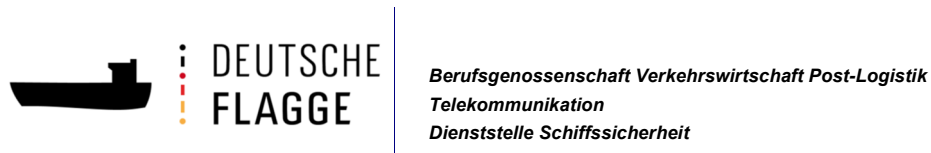
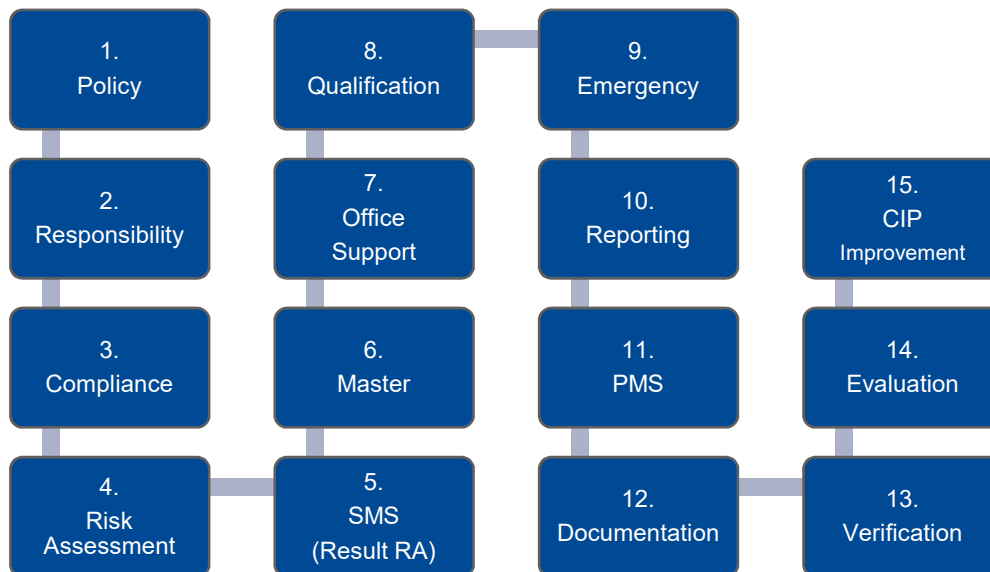


# ISM Cyber Security



## ISM Cyber Security Process



The ISM Code is a mandatory international instrument to establish measures for the safe management and operation of ships. The modular concept of the Code allows the integration of necessary cyber security measures in the Safety Management System (SMS) of the company.

Such integrated management system corresponds with the requirements of the IMO Resolution MSC.428(98) and fulfils the IMO GUIDELINE ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/Circ.3) whilst it is able to avoid a single competing system which could lead to additional administrative and financial burdens of the company.

The integration allows the company to amend their own safety management system with the required and specific Cyber Risk requirements that encourage the management and acceptance of changes.

## Cyber Risk Management

The increasing interactivity and degree of networking as well as the increasing disappearance of network borders on board are encountering an increasing potential for criminal cyber activities and increasingly shorter attack cycles. Ships may become a direct and thus externally controlled target. However, they may be accidentally damaged by a crew member by introducing a malicious software not specifically intended for the ship, e.g. via network access by an e-mail attachment or USB stick. Thereby in an unprotected network system, dependents of a crew member could theoretically bring down everything that is controlled by software - from the radar to engine control sensors. In addition, in crisis areas, the GNSS signals (e.g. GPS) may be disturbed in a way that makes them inoperable on board - or spontaneously showing offset positions by miles. If the ship remains unprotected, the hazard can increase exponentially. These and other concrete and less concrete hazards make it necessary to support the safe operation of ships by an individual cyber risk management.

### 1. Policy

The top management of a shipping company recognizes the fundamental risks to the safe ship operation through cyber crime and the need for regulation and those for the expansion of the own ISM management objectives. The existing policy needs to be amended with cyber security aspects and required measures. Cyber security becomes a direct concern of the management board.

### 2. Responsibility

The ultimate responsibility in cyber security remains with the top management. To the extent possible and depending on company's organization and size, an appropriate person - usually the head of the company IT department - will be designated as the responsible person for managing and protecting against cyber risks and to assist the Master in conducting assigned shipboard tasks and responsibilities.

### 3. Compliance

Rules, guidelines and recommendations of the IMO, Flag State, Class and related industry are identified and the essential requirements are derived. They form a basis for creating and updating the Risk Assessment (RA) and Company's SMS. Legal registers will be amended or recreated accordingly and list these guidelines and recommendations.

### 4. Risk Assessment

With the ISM RA the risks and necessary safe guards are being identified. Unless an equivalent system exists, the following approach can be used for a systematic assessment:

1. Preparation:
  1. HAZID Hazard Identification
  2. RESID Resource Identification
  3. TOP Potential safe guards
2. Assessment: Based on the preparation: determining the risks, safe guards and responsibilities.

### 5. SMS (Result RA)

The results of the risk assessment - and thus the necessary safe guards – are a subject to be included into the SMS of the company. They are recorded as a process or operating instruction or in another suitable way. Basically, the required measures should be made known to the crew. If the RA determines that certain measures should not be made public or should not address all persons within the Company, they can be a subject to the SSP.

### ISM objective

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

### Managing Directors & Priority

Queries to the P&I and H&M insurers can influence the consideration of the significance and priority, and thus the scope of the measures, especially when considering financial risks.

### Cyber Risk Management

The measures should fit with the organization size. The aim of achieving a continuous improvement process should always outweigh the attempt to regulate and cover all aspects at once.

### Compliance

IMO Resolution MSC.428(98)  
 IMO Guidelines MSC-FAL/Circ.3  
 ISM Circular 04/2017  
 The Guidelines on Cyber Security on-board Ships (BIMCO, ICS Guide)

Additional useful information regarding Cyber-Security can be found under [www.bsi.bund.de](http://www.bsi.bund.de)

### IPDRR Check

Are the ISM measures covering following aspects?

- |                 |   |
|-----------------|---|
| <b>Identify</b> | Identification of hazards and critical systems. |
| <b>Protect</b>  | Protection against attacks.                     |
| <b>Detect</b>   | Identification of an attack.                    |
| <b>Respond</b>  | Measures to respond to an attack.               |
| <b>Restore</b>  | Measures to be done after an attack.            |

## HAZID

### Hazard Identification

Create a list without rating & risk determination with all potential hazards and potentially endangered assets - GAIN AN OVERVIEW

IT	IF	OT	ACP
<b>Information technology and networks</b>  Office-PC's EMAIL & Internet IP phone SAT phone weather PC PMS Server WLAN / LAN (Cargo-PC) ...	<b>Interface – IT &amp; OT</b>	<b>Operational technology - System installation</b>  GNSS AIS RADAR & ECDIS Engine control System- and valve control Sensors Steering gear Alarm & monitoring	<b>Access Points</b>  USB LAN WLAN BT DVD/CD ROM Mobile mass storage & mobile units ... Concrete identification: at which plant?

## HAZID

List of all potential hazards and potentially endangered systems on board as a non-exhaustive list to be further updated which serves as the basis for the risk assessment.

If it is created in a team of various participants (e.g. Masters, engineers, DPA, quality manager, CSO, superintendents, IT managers / experts, top management, etc.) and subdivided in advance into the four areas IT, IF, OT and ACP, the list can provide a comprehensive basic picture of the hazards.

## RESID

### Resource Identification

Create a competence list: potential internal or external resources?

IT	IF	OT	ACP
Competences: Own? Contractor?  List all maker's and possible service contractors.	Competences: Own? Contractor?	Competences: Own? Contractor?  List all maker's and possible service contractors.	Competences: Own? Contractor?


## Externals & contractors

Makers and contractors may have to be involved if the own resources are not sufficient - this may be necessary in particular for OT and IF protection.

The RESID list should identify which resource becomes necessary.

## T Technical Measures

Example of possible measures

Firewall Anti-virus software Spam-Filter Firewall & anti-virus software & spam-filter installed on all relevant PCs USB lock (mass storage media) Backup Storage (external solution) 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) Configuration management Separation of internal and external systems VPN		Remote access control: authentication of accesses (RAS,VPN) Sealing access of the devices (USB,LAN), Seal management BUS Management Networks: multiple segmentation (Operation/Master/Crew/...), especially WLAN networks (secured to the latest standard) Stand alone solution instead of network-system (e.g. cargo-PC) Quarantine PC (for virus checks) Software: access differentiation - different levels. Only those persons get rights that need them (software, drives)	Crew Internet email: Stand alone solution instead of "cabin networking" (physical separation from the network) Log files for IT experts (follow-up) Avoid simple cloud services (the Company), otherwise provide own services Activation of automatic updates and patch services: - Software in general - MS Office - OT systems - IT system - anti-virus software  Unnecessary software functions & plug-ins are removed or locked. Server location: restricted area
---	---	---	--


## TOP measures:


List all potential safe guards as a non-exhaustive list to be further updated. The list serves as another basis for the risk assessment.

One way of developing could be a "Brain Storming" with IT, DPA, QM / QHSE, Nautical & Technical Department, top management or others.

## Data protection

Cyber security should include measures for personal data protection.

O Organizational Measures		Example of possible measures
Policy of the Management Board (Ultimate Responsibility)  Password policy / Password management  Dynamic (regular) changes of password  Assignment of access rights (different levels)  Clear defined responsibilities at shore side  Designation of an IT expert Responsibilities at sea Responsibilities shore Responsibilities of third parties  Contractor service on board (authorization, work permit) Backup organization (regular) Audit  Inspection by IT (internal or external safety contractors) PMS – regular IT checks PMS – software update Administrators only get the rights they need	 Manual Updates (PMS) for time / system critical patches: - for stand-alone units - IT/OT without auto-update - Antivirus Software - ...  Screen lock (automatically after x minutes / manually when leaving the work station)  Office support: - Contingency plan office - Hotline / contacts  Emergency recovery plan PMS Backup (maintaining the history)  OT access authorization, system restrictions, work permit for contractors Expert consulting if own IT is overwhelmed (emergency contact)  Supervision (monitoring / detection)	Monitor & control: terrestrial navigation (check GNSS, ECDIS)  Navigation: redundancy, backup astronomical navigation  Nautical charts as backup for critical sensitive areas  ARPA and evaluation, error of speed input (ARPA: RADAR data instead of AIS data. Speed: LOG input instead of GPS.)  Continuous weak point analysis and evaluation of the reporting system  Ensure: all PC's of the Company are affected and need to be protected and subject to inspections, especially mobile notebooks  Avoid single competences (Administrator, knowledge can be lost in case of changes)  Keep administrator documentation available (knowledge base)  Maintain information flow (seafarers, shore employees)

P Personal Measures		Example of possible measures
Initial familiarization Recurrent familiarization Occasional familiarization Shore based training  Training focus navigation: Detecting manipulation GNSS, AIS  Awareness programs	 Declaration of omission for manipulation and illegal access to networks (crew hacking - contract, contract supplement)  Disciplinary measures in case of intentional / non-intentional disregard of instructions  Timely transfer of information to employees (active communication)	On-demand training (administrator, employees)  Training content: behaviour, monitoring, detection, response measures, password management  Posters & info material

**Risk Assessment**

Processing the RA to identify and assess the risks.

The risk is determined by the product of the *likelihood* x *severity*.

If a risk becomes apparent, appropriate safeguards should be initiated by considering a specific hierarchy which is similar to the TOP measures principle of occupational health & safety standards:

(T) Technical,  
 (O) Organizational  
 (P) Personal.

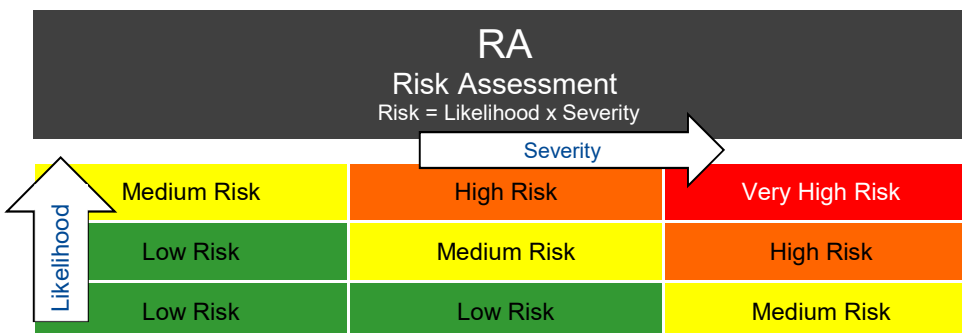
This covers technical, processual and human aspects.

Technical control measures have priority.

Example EMAIL traffic:  
 (P) *Personal behavioural measures: instruction to crew "do not open attachments with .exe or .mpg".*  
 (T) *Technical measures: A filter only allows receiving .JPG, .PDF whilst .exe files are blocked.*

Personal behavioural measures may be implemented faster and could be a cheaper way. But it cannot be assured and cannot be proved safe. This is only possible by technical measures.

The RA must be constantly reviewed and updated due to the rapid changes and development of new risks



### 6. Master

The ISM lists qualification procedures for the master so that he can meet those SMS requirements directed to his position. The company's organization takes into account that the new cyber security tasks are not solely the responsibility of the captain.

### 7. Office Support

By a suitable organization, the captain will receive qualified land-based support to fulfil his SMS tasks. This includes

- responding to a cyber attack,
- responding to the consequences of an attack.
- restore (backup measures).

### 8. Qualification

Upon employment new crew members and office staff receive a familiarization in the company's SMS cyber security activities. They receive an additional familiarization if job tasks are changing or personnel is getting promoted.

The instruction will be necessary for all persons with cyber security tasks and for all persons being in contact with a ship.

Familiarization, instruction and further training measures are regularly recurring and should be repeated as necessary. The SMS contains a training and qualification plan and describes measures to determine training needs. This includes seafarers and office personnel. The scope depends on the position on board / in the company - not everyone has to know everything.

### 9. Emergency

The SMS contains a cyber security contingency plan for the sea and shore office sector. This contingency plan is regularly practiced through exercises, simulations and training with the aim of reflective action. The shore organization has emergency plans in place to assist the captain. The plans include measures to:

- respond to an attack and its consequences,
- restore (backup measures).

An IT manager (if available) may support the shore based emergency response team.

### 10. Reporting

Incidents, accidents, near-misses and other relevant occurrences are reported to the responsible departments by using the ISM reporting system. Reports are subject to an assessment and analysis. As a result, corrective and preventative actions will be determined and communicated.

Aim: continuous improvement process.

## Risk

### Navigation

Masters and nautical officers should be trained to know, recognize and respond to hazardous situations. In addition to general navigational instructions and qualification measures, the existing ISM emergency plans should be amended as necessary.

For example, hazards can result from:

- Failure or manipulation of GPS and DGPS data (jammer).
- Failure or manipulation of AIS data.
- Incorrect speed input leads to faulty ARPA evaluation.
- Incorrect ECDIS information.
- Failure (shut down) and reboot error of the radar equipment.
- Failure depth echo sounder and other software-based and or integrated navigation systems.
- Impact on the control and monitoring of the machinery and power management.

### Human element

Lack of awareness, missing or failing to conduct recurring familiarization and training measures for seafarers and shore staff increase the likelihood of misconduct.

### IT (limiting)

The RA and SMS should not be reduced to IT only. OT, interfaces and access to IT / OT should be included in any case.

### Sustainability

RA and SMS should be continually reviewed and adjusted to respond to the changing cyber threats. One-time integration into the SMS is inadequate.

### Risk Ship-Shore-Connections

Available connections to the "outside" of a system may become an unprotected gateway.

### Risk container stowage planning

Correctness of container information (weight, dangerous goods, stowage positions) is primarily the task of the terminal and the charterer and is an important component for the safe carriage of cargoes. Despite that fact, the RA and SMS should also reflect the electronic data exchange regarding stowage planning between shore and ship.

11.  
PMS

PMS (Planned Maintenance System): the safety measures that have been identified at the RA as recurrently been put in practice, e.g. software updates, are added to the PMS. The PMS monitors and documents those measures.

The Critical Equipment area will be amended to the needs and required details determined via the RA.

12.  
Documentation

Generally, the SMS describes the applicable requirements for any documentation. These are taken over for the field of cyber security.

If documented measures and requirements are within a sensitivity range that does not permit public documentation in the SMS, specific measures should be implemented which are accessible only to a limited group of persons on board and ashore. Examples: Presentation of administrator rights on board, and password management, backup and recovery management.

13.  
Verification

Internal audits on board and onshore at the office will be amended with cyber security aspects and will be conducted at intervals not exceeding 12 months.

The implementation of the cyber security management to the company ISM system as well as the continuous updating is monitored and verified by audits and reviews.

14.  
Evaluation

The Company regularly verifies and evaluates the safety management system considering following questions:

Does the organization (Sea & Office) work according to the SMS requirements?

Are the measures of the SMS effective?

Are internal auditors qualified in cyber security?

Are the results of the audits brought to the attention of relevant personnel?

Are necessary corrective and preventive measures initiated / implemented promptly?

15.  
CIP  
improvement

Cyber security is undergoing continuous and major changes. Therefore, a one-time setup and implementation of safe guards is insufficient. The company should take into account the constant changes and identified weaknesses in its own system and must ensure that the risk assessment system and SMS are updated, thereby initiating the continuous improvement process.

## ISM Check

**Risk Assessment** ISM 1.2

Hazards identified (HAZID List)?

Risks assessed?

Measures implemented to mitigate the risks?

**Compliance** ISM 1.2

National and international rules and guidelines available and considered?

**Policy** ISM 2.1

Available: description of the basic measures to achieve the objectives?

**Responsibilities** ISM 3.2

Responsible persons and their assigned tasks identified?

**Master** ISM 6.1, 6.2

Qualification measures for the Master?

Qualified shore support?

**Familiarization** ISM 6.3

On employment and regularly recurring?

For seafarers and shore staff?

Continuous qualification measures?

**Qualification plan** ISM 6.5

Training needs and training plan identified?

**SMS instructions** ISM 6.5

RA result? Qualified instruction?

**Emergency preparedness** ISM 8.1, 8.2

Contingency plan sea / shore?

Regular drills based on the plan?

Shore support (emergency response team)?

**Reporting system** ISM 9.1, 9.2, 9.3

Reports: occurrences, accidents, near-misses?

Reports are assessed and analysed?

Corrective & preventive action implemented?

**Maintenance** ISM 10.1, 10.2, 10.3

Measures are integrated to and documented at the PMS. Critical Equipment – checked?

**Documentation** ISM 11

Requirements available for dealing with general and sensitive data with limited accessibility?

**Verification** ISM 12.1

Internal audits amended with cyber security aspects?

**Evaluation** ISM 12.2 – 12.7

Organization is working according to the SMS?

SMS measures effective?

Auditors qualified?. Results communicated.

Corrective & preventive action?

## Check of sensitive areas

Administrator rights on board?

Password management?

Backup and recovery management?