by incorporating the issue of information security (IT & OT).

- Expand policy to include cyber risk aspects

2.1
ISMS.1

2. Responsibility

The ultimate responsibility for the CRM on board the ships of a company lies with its top management. It can – depending on the structure and size of the shipping company – delegate responsibility and tasks.
All persons assigned to CRM tasks are recorded in the SMS.

- Delegate responsibility from company management to responsible person
- Designate responsible person(s)
- Update task descriptions and ways of communication in the SMS (e.g. job description and organizational structure)

3.2
ISMS.1

3. Compliance

Legal registers list applicable rules and recommendations, e.g. by the IMO, flag state administrations, the Federal Office for Information Security (BSI), classification societies, industry associations. These provide the relevant requirements and form a basis for the preparation and updating of the management system / SMS and the Risk Assessment (RA).

- Update existing legal registers to include documents regarding information security:
  - Provisions to be met
  - Guidelines to be considered

1.2
ORP.5
CON.2
CON.7

4. Risk Assessment

Through Risk Assessment (RA), hazards are identified, risks assessed and required protective measures determined. For this, the existing ISM RA can be used. The extent of it depends on factors such as company structure, ship type, degree of automation on board and access to IT/OT. Comprehensive vulnerability assessments (e.g. penetration tests) are also useful tools for Hazard Identification (HAZID) and Risk Assessment (RA).

- Evaluate risks.
- ISM Note:

  The risks for shipboard operations are to be considered, i.e. using RA, effects and consequences of a cyber incident have to be considered just as much as the likelihood of a cyber incident itself.
- Notice IT-Grundschutz profile:

  The Basic and Standard Requirements of the IT-Grundschutz modules are based on a consideration of the potential threats and the resulting risks, so that appropriate measures for the normal protection needs and for typical application scenarios provide sufficient protection. For deviating scenarios, the profiles contain notes on "Performing a risk analysis based on IT-Grundschutz".
- Notice ISPS risk assessment

  Please refer to the section "ISPS Code" on page 2 for information on the ISPS risk assessment.
- determine measures to minimize risks
- carry out regular control of effectiveness

1.2
Notice
Notice
IT-Grundschutz profiles
Notice

5. SMS (Result RA)

One outcome of the RA are technical, organizational und personal protective measures. They are outlined as process or procedural instructions in the SMS, and in this way are made available to the crew.

- Create procedures and guidance in the SMS, change and update as appropriate
- Use suggestions from the IT Grundschutz profiles, e.g. by referring to individual elements
- Refer to the SSP, as appropriate, e.g. regarding confidential information and measures that are not intended to be made freely accessible

1.4
9.4
IT-Grundschutz profiles

6. Master

The SMS describes the CRM responsibility and the master's tasks as well as his or her decision-making and managerial authority. Aside from implementing and monitoring the measures, this includes recognizing and reporting deficiencies and vulnerabilities to the shipping company as well as motivating the crew to participate. Qualification activities may be required for CRM and have to be documented in the SMS.

- Update task description of master (e.g. job description)
- Determine qualification requirements
- Determine qualification activities
- Assure overriding authority
- Motivation: support with appropriate tools and specific guidelines

5
6.1
6.2
6.1
ORP

7. Office Support

With the appropriate organizational set-up, the master is provided with competent shore-based support by the shipping company to
- React to a cyber incident,
- React to the consequences of such an incident,
- Re-establish systems (backup & restore).

- Designate the responsible person(s)
- Determine tasks of the "shore-based organizational set-up"
- Update task descriptions
- Form an emergency team (also refer to module 9)
- Prevention
- Take IT-Grundschutz profiles for shipping companies - shore operations into account

3.2
3.3
4
6.5
6.2
9.4.12
IT-Grundschutz profiles

8. Qualification

The SMS describes the CRM responsibilities and tasks of crew and office personnel concerned. These persons will be instructed when they commence their duties, when these change and at regular intervals. In addition, the SMS contains a training and qualification plan as well as measures to determine the need for training (office personnel / crew).

- Update description of tasks in the SMS (e.g. job description)
- Extend qualification plan (matrix)
- Extend training plan (matrix)
- Requirements for instructions for office personnel and crew
- Measures to raise awareness in accordance with BSI ORP
- Tasks of the crew

6.4
6.5
8.2
9.4.7
9.4.9
ORP

9. Emergency

The existing ISM emergency plans are complemented with aspects of CRM (on board & in the shore-based office) and practised regularly with drills, simulations and training sessions (Aim: acting in a reflective manner).
The plans include:
- Reacting to cyber incidents and their consequences
- Re-establishment (backup & restore)
- Emergency phone numbers and report chains
- Emergency team "shore-based office" (incl. composition)

- Emergency plan for the ship
- Emergency plan for the shore-based office
- Emergency team & its set-up at shore-based office
- Add to ISM Drill Plan
- Emergency contact details
- Emergency report chains

8.1
8.2
8.3
9.4.4
9.4.6
DER

10. Reporting

Incidents, accidents, near-accidents and other relevant events are reported via the ISM reporting process to the responsible internal department where they are evaluated and analysed. Consequently, corrective actions and preventative measures are initiated. Aim: continuous improvement. Descriptions of reporting chains and external reporting obligations are provided.

- Specification about how to report
- Contact details
- Reporting chains

9.1
9.2
9.4.12
DER.2.1

11. PMS

Ensuring the maintenance of the ship and equipment is already addressed with a procedure in the SMS and is updated to include CRM measures. Protective measures derived from Risk Assessment that need to be concurrently reviewed or conducted on a regular basis are managed with the PMS (Planned Maintenance System / planning, execution, documentation). This may include software updates. The segment Critical Equipment is updated.

- Define verification and maintenance tasks
- Manage tasks in the PMS
- Review list "critical equipment" and update as appropriate

10.1
10.2
10.3
10.4
9.4.16
ISMS.1

12. Documentation

Requirements for documentation and access to these are already part of the SMS; CRM matters are added.

- Update existing procedure
- Update ISM documentation

ISM 11
10.4
ISMS.1

13. Verification

The management system, the degree of implementation and the effectiveness are verified continuously with internal and external audits in accordance with defined procedures. Internal audits on board and at the shore-based facilities are updated to include the topic CRM and are conducted at intervals not exceeding 12 months.

- Update internal audit procedure
- Update internal verification lists & verification criteria
- Train auditors

ISM 12.1
9.4.8
DER.3.1

14. Evaluation

The safety management is evaluated regularly on an annual-basis to verify whether the organizational set-up on board and at the shore-based office works in accordance with the SMS requirements, the measures are effective, the personnel and internal auditors are sufficiently trained and audit results are disclosed – as far as reasonable – and necessary corrective actions are initiated promptly.

- Incorporate topic into Management Review
- Summarize results of the audits, incidents and near-incidents, received advice, analyses, corrective actions / preventative measures, follow-up measures of previous or other evaluations, compliance with policy, existing resources.

12
8.5
9.4.11
DER.3.1

15. CIP Improvement

Continuous improvement process – the shipping company must provide for on-going changes and identified vulnerabilities in its system and ensure that the SMS and RA systems are updated, which initiates the continuous improvement process.

- Determine measures for CIP and updating of SMS

SMS
14
DER.3.1
ISMS.1

Appendix I - Operating instructions for the IT-Grundschutz profiles for shipping companies

An IT-Grundschutz profile is a model security concept that serves as a template for institutions with similar framework conditions, for example in a specific industry. In an IT-Grundschutz profile, the individual steps of a security process are bundled and documented for a defined area of application. This includes: defining the area of application, conducting a generalized structural analysis, determining the need for protection and modelling for this area, selecting and adapting the IT-Grundschutz modules to be implemented and describing specific security requirements and measures.

Users can transfer the security consideration to the individual framework conditions of their company and increase the security level in the company in a modular way. This saves them a lot of time and work. An IT-Grundschutz profile is thus a practical solution for taking the first steps towards information security with manageable personnel and financial expenditure.

With the IT-Grundschutz profiles for shipping companies recommended here, practical model security concepts are available. In the IT-Grundschutz profile for shipping companies – ship operations, the processes "technical operation", "nautical operation", "landing operation" and "communication" have already been identified and offer so-called maps for the implementation of the necessary requirements for ensuring information security on board. The IT- Grundschutz profile for shipping companies – shore operations focuses on the processes "Accounting" and "Technical Management" and serves as an implementation aid for the topics listed under point 7 concerning shore support.

Notice for the usage of the IT-Grundschutz profiles

The two IT-Grundschutz profiles each describe how the model security concept serves as the basis for the information security process in the shipping company and is to be adapted to the real conditions in operation. At this point, additional helpful tips for handling the individual IT-Grundschutz modules are summarized.

How can I work with the original IT-Grundschutz module in a time-saving and targeted manner?

The original IT-Grundschutz module is located on the BSI website and can be reached there. The structure is always the same, and the individual chapters can be accessed in a targeted manner using "jump labels". This saves a lot of time, because you can access the text passages that are relevant for you directly.

Chapter (Content)	Recommended Reading
1. Description (Introduction, Objectives, Demarcation from other modules)	CAN – offers general background information and is used for classification
2. Threat Landscape	CAN – overview of risks that can occur if the requirements are not implemented
3. Requirements	
3.1 Basic Requirements	MUST – the Basic Requirements are the necessary requirements for increasing information security in your company
3.2 Standard Requirements	MUST – if Standard Protection is sought
3.3 Requirements in Case of Increased Protection Needs	CAN – e.g. relevant, if this module is based on a particularly sensitive target object of your company
4. Additional Information (Literature)	CAN – for more detailed information on the topic
5. Appendix: Cross-Reference Table for Elementary Threats	CAN – here you can see which risks you were able to minimize by implementing the module

[!] IMPORTANT: Basic Requirements are a MUST, Standard Requirements a SHOULD
Each requirement with the numbering A.1 to A.n contains MUST or SHOULD record. Consider the text section like a checklist: Each sentence is a separate requirement to be considered. If it has already been fulfilled in your company – tick it. If it is NOT fulfilled, then there is still something to do.

How can I use the implementation instructions for the IT-Grundschutz module?

The BSI has issued practical Implementation Guidance for many IT-Grundschutz modules. The good news is that you don't have to read the comprehensive explanations in their entirety, but only what really interests you at the moment. The trick: A becomes M. For each requirement with the abbreviation A.[number] in the module there is a suitable measure with the corresponding abbreviation M.[number] in the implementation notes (if these are available). In the online version, jump labels also facilitate direct access to the "basic measures".

For example: The basic requirements „OPS.1.1.4.A1 Creation of a concept for protection against malware” in the module “OPS.1.1.4 – Protection against malware” corresponds to the measure “OPS.1.1.4.M1 Creation of a concept for protection against malware” in the corresponding implementation notes.

Appendix II - Glossary

ACP list: Access point list – listing all electronic access points to the ship's IT and ship's OT as basis for the Risk Assessment and identification of potential vulnerabilities.

APP: Application – application software in general and not limited to smart phone and tablet applications.

Audit: Systematic, independent internal or external process for verification of a management system and to gain proof and evaluate this proof to determine if defined audit criteria have been met and the requirements of the management system have been implemented.

Awareness: Being aware and paying attention – missing or intermittent instructions/professional development training of crew and shore-based office personnel increase the likelihood of improper actions when preventing, recognizing and reacting to hazards and threats.

BDSG: The German Bundesdatenschutzgesetz (Federal Data Protection Act, BDSG) complements Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)), which is directly applicable, by defining those areas where the EU Regulation leaves room for the member states to decide the scope. Since the protection of data is required, the BDSG is an element that needs to be considered in the management system.

Cargo: The accuracy of cargo details (weight, dangerous goods, stowing position e.g. for loading of containers) is primarily the task of the terminal and the charterer. The secure data exchange between shore and ship and, therefore, safe stowing must remain guaranteed.

Certification: A certification in addition to ISM is not required with regard to IMO, but such requirements may become necessary when operating in the private sector or due to identified hazards and risks, the management of the operations or the size of the company.

CIP: Continuous improvement process – a fundamental principle to update and further develop the management system through continual adaptation and improvement, in particular as a result of evaluations.

Corrections: Corrective actions (CA) to remove a recognized deviation or vulnerability.

Cyber Risk Management (CRM): This comprises company principles, procedures and resources that a company has implemented and further developed, the purpose of which is to recognize, reduce and defend against potential risks resulting from using IT and OT.

Hazard: Source, situation or action that may lead to damage.

HAZID: Hazard Identification – list of potential hazards systems and equipment at risk, as a non-exhaustive list that requires continuous updating. This hazard identification serves as a basis for the Risk Assessment

Industrial Guideline: "Guidelines on Cyber Security Onboard Ships" - this is recognized information by professional associations and may be of assistance in developing and updating the management system. Details can be obtained with BIMCO or the other authors.

Integrated: Cyber Risk Management can be integrated into the existing SMS of the shipping company with individual measures and procedures or, alternatively, be managed as an independent management system with an interface to the ISM SMS

IPDRR: The management system should consider the IPDRR principles and measures recommended by the IMO:

IDENTIFY	Identifying hazards
PROTECT	Protection from "hazards"
DETECT	Identifying an "incident"
RESPOND	Reacting to an "incident"
RESTORE	Re-establishment of affected systems

ISM Code: International Safety Management Code. This is an internationally applicable standard for measures to manage the safe operation of ships and to prevent marine pollution. The Code stipulates required measures for the management of safe operation of ships. Because of the Code's modular set-up, safety measures that have become necessary due to cyber threats can be integrated into the existing Safety Management System (SMS) of the shipping company.

ISM-certified: The Safety Management System of the shipping company undergoes initial and annually recurrent verification by internal and external audits. The verification of the implementation of these systems on board the ship also occurs on a regular basis with external and internal audits. This is subsequently certified.

ISMS: Information Security Management System (ISMS) - a management system from the IT sector; there is no connection with IMO and the ISM Code. Thus, there is a likelihood of confusion.

ISPS Code: International Ship and Port Facility Security (ISPS) Code, has been applicable to ships flying the German flag since 2004.

IT-Grundschutz: The IT-Grundschutz are recommendations for implementing information security and consist of system and process modules with concrete recommendations for action.

Appendix II - Glossary continued

IT / OT: IT: Information technology and networks, e.g. communication facilities, email / telephone as well as internet, office PC, PMS server, wifi.

OT: System units / operational PCs (e.g. GNSS, Radar, ECDIS, machine control, sensors, alerts, monitoring).

RA and SMS must not only be limited to IT – measures must consider OT and interfaces between IT and OT.

Navigation: Possible hazards may be:

- Failure or manipulation of GPS / DGPS.
  GPS spoofing: false position data.
  GPS jamming: interfering transmitter, signal interference or signal prevention.
- Failure or manipulation of AIS Data.
- Inaccurate speed input leads to inaccurate ARPA processing.
- Inaccurate ECDIS information.
- Failure (crash) and reboot error of the radar equipment / integrated equipment.
- Manipulation or failure of DP systems.
- Failure of echo sounder and other software-based and/or integrated navigation systems.
- Interference of control and monitoring of the machinery installations / units.
- Inaccurate voyage planning.

Procedure: Specification of how a task or a process is to be carried out.

RA: Risk Assessment – the process of assessing the risk of a hazard. The RA is utilized to determine the risks and the required counter and protective measures.

RA method: Different models and approaches exist. The choice of the method and its practical implementation rests with the company.
Example of the HAZID and the RESID model:
The first step is to identify the hazards (HAZID list) and the resources (RESID list). In addition, all ways to access the ship's IT or ship's OT are identified (ACP list). If the ACP list generates no access points, the scope of the required measures is too narrow. Based on these lists, the risks of the identified hazards are evaluated and, if required, protective measures are determined according to the TOP hierarchy of measures (technical measures take precedence over personal and behavioural measures).

Risk: Connection between the probability of occurrence and the severity of damage of a hazard or a hazardous event.

Risk =
Probability of occurrence x Severity of any damage

To reduce a risk means to positively influence the probability of occurrence and/or the severity of damage with a protective measure. In case of an acceptable risk, measures may be omitted. A risk is acceptable if it has been reduced to a point where it can be tolerated taking into consideration the legal and contractual obligations as well as the company's policy.

Risk Analysis: refer to RA.

Risk matrix: Presentation of the different risks to conduct the risk assessment, from low risk via medium, still tolerable risk (ALARP) to very high risk. Example: risk matrix according to Nohl.

Requirements: There are no specific requirements for the contents and formal approach or composition of a management system. Legal requirements: Chiefly, an obligation for Cyber Risk Management arises from IMO requirements with regard to the ISM Code, the GDPR of the EU and the German BDSG.

RESID: Resource Identification – listing the resources and competences as a basis for the evaluation as to whether in-house options are sufficient or manufacturers, external service providers or experts need to be consulted. It is a basis for Risk Assessment (see also HAZID) and lists potential manufacturers and service partners.

Scope: Depending on the realized hazards, the scope of the measures must be in relation to the determined hazards and the size of the organization. The aspiration for continuous improvement should always be preferable to the attempt at a singular all-encompassing and conclusive regulation.

TOP: Hierarchy of measures – reduce an existing risk with protective measures according to the TOP hierarchy:

(T) technical

(O) organizational

(P) personal

(T) measures take precedence over (O) and (P), a technical measure is safer than directions of conduct (P).

Example e-mail correspondence:
(P): Direction to crew "don't open attachments ending in .exe & .mpg".
(T): a filter only allows for attachments ending in .pdf & .jpg. This (T) measure is safer than the direction of conduct (P).

Refernce to other glossaries by the BSI:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyberglossar/cyberglossar_node.html

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/glossar_node.html

Appendix III - Rules & Guidelines

Reference to further information, rules and guidelines.

IMO Resolution MSC.428(98)	*IMO* *www.imo.org*
IMO Guidelines MSC-FAL.1/Circ.3	*IMO* *www.imo.org*
ISM Circular 04/2017	*BG-Verkehr* *www.deutsche-flagge.de*
ISM Circular 04/2018	*BG-Verkehr* *www.deutsche-flagge.de*
IT-Grundschutz profiles for shipping companies – shore operations	*BSI* *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_for_Shipping_Companies_Minimum_Protection_for_Shore_Operations.pdf?__blob=publicationFile&v=6*
IT-Grundschutz profiles for shipping companies – ship operations	*BSI* *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_for_Shipping_Companies_Minimum_Protection_for_Ship_Operations.pdf?__blob=publicationFile&v=4*
The Guidelines on Cyber Security on-board Ships (Industrial Guidelines)	*BIMCO, CLIA, ICS, INTERCARGOL, INTERMANAGER, INTERTANKO, IUMI, OCIMF, WORLD SHIPPING COUNCIL* *www.bimco.org*

Appendix IV - Owners-Master

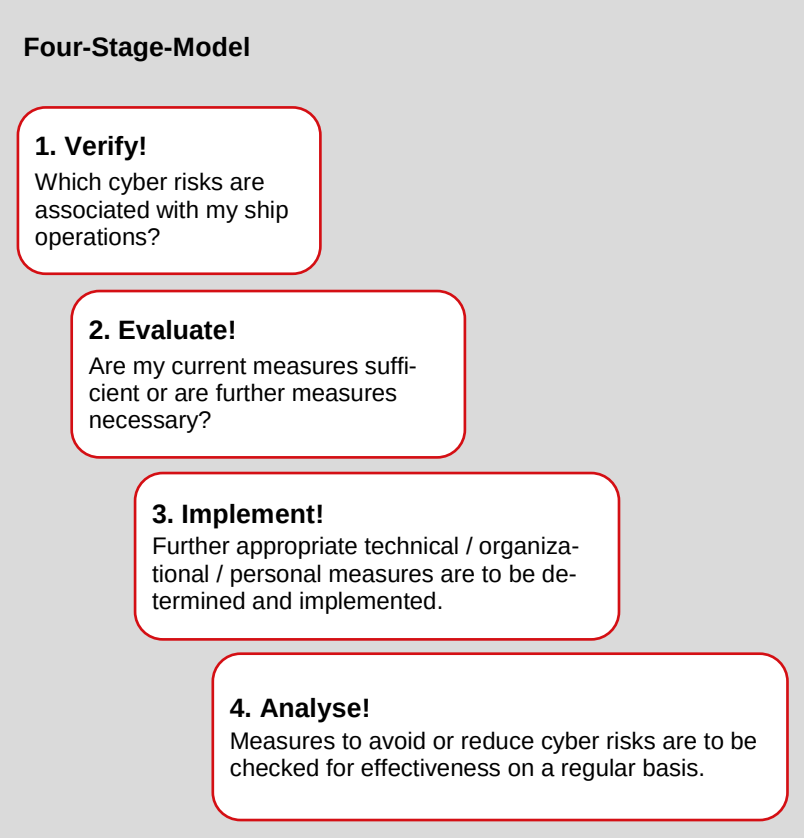
The following lists possible examples of technical, organizational and personal measures and serves as guidance for so-called Single-Ship-Owners-Masters or shipping companies with comparable ship operations.

For the Four-Stage-model applies:

- VERIFY
- EVALUATE
- IMPLEMENT
- ANALYSE.

The depicted measures are very simplified and do not reach the level of information security suggested in this document.

The **Ship Safety Division** suggests these measures as a guidance in case other measures described in this document cannot be implemented due to the size of owner-master companies.



T Technical Measures

USB / LAN lock & sealing
barrier for mass storage media, sealing access of the devices (USB,LAN)

Physical removing
of CD/DVD, Floppy- and other relevant drives

Stand alone solution
one PC instead of a network system (e.g. cargo-PC)

Quarantine PC
network independent PC for virus checks

Access limitation
physical barrier - Server location: restricted area

Backup Storage
data saving on external mass storage media

Protection & filter
- firewall
- anti-virus software
- spam-Filter

Software / APPS
- install only required apps / software
- unnecessary functions & plugins deactivated

Software access management
access differentiation - different levels. Only those persons get rights that need them (software, drives)

Updates / Patches:
APPS, MS Office, IT, OT – to be kept updated to close software gaps

Cloud
avoid simple cloud services

Physical separation
separation of internal and external systems

VPN – encryption
virtual Private Network, encryption of communication

Remote access control:
authentication of accesses (RAS,VPN)

Networks:
multiple segmentation (Operation/Master/Crew/…)

WLAN protection
secured to the latest standard, different networks for crew & ship operations

Email
crew Internet email: Stand alone solution instead of "cabin networking" (physical separation from the network)

blocking certain email attachment like .exe, .cpl, .bat, .com, .scr, .vbs, .vba (e.g. crew allowed: only .jpg,.txt,.pdf).

limitation on email attachments (account depending)

Access control
IT operation requires Login / authentication

O Organisational Measures

Rights
restrict Administrator's rights and access rights

Responsibilities & duties
define and manage: sea / shore / third parties

Contractors / third party on board
authorisation, work permit, access limitation, warning notices, OT access authorisation

PMS System
extend for planning, implementation & documentation
- regularly IT reviews
- updates / patches
- backup

IT inspections / reviews
- internal or external safety contractors
- advice by expert consulting

Screen lock
automatically after x minutes / manually when leaving the work station

Office support by owner
- hotline / contact / advice
- emergency / contingency plan office
- recovery plan

Expert consulting
seek advice if own IT is overwhelmed (emergency contact)

Supervision
monitoring / detection)

Data management
regulations on data economy

P Personal Measures

Familiarization
- initial
- recurrent
- occasional

Qualification
training, CBT & info programs Info-Programme (raise awareness)
- shore
- sea

Possible content
- navigation: detect manipulation of GNSS, AIS, track control
- monitor & detect
- react & notify
- recovery
- awareness
- hazards
- protection measures
- behaviour based measures

Information
posters, electronic media & other information material

Behavioural notes
displays, text instruction via the screen saver

Behavioural instructions (a)
Clear instructions for sensible areas

Behavioural instructions (b)
declaration of injunction for manipulation, hacking Manipulation / network access (crew hacking, contracts, contracts addendum)

Disciplinary measures
in case of a conscious disregard of the requirements (negligence)

Qualification measures
in case of unconscious disregard of the requirements