SVENSK
SJÖFART
SWEDISH SHIPOWNERS´ ASSOCIATION

SJÖFARTSLUNCH
CYBER RISK MANAGEMENT

Program

12.00 Status i frågan inom IMO och EU samt implementering av *Resolution MSC.428(98) – Maritime cyber risk management in safety management systems* – Johan Isaksson, Transportstyrelsen

12.20 Inledning och information om cyber risk management guidelines – Christina Palmén, Svensk Sjöfart

12.40 Exempel från rederier om hur man arbetar med frågan

- Sten Rosenqvist, Eckerö
- Donald Werner, Furetank

13.15 Frågor och diskussion

13.30 Slut

SVENSK SJÖFART
SWEDISH SHIPOWNERS' ASSOCIATION

Inledning och information om cyber risk management guidelines

Christina Palmén, Svensk Sjöfart

SVENSK
SJÖFART
SWEDISH SHIPOWNERS´ ASSOCIATION

Cyber risk management guidelines

3 mars 2020
Christina Palmén, Svensk Sjöfart

Cyber security

Cyber risk management

Cyber risk management and the safety management system

[IMO Resolution MSC.428(98)](#) makes clear that an approved SMS should take into account cyber risk management when meeting the objectives and functional requirements of the ISM Code.

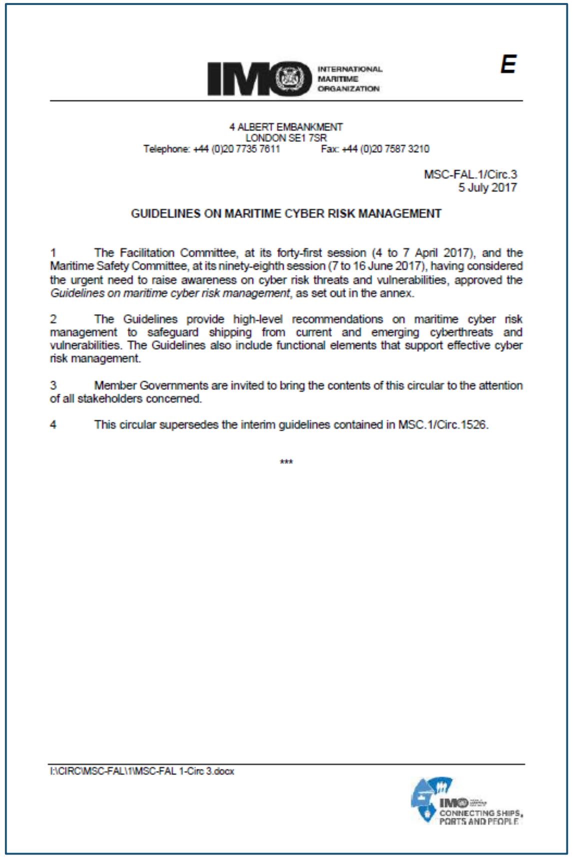
The guidance provided in the **Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3)** provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management.

The guidelines on cyber security onboard ships – Annex 2

The guidance in this annex is designed to provide the minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS.

SVENSK SJÖFART
SWEDISH SHIPOWNERS' ASSOCIATION

IMO Guidelines on maritime cyber risk management


IMO INTERNATIONAL MARITIME ORGANIZATION E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

I:\CIRC\MSC-FAL\1\MSC-FAL 1-Circ 3.docx

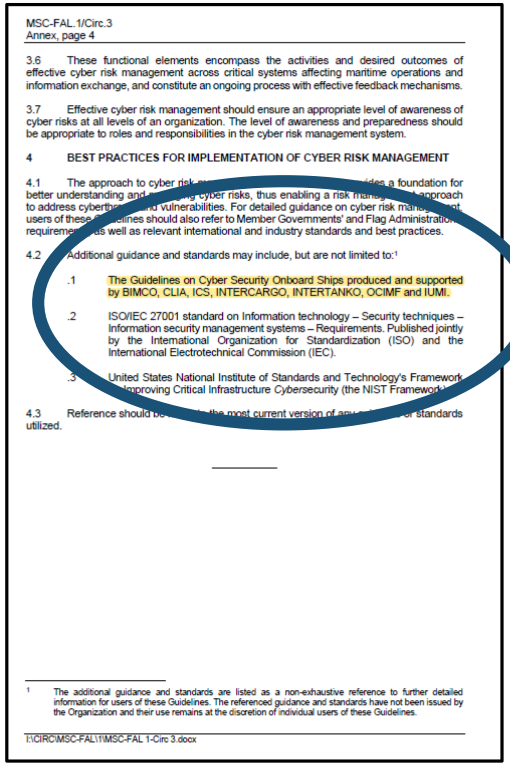
IMO CONNECTING SHIPS, PORTS AND PEOPLE

The Guidelines on cyber security onboard ships

Cyber Security Workbook for On Board Ship Use

The Guidelines on cyber security onboard ships

IMO Guidelines on maritime cyber risk management


MSC-FAL.1/Circ.3
Annex, page 4

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk [illegible] provides a foundation for better understanding and [illegible] cyber risks, thus enabling a risk [illegible] approach to address cyberthr[illegible] vulnerabilities. For detailed guidance on cyber risk [illegible], users of these [illegible] should also refer to Member Governments' and Flag Administration[illegible] requirements as well as relevant international and industry standards and best practices.

4.2 Additional guidance and standards may include, but are not limited to:[1]

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

.2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

.3 United States National Institute of Standards and Technology's Framework [illegible] Improving Critical Infrastructure *Cyber*security (the NIST Framework).

4.3 Reference should be [illegible] the most current version of any [illegible] standards utilized.

[1] The additional guidance and standards are listed as a non-exhaustive reference to further detailed information for users of these Guidelines. The referenced guidance and standards have not been issued by the Organization and their use remains at the discretion of individual users of these Guidelines.

I:\CIRC\MSC-FAL\1\MSC-FAL 1-Circ 3.docx

4.2 Additional guidance and standards may include, but are not limited to:[1]

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

.2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

.3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure *Cyber*security (the NIST Framework).


CYBER RISK MANAGEMENT APPROACH
Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protection measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a prioritised contingency plan to mitigate any potential identified cyber risk.
Respond to and recover from cyber security incidents
Respond to and recover from cyber security incidents using the contingency plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

Identify threats

Understand the external cyber security threats to the ship.

Understand the internal cyber security threat posed by inappropriate use and lack of awareness.

Identify vulnerabilities

Develop inventories of onboard systems with direct and indirect communications links.

Understand the consequences of a cyber security threat on these systems.

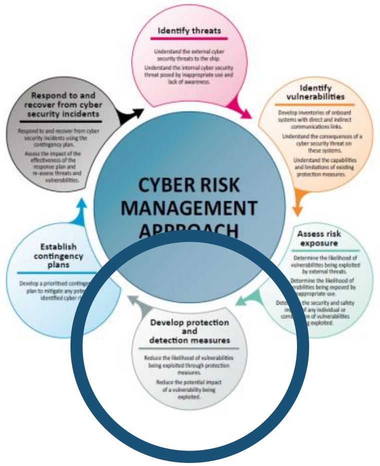
Understand the capabilities and limitations of existing protection measures.

Assess risk exposure

Determine the likelihood of vulnerabilities being exploited by external threats.

Determine the likelihood of vulnerabilities being exposed by inappropriate use.

Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.



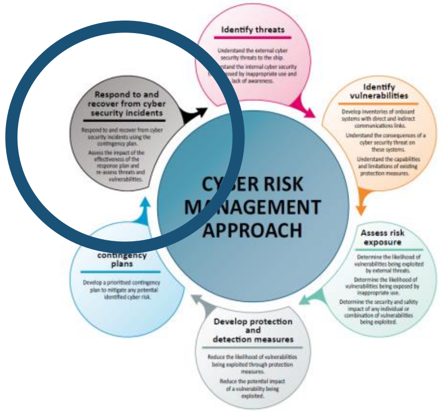
Develop protection and detection measures

Reduce the likelihood of vulnerabilities being exploited through protection measures.

Reduce the potential impact of a vulnerability being exploited.

Establish contingency plans

Develop a prioritised contingency plan to mitigate any potential identified cyber risk.



Respond to and recover from cyber security incidents

Respond to and recover from cyber security incidents using the contingency plan.

Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

The Guidelines on cyber security onboard ships

ANNEX 2 Cyber risk management and the safety management system

IMO Resolution MSC.428(98) makes clear that an approved SMS should take into account cyber risk management when meeting the objectives and functional requirements of the ISM Code. The guidance provided in the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. The guidance in this annex is designed to provide the minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS.

IMO Guidelines on maritime cyber risk management / The Guidelines on cyber security onboard ships – ANNEX 2

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVERY

IDENTIFY[20]

Roles and responsibilities[21]	
Action	**Remarks**
ISM Code: 3.2 Industry Guidelines: 1.1 Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	An updated safety and environment protection policy should demonstrate: ■ a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment ■ an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks ■ an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.
ISM Code: 3.3 Industry Guidelines: 1.1 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[22] onboard ships and are responsible for the SMS. Allocation of responsibility and authority may need to be updated to enable CRM. This should include: ■ allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel ■ incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.

Cyber Security Workbook for On Board Ship Use

- 1st Edition 2019

3 punkter att ta med

- 1 januari 2021
- Guidelines on Maritime Cyber Risk Management (MSC-FAL/Circ.3)
- The guidelines on cyber security onboard ships - Annex 2!

SVENSK SJÖFART

SWEDISH SHIPOWNERS´ ASSOCIATION

Exempel från rederier

Sten Rosenqvist, Eckerö

Rederi Ab Eckerö

Cyber Security
Risk Management

Sten Rosenqvist, Säkerhetschef DPA/CSO

Rederiaktiebolaget ECKERÖ

Eckerös 5 affärsområden

ECKERÖ LINE	BIRKA CRUISES	ECKERÖ LINJEN	WILLIAMS	ECKERÖ SHIPPING
Eckerö Line bedriver passagerar- och lasttrafik mellan Helsingfors och Tallinn.	Birka Cruises bedriver kryssningstrafik mellan Stockholm och Mariehamn.	Eckerö Linjen bedriver passagerartrafik mellan Grisslehamn och Eckerö samt erbjuder olika turism- och reseprodukter.	Williams Buss bedriver linje- och chartertrafik.	Eckerö Shipping bedriver ro-ro trafik med inriktning på exportindustrin

Rederiaktiebolaget ECKERÖ

Koncernstaber & support

Ekonomi & Finans	IT System	Personal	Inköp och Logistik	Fleet Management

Fartygsflotta

M/S Finlandia

Byggd :2001, Daewoo Shipbuilding & Heavy Machinery Ltd., Sydkorea
Längd: 175 m Bredd: 27,6 m. Kapacitet: 2.080 passagerare.
Frakt: 610 bilar (1808 fraktmeter). **Helsingfors – Tallinn.**

M/S Eckerö

Byggd :1979, Aalborg Værft A/S, Aalborg, Denmark
Längd: 121 m Bredd: 24,5 m. Fart: 20 knop. Kapacitet: 1.630 passagerare.
Frakt: 265 bilar (515 fraktmeter).
I trafik för Eckerö Linjen Ab, **Eckerö – Grisslehamn.**

M/S Birka

Byggd: 2004, Aker Finnyards Oy, Raumo, Finland
Längd: 177 m. Bredd: 28 m. Fart: 21 knop.
Kapacitet: 1.800 passagerare, 715 hytter/1.800 bäddar
I trafik för Birka Cruises AB, **Mariehamn – Stockholm**.

M/S Finbo Cargo

Byggd: 2000, Astilleros Espanoles S.A. (AESA), Sevilla, Spanien
Längd: 180 m Bredd: 25 m. Fart: 22 knop. Kapacitet: 366 passagerare.
Frakt: 2000 fraktmeter. **Helsingfors – Tallinn.**

Rederiaktiebolaget ECKERÖ

Ro-Ro Flotta

Exporter

Levererad: 1991
Dödvikt: 5 765 ton
Chartrad till Holmen Paper AB

Shipper

Levererad: 1992
Dödvikt: 5 755 ton
Chartrad till Holmen Paper AB

Transporter

Levererad: 1992
Dödvikt: 5 387 ton
Chartrad till DFDS

Rederiaktiebolaget ECKERÖ

Cyber Risk Management

Jaha, vad är det här nu då!

- YK2
- MRV
- IHM
- GDPR

Och nu:
MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management

Men det här gör vi ju redan?

Rederiaktiebolaget ECKERÖ

Myndigheter och klass

Flaggadministrationer

- Transportstyrelsen, SVERIGE
- Transport- och kommunikationsverket, FINLAND

Klassningssällskap

- Bureau Veritas
- DNVGL
- Lloyds Register

Hamnstatsmyndigheter

- Transportstyrelsen, SVERIGE
- Transport- och kommunikationsverket, FINLAND
- Estonian Maritime administration, ESTLAND

Rederiaktiebolaget ECKERÖ

1.2 ISM DOKUMENTATION

REDERIETS SÄKERHETSORGANISATIONSSYSTEM (SMS)

COMPANY	PAX SHIPS	CARGO SHIPS
COMPANY & SAFETY MANUAL Doc. Mgmt. no: 210.000 Manual describing the company's safety and environmental-protection policy, goals and company organization, instructions/procedures to ensure safe operation, responsibilities and authority, reporting, audits and review.	**COMPANY & SAFETY MANUAL** Doc. Mgmt. no 210.000 Manual describing the company's safety and environmental-protection policy, goals and company organization, instructions/procedures to ensure safe operation, responsibilities and authority, reporting, audits and review.	**COMPANY & SAFETY MANUAL** Doc. Mgmt. no: 210.000 Manual describing the company's safety and environmental-protection policy, goals and company organization, instructions/procedures to ensure safe operation, responsibilities and authority, reporting, audits and review.
EMERGENCY CONTINGENCY MANUAL Doc. Mgmt. no: 210.005 Manual which describes procedures to prepare for, and respond to emergency, critical and specific situations including alerting routines. ISM Code chapter 8	**EMERGENCY CONTINGENCY MANUAL** Doc. Mgmt. no: 210.005 Manual which describes procedures to prepare for, and respond to emergency, critical and specific situations including alerting routines. ISM Code chapter 8	**EMERGENCY CONTINGENCY MANUAL** Doc. Mgmt. no: 210.005 Manual which describes procedures to prepare for, and respond to emergency, critical and specific situations including alerting routines. ISM Code chapter 8
SAFETY TRAINING MANUAL **FIRE TRAINING MANUAL** Doc. Mgmt. no: 210.010 Vessels instructions regarding safety equipment	**SAFETY TRAINING MANUAL** **FIRE TRAINING MANUAL** Doc. Mgmt. no: 210.010 Vessels instructions regarding safety equipment	**SAFETY TRAINING MANUAL** **FIRE TRAINING MANUAL** Doc. Mgmt. no: 210.010 Vessels instructions regarding safety equipment
CHECKLIST BINDER Doc. Mgmt. no: 210.015 Ship specific checklists for safety and operational routines	**CHECKLIST BINDER** Doc. Mgmt. no: 210.015 Ship specific checklists for safety and operational routines	**CHECKLIST BINDER** Doc. Mgmt. no: 210.015 Ship specific checklists for safety and operational routines
DOCUMENT MANAGEMENT SYSTEM **00-Book (departments filing system)** Doc. Mgmt. no: 210.020 Binder which in detail describes the department filing and documentation of operational routines, and instructions for handling of above.	**DOCUMENT MANAGEMENT SYSTEM** **00-Book (vessel filing system)** Doc. Mgmt. no: 210.020 Binder which in detail describes the department filing and documentation of operational routines, and instructions for handling of above.	**DOCUMENT MANAGEMENT SYSTEM** **00-Book (vessel filing system)** Doc. Mgmt. no: 210.020 Binder which in detail describes the department filing and documentation of operational routines, and instructions for handling of above.
SOPEP MANUAL* Doc. Mgmt. no: 210.030	**SOPEP MANUAL*** Doc. Mgmt. no: 210.030	**SOPEP MANUAL*** Doc. Mgmt. no: 210.030
CARGO SECURING MANUAL* Doc. Mgmt. no: 210.035	**CARGO SECURING MANUAL*** Doc. Mgmt. no: 210.035	**CARGO SECURING MANUAL*** Doc. Mgmt. no: 210.035
BALLAST WATER MANAGEMENT PLAN* Doc. Mgmt. no: 210.050	**BALLAST WATER MANAGEMENT PLAN*** Doc. Mgmt. no: 210.050	**BALLAST WATER MANAGEMENT PLAN*** Doc. Mgmt. no: 210.050
EMERGENCY TOWING BOOKLET Doc. Mgmt. no: 210.045	**EMERGENCY TOWING BOOKLET** Doc. Mgmt. no: 210.045	**EMERGENCY TOWING BOOKLET** Doc. Mgmt. no: 210.045
ENVIRONMENT MANAGEMENT MANUAL including SEEMP Doc. Mgmt. no: 225 and 230	**ENVIRONMENT MANAGEMENT MANUAL including SEEMP** Doc. Mgmt. no: 225 and 230	**ENVIRONMENT MANAGEMENT MANUAL including SEEMP** Doc. Mgmt. no: 225 and 230
HULL OPENING OPERATING AND MAINTENANCE MANUAL Doc. Mgmt. no: 210.040	**HULL OPENING OPERATING AND MAINTENANCE MANUAL** Doc. Mgmt. no: 210.040	**HULL OPENING OPERATING AND MAINTENANCE MANUAL** Doc. Mgmt. no: 210.040
SEARCH AND RESCUE CO-OPERATION PLAN Doc. Mgmt. no: 210.025	**SEARCH AND RESCUE CO-OPERATION PLAN** Doc. Mgmt. no: 210.025	**GARBAGE MANAGEMENT PLAN**
Makers instruction and operating manuals Doc. Mgmt. no: 155 and 160	**Makers instruction and operating manuals** Doc. Mgmt. no: 155 and 160	**Makers instruction and operating manuals** Doc. Mgmt. no: 155 and 160
Drawings and plans Doc. Mgmt. no: 160	**Ships drawings and plans** Doc. Mgmt. no: 160	**Ships drawings and plans** Doc. Mgmt. no: 160

* Manual which is to be approved by Flag or RO, no alterations or revisions shall be made without approval.

All other SMS documentation, except makers instructions/operating manuals and drawings, shall be "controlled documents" which means that it is approved and dated as described in chapter 1.3 Revision of manuals.

Ovanstående beskriver schematiskt vilka pärmar som ingår i säkerhetsorganisationssystemet, vilket styr organisationens verksamhet. Rutor med <u>bred</u> ram ingår i rederiets ISM dokumentationssystem, de övriga anger stödmanualer för att beskriva helheten i verksamheten.

Safety Mgmt System

Rederiaktiebolaget ECKERÖ

Fördelar

ISM:

När man tänker efter är det helt logisk att detta implementeras i SMS systemet, ger BFH och övriga befattningshavare befogenheter och ansvar att tillse så rutinerna implementeras och efterföljs

Drift/tekniskt management:

Ger mer enhetliga och säkrare rutiner då nya system sätts ombord eller existerande system uppgraderas.

IS/IT:

Mer befogenheter och möjligheter att styra upp installationer så det görs enligt säkra rutiner med avseende på skyddsmekanismer.

I och med ISM implementeringen ger det även IT avdelningen befogenheter att ge ut info och direktiv som förbättrar IT skyddet.

Rederiaktiebolaget ECKERÖ

Nackdelar

ISM:

Formuleringen av ISM texter; känns svårt och trevande att veta hur man skall formulera rutiner, processer, tillstånd i praktisk text pga att det är så nytt och begränsad tillgång till existerande information. Avgränsningar är också en utmaning.

Drift/tekniskt management:

Kan tänkas att driftsmässiga störningar kan leda till mer tröghet i processerna för att åtgärda problem som uppstår.

IS/IT:

Ansvar för samtliga medarbetare för att verkligen följa rutiner och känna till interna regler gällande säkerhetsaspekter.

Systembeställare både iland och ombord måste känna till rutinerna och ta reda på vad nya system kräver för att fungera i våra system, kräver mer arbete i planerings- och upphandlingsprocessen.

Leder oundvikligen till ett visst merarbete för att kartlägga och system och applikationer samt genomföra riskbedömningar.

Rederiaktiebolaget ECKERÖ

Vad har vi redan på plats?

ISM:

Inom organisationen och ombord finns en vana att ta till sig nya rutiner och regler genom ISM/SMS systemet. Även kännedomen om att nya rutiner måste implementeras samt granskas utifrån av olika myndigheter och genom interna/externa kontrollmekanismer

IS/IT:

Till stor del finns redan skyddsmekanismerna på plats såsom

- Antivirus system
- Brandväggar
- Lösenordshantering

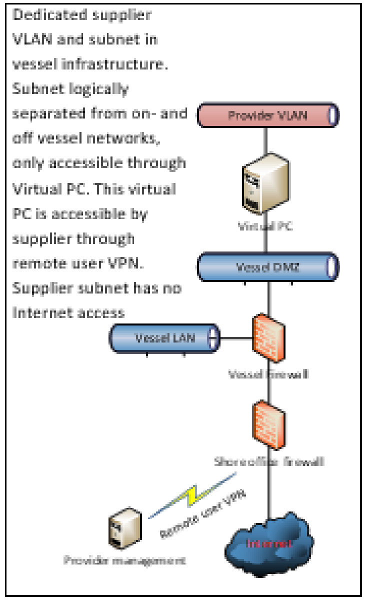
Som en meny på en restaurang

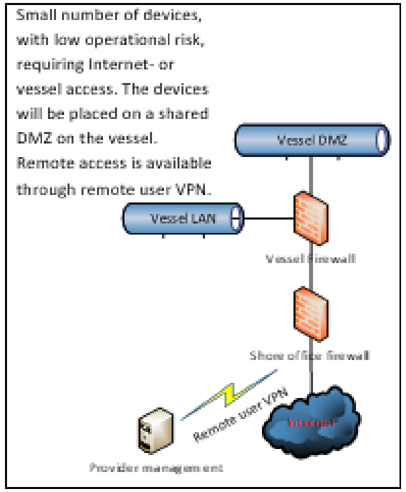
Rederiaktiebolaget ECKERÖ

System name		
Supplier/Manufacturer		
I the system remote controlled?	☐ Yes How?	
System requires Internet connectivity	☐ Yes	Estimated monthly data usage Mbytes
Which services on the Internet are required?		
Internet connection availability requirements (SLA)		%
How critical is the system to the operation of the vessel?		☐ High ☐ Medium ☐ Low

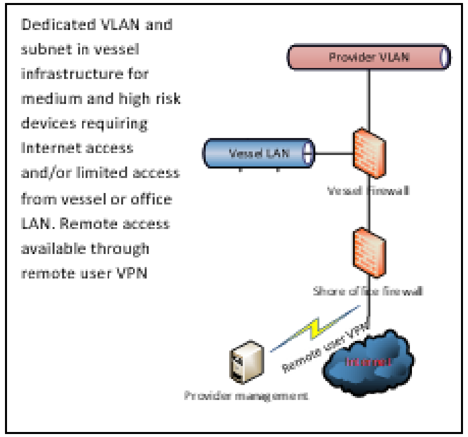
Eckerö contact	
Other system access requirements	

Below are the network connectivity options available to supplier provided equipment.





If the supplier chooses to provide Internet connectivity through a dedicated connection, for example mobile network, it is mandatory the supplier takes necessary measures to prevent unauthorized access to the system.



Menyn:

En enkel blankett som är tänkt att användas då nya system skall läggas till ombord.

Den ger också användarna en enkel överskådlig bild över hur applikationer och system är uppbyggda i förhållande till de olika skyddsmekanismerna.

Vad återstår för att vi skall känna oss redo för nästa DoC besiktning?

ISM:

Formulera text, riktlinjer och regler till ISM/SMS systemet. Överens om att hålla det på en rimlig nivå både vad gäller omfattningen samt språkligt för att personalen skall kunna förstå och ta in informationen.

IS/IT:

Information om implementering och cyber risk management i allmänhet inom landorganisationen samt till fartygen. Kan uppnås genom tex:

- Intranät
- Utbildningar
- Direktiv och information

Rederiaktiebolaget ECKERÖ

Erfarenheter

Information om de nya reglerna

Om vi klarar av att ge ut tydlig information och klara regler och riktlinjer upplevs detta inte som något negativt av användare iland och ombord, utan kan förenkla det dagliga arbetet genom att reda ut många tveksamheter och oklara saker i den dagliga verksamheten idag.

Praktiska enkla åtgärder som behöver förtydligas

USB minnen

Externa leverantörer som ansluter sig på våra system

Utmaning: Dockning av fartyg

Status i frågan inom IMO och EU samt implementering av *Resolution MSC.428(98)* – *Maritime cyber risk management in safety management systems*

Johan Isaksson, Transportstyrelsen

Cyber risk management inom IMO och EU

Svensk Sjöfart 3 Mars, 2020

TRANSPORT
STYRELSEN


NUROFEN
MIGRAINE PAIN
MIGRAINE PAIN
FAST TARGETED RELIEF FROM PAIN
24 CAPLETS
ibuprofen lysine 342mg (equiv. ibuprofen 200mg) AUST R 96215 (capsule shaped tablets)
NUROFEN
NUROFEN
from
2017
The Guardian

Cyber risk management

- Bakgrund – ISM och ISPS
- EU:s arbete – ENISA

✓ Nytt direktiv ”Cybersecurity Act” – 2019/881 (27 juni 2019)

✓ Nytt mandat för ENISA

✓ Krav på Certifiering av ICT produkter

IMO res. MSC.428(98)

- Resolution och riktlinjer
- ✓ Implementering – Genom ISM https://transportstyrelsen.se/sv/sjofart/Fartyg/sjosakerhetsarbete/aktuell-information/
- ✓ Tillsyn – Systemtillsyn genom sedvanlig auditering vid certifiering
  - ➢ Senast genomfört som del av rederiets SMS vid första årliga verifieringen av rederiets DOC efter 1 januari 2021

NIS (EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/1148)

- Tillämpning och omfattning
- MSB och TS
- Rederiers roll
- TS tillsyn inom NIS

Tack för uppmärksamheten!

Frågor?

TRANSPORT
STYRELSEN

Tack!

Missa inte Svensk Sjöfarts öppna årsmötesseminarium 23 april!