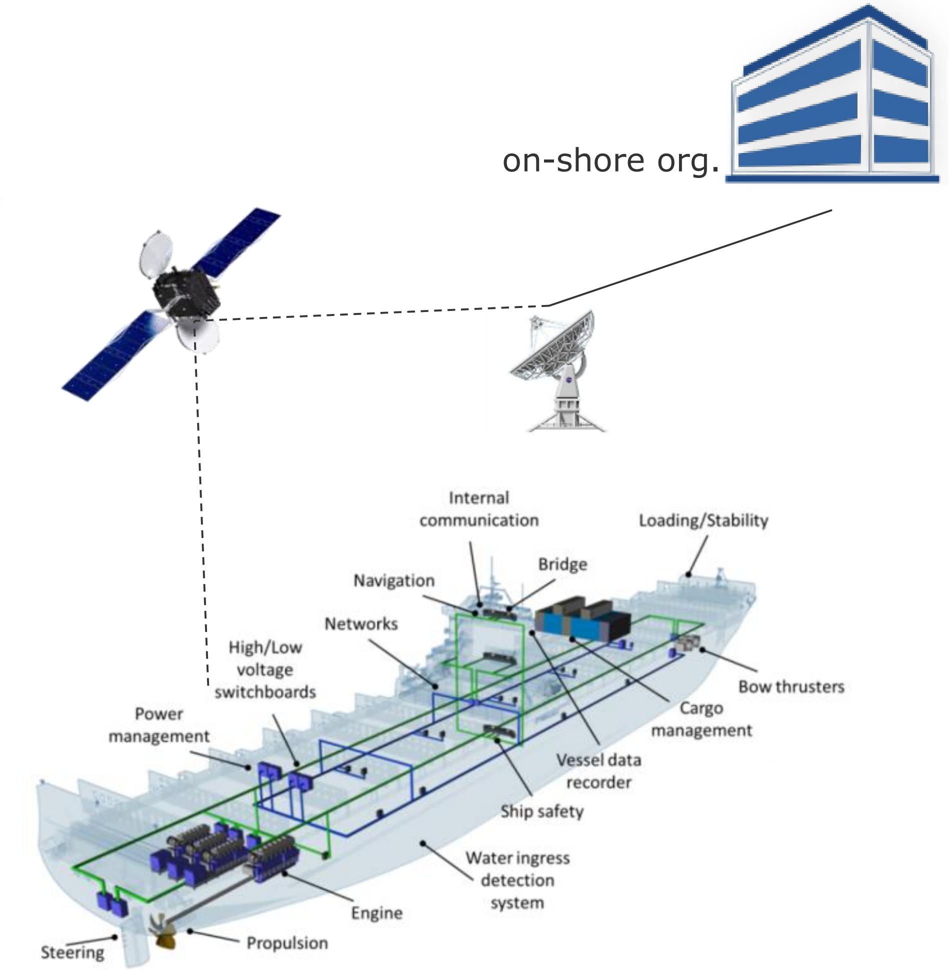
Cyber Risks from the Perspective of a Classification Society

CCNR - Workshop on cybersecurity in inland navigation

Svante Einarsson: Team Leader Cyber Security

05 September 2019

Safety in shipping today heavily depends on cyber systems



Information Technology (IT)

- IT networks
- E-mail
- Administration, accounts, crew lists, …
- Planned Maintenance
- Spares management and requisitioning
- Electronic manuals & certificates
- Permits to work
- Charter party, notice of readiness, bill of lading…

At risk:

Mainly

finance

and

reputation

Operation Technology (OT)

- PLCs
- SCADA
- On-board measurement and control
- ECDIS, GPS
- Remote support for engines
- Data loggers
- Engine & Cargo control
- Dynamic positioning, …

At risk:

Life,

property

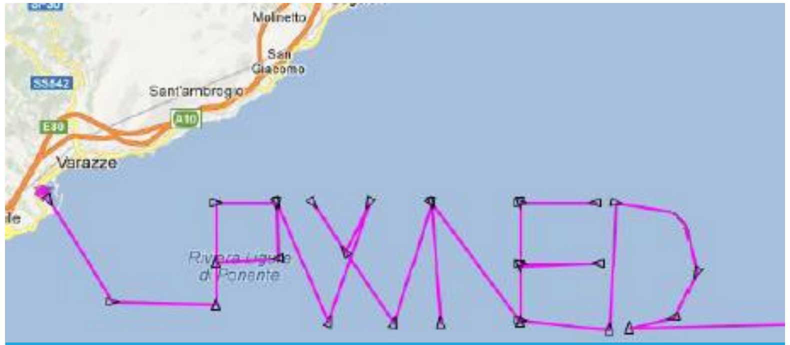
and

environment

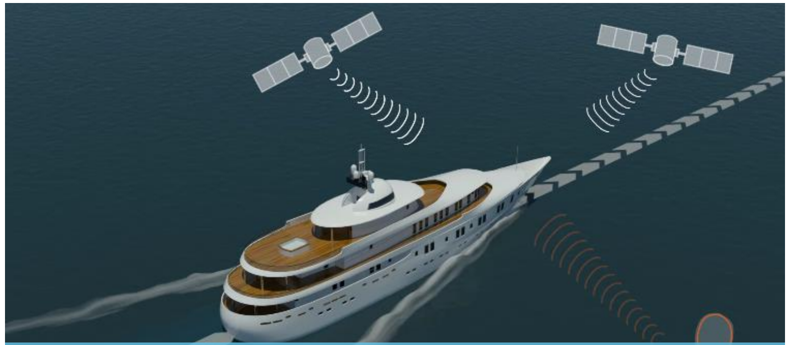
+

all of the above

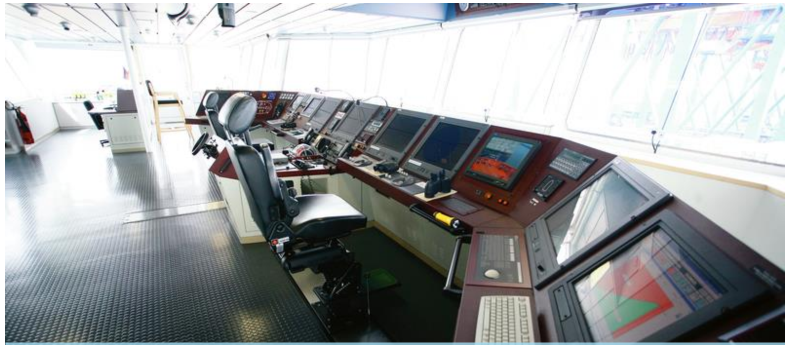
The cyber threat to ship, its crew and environment



AIS Spoofing



GPS Jamming of Spoofing



ECDIS ransomware & chart spoofing

ECDIS updating resulting in loss of fuel control & ballast water valves

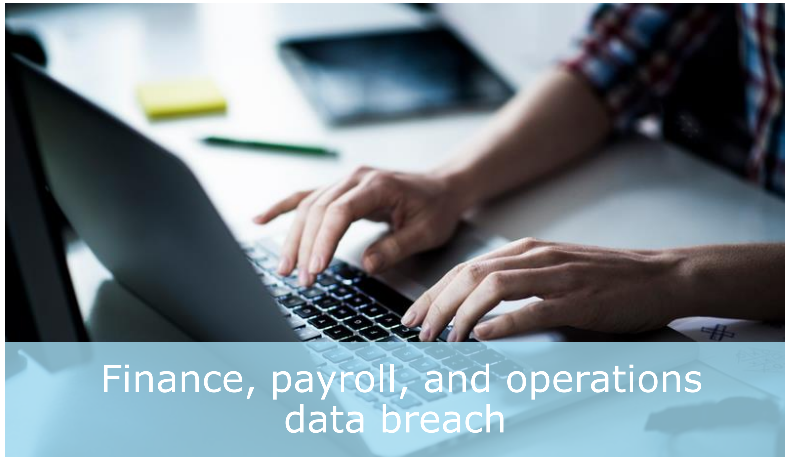
Hackers took "full control" of navigation systems for 10 h

Loss of main switchboard due to ransomware

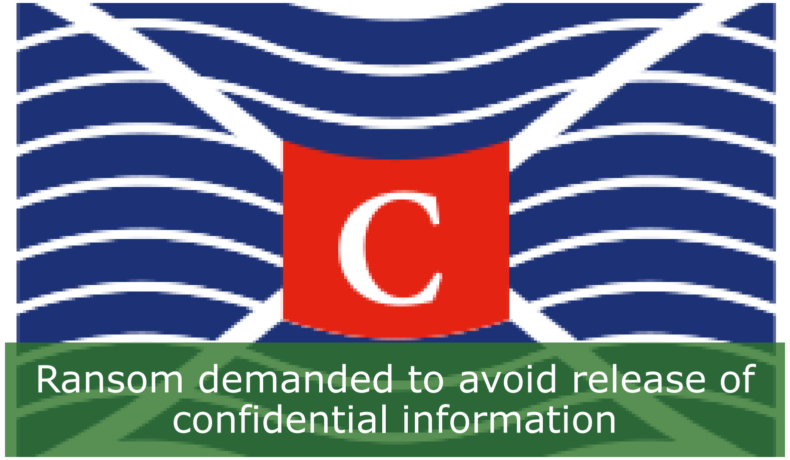
The cyber threat also includes risks to the enterprise

Hacking of cargo tracking system for smuggling purposes

Pirate attack supported by cyber attack



Finance, payroll, and operations data breach



Ransom demanded to avoid release of confidential information

NotPetya cyber attack hits corporate earnings

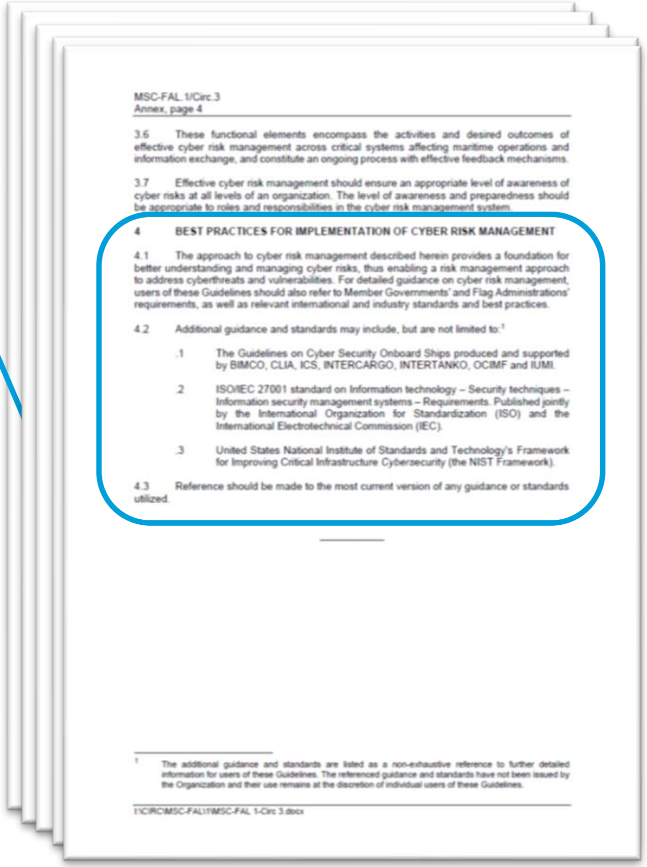
- Maersk hit by cyber attack on Tuesday 27th June.
- Via an update to an accounting system in Ukraine
- Spread like a worm from an infected machine
- Global network is infected & all company systems down
- Forced to halt operations at 76 port terminals
- Reinstall 4000 servers, 45000 PCs, & 2500 applications
- Impact to earnings: $200 to 300m (mainly Maersk Line)
- NotPetya was not targeted specifically for Maersk
- Vulnerability fix by Microsoft on March 14th (MS17-010)

Cyber security regulations are evolving…
i.e. IMO Resolution MSC.428(98)

- AFFIRMS that … **safety management system should take into account cyber risk management** in accordance with the ISM Code.
- Where to start: MSC-FAL.1/Circ.3
  - IT and OT systems
  - Identify – Protect – Detect – Respond – Recover
  - referring to international best practices
- However, not addressing:
  - how to assess the risk,
  - prescriptive or goal-based safety requirements,

Impact:
Cyber risks should be addressed in safety management systems no later than the first annual verification of DoC after 1 January 2021. This is a non-mandatory requirement.

Outcome:
MSC 98 adopted recommendatory MSC-FAL.1/Circ.3 superseding the interim guidelines



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 management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' 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 for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

4.3 Reference should be made to the most current version of any guidance or 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.

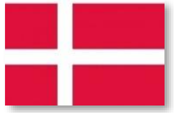
I:\CIRC\MSC-FAL\1\MSC-FAL 1-Circ 3.docx

Flag states requriements are developing

- USCG CG-5P Policy Letter No. 08-16 require incident reporting (Dec 2016)
- The Coast Guard Blog for Maritime Professionals, 2017-06-30: IMO approves resolution on cyber risk management

- Marshall Islands - Marine Guideline No. 2-11-16 affirms MSC.428(98) (April 2018)

- BG Verkehr ISM Cyber Security affirms MSC.428(98) (June 2018)



- Danish Maritime Authority - Order no. 46 makes MSC.428(98) and MSC-FAL.1/Circ.3 mandatory (January 2019)

- Norwegian Maritime Athority – News article: Cyber risks in the maritime sector, 2019-08-19, require cyber risk management according to ISM code

- Data Processing and Cybersecurity Notification Obligation Act (Jan 2016)

- Irish Department of Transport, Tourism and Sport affirms MSC.428(98) (March 2018)

- Maritime and port authority of Singapore affirms MSC.428(98) as quickly as possible, no later than 1st of Jan 2021

- Indian Ministry of Shipping – ENGG. Circ. No.06 of 2017 makes MSC.428(98) and MSC-FAL.1/Circ.3 mandatory from 1st of Jan 2021

- Hong Kong Merchant Shipping Information Note No 40/2017 affirms MSC.428(98)

Commercial stakeholder requirements

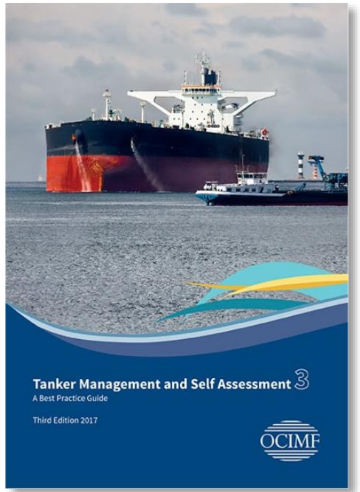
Releases cyber security clause

(2019-06-04)

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

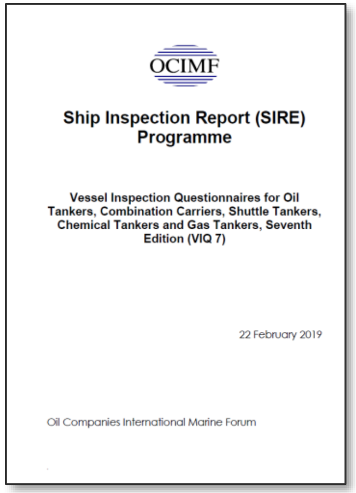
The tanker sector leading the way on cyber security



Tanker Management and Self Assessment 3
A Best Practice Guide

Third Edition 2017

OCIMF



OCIMF

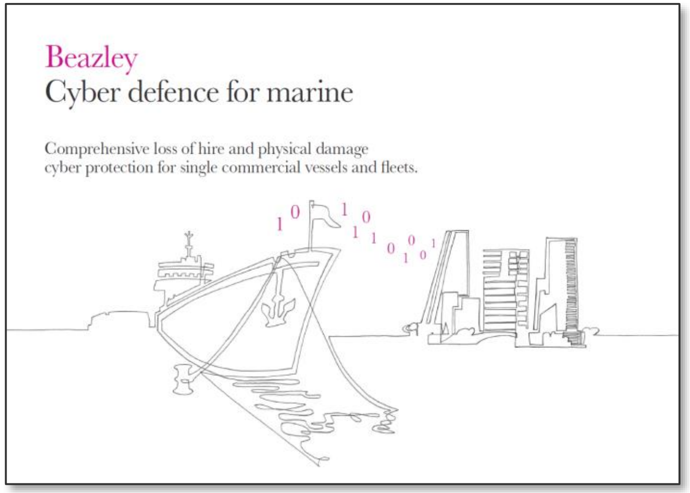
Ship Inspection Report (SIRE) Programme

Vessel Inspection Questionnaires for Oil Tankers, Combination Carriers, Shuttle Tankers, Chemical Tankers and Gas Tankers, Seventh Edition (VIQ 7)

22 February 2019

Oil Companies International Marine Forum

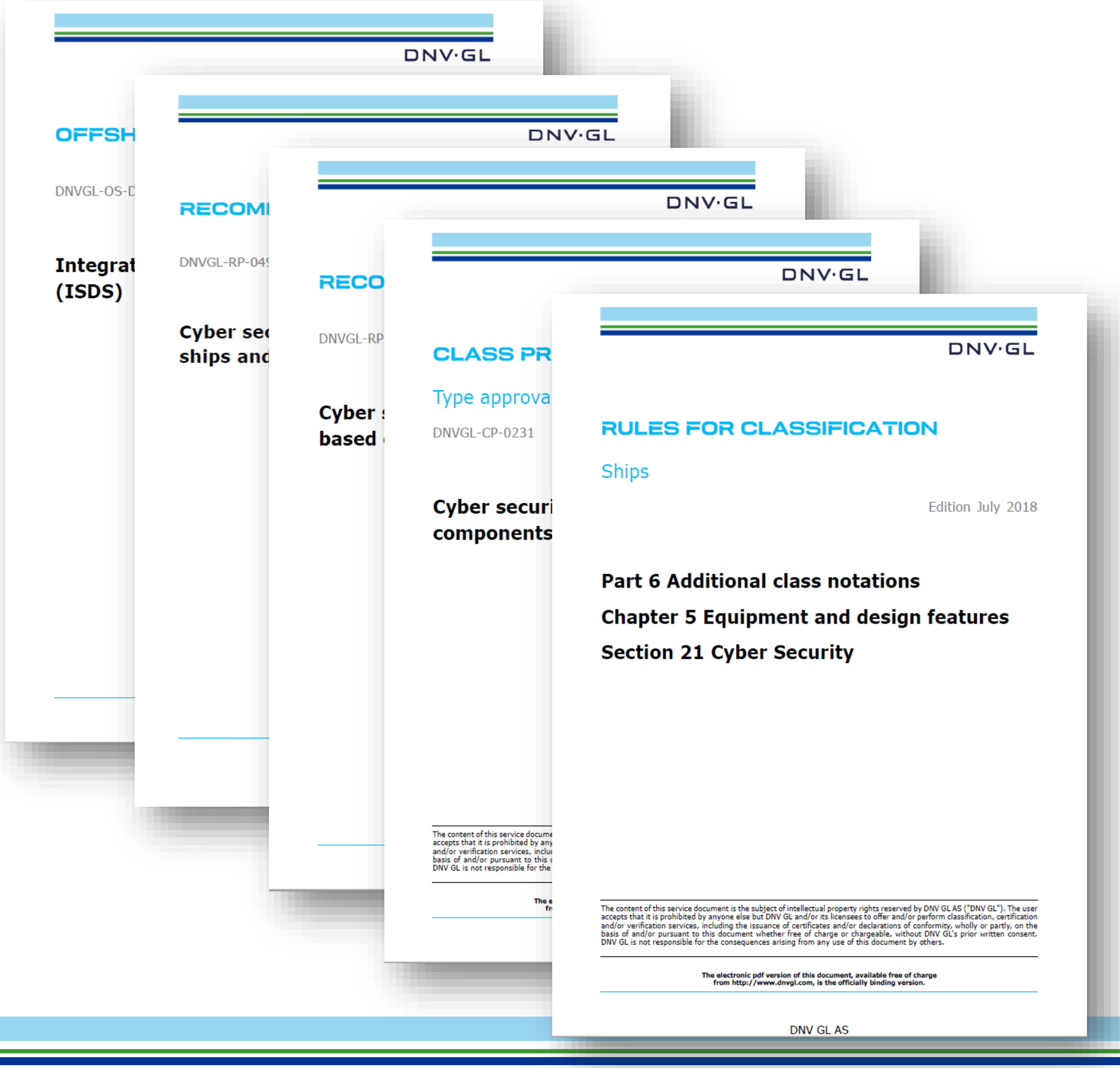
The insurance sector starting to provide cyber cover



Beazley
Cyber defence for marine

Comprehensive loss of hire and physical damage cyber protection for single commercial vessels and fleets.

...and DNV GL has follow-up with additional support



DNV·GL

OFFSH

DNVGL-OS-D

Integrat
(ISDS)

DNV·GL

RECOMI

DNVGL-RP-049

Cyber sec
ships and

DNV·GL

RECO

DNVGL-RP

Cyber
based

DNV·GL

CLASS PR

Type approva

DNVGL-CP-0231

Cyber securi
components

DNV·GL

RULES FOR CLASSIFICATION

Ships

Edition July 2018

Part 6 Additional class notations

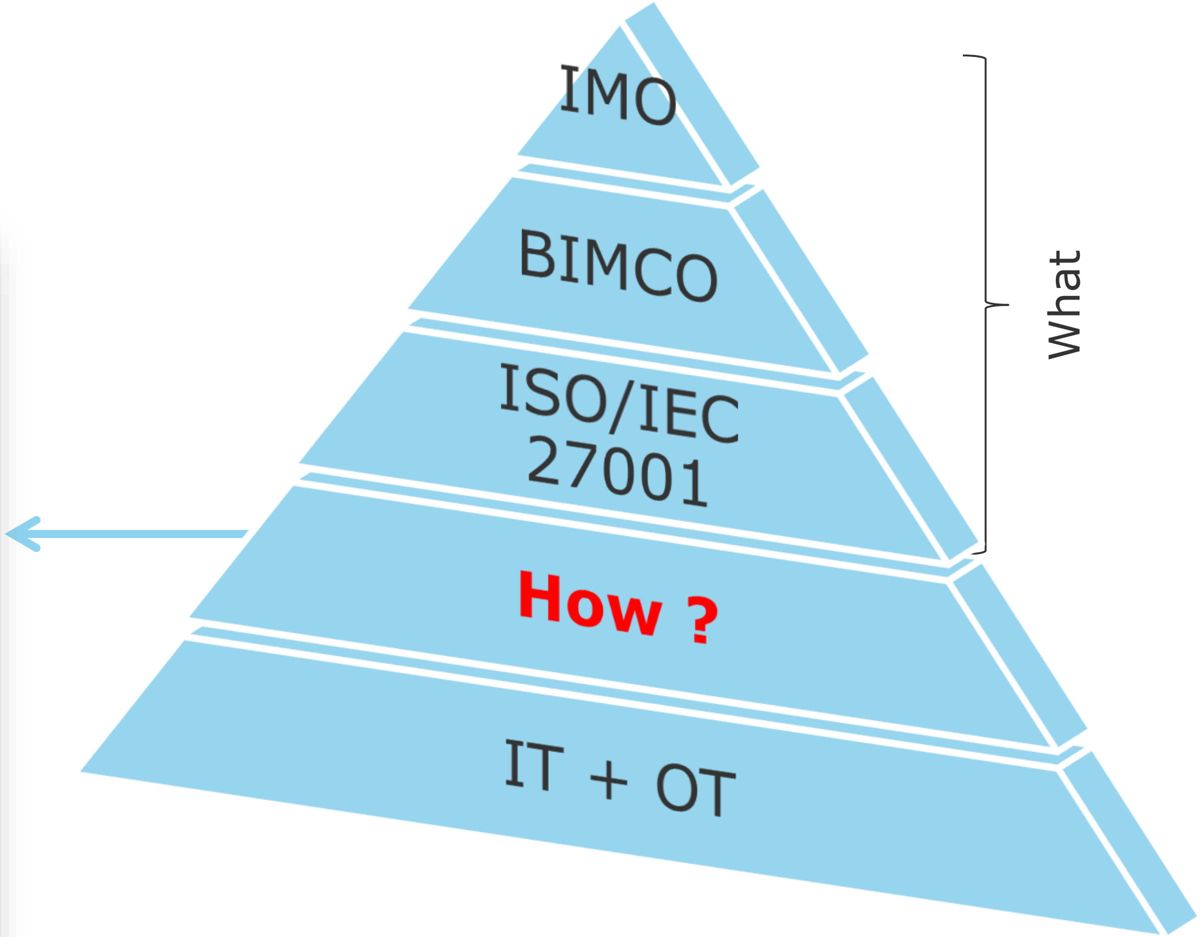
Chapter 5 Equipment and design features

Section 21 Cyber Security

The content of this service document is the subject of intellectual property rights reserved by DNV GL AS ("DNV GL"). The user accepts that it is prohibited by anyone else but DNV GL and/or its licensees to offer and/or perform classification, certification and/or verification services, including the issuance of certificates and/or declarations of conformity, wholly or partly, on the basis of and/or pursuant to this document whether free of charge or chargeable, without DNV GL's prior written consent. DNV GL is not responsible for the consequences arising from any use of this document by others.

The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

DNV GL AS



All Three Pillars of Cyber Security must be addressed

People

- Training & Awareness
- Professional skills & qualifications
- Emergency drills
- Authorizations & authentication
- Physical Security

Technology

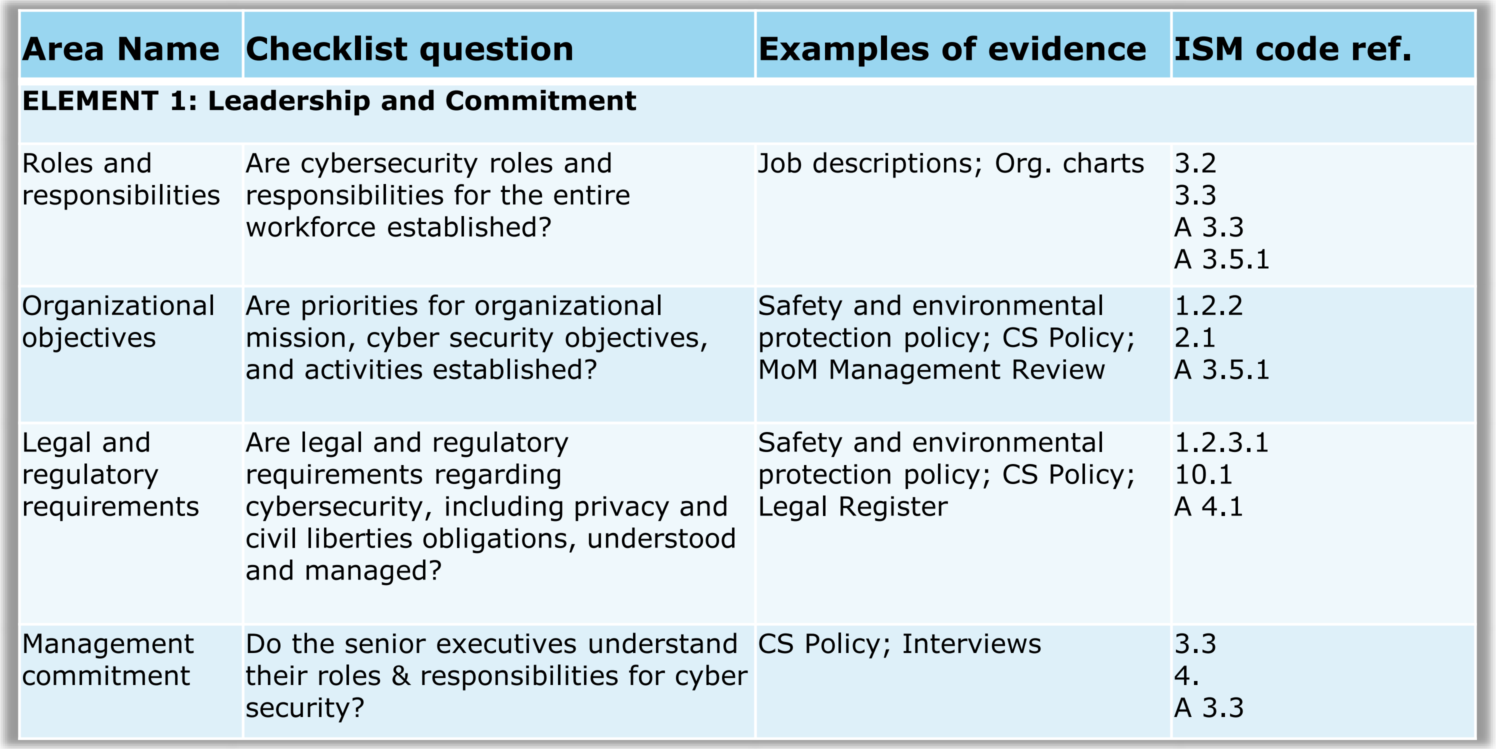
- System design
- Hardening of connections
- Software configuration
- Encryption protocols
- Jamming & spoofing
- Detection & monitoring

Process

- Management Systems
- Governance Frameworks
- Policies & procedures
- Vendor/Third party contracts-follow up
- Audit regimes

DNV GL Cyber Security ISM audit checklist (to be released in fall of 2019)

- Check list elements:
  1. Leadership and commitment
  2. Identify
  3. Protect
  4. Detect
  5. Respond
  6. Recover
  7. Continous improvement
- ~ 25 areas
- ~ 75 topics

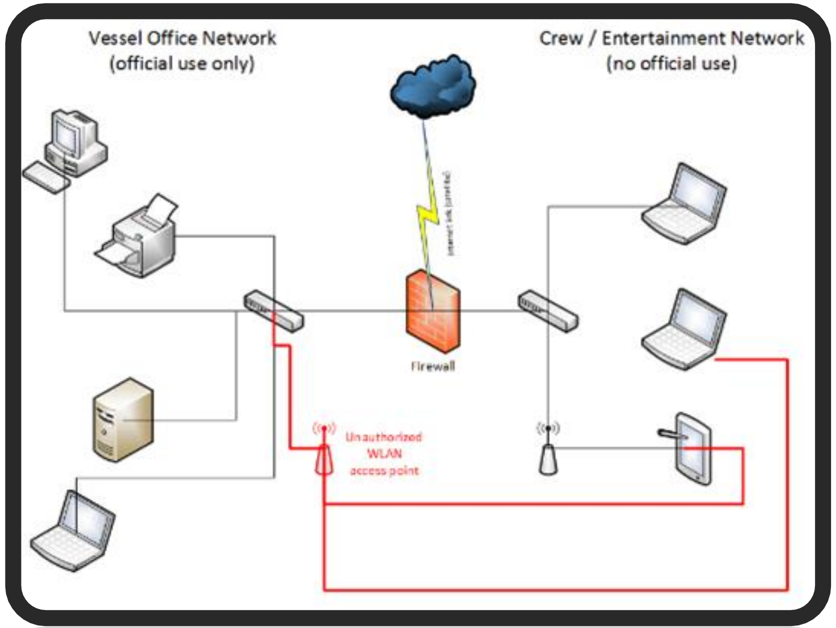


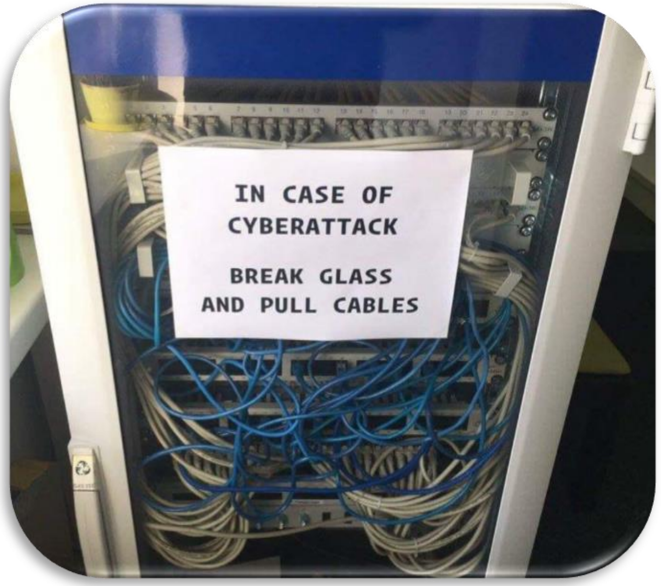
Area Name	Checklist question	Examples of evidence	ISM code ref.
ELEMENT 1: Leadership and Commitment			
Roles and responsibilities	Are cybersecurity roles and responsibilities for the entire workforce established?	Job descriptions; Org. charts	3.2 3.3 A 3.3 A 3.5.1
Organizational objectives	Are priorities for organizational mission, cyber security objectives, and activities established?	Safety and environmental protection policy; CS Policy; MoM Management Review	1.2.2 2.1 A 3.5.1
Legal and regulatory requirements	Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?	Safety and environmental protection policy; CS Policy; Legal Register	1.2.3.1 10.1 A 4.1
Management commitment	Do the senior executives understand their roles & responsibilities for cyber security?	CS Policy; Interviews	3.3 4. A 3.3

Benefit: providing concrete requirements to uniformly check cyber security resiliance and compliance with the IMO Resolution MSC.428(98) and the ISM Code

Examples of findings

- Unsafe behaviour
- Disaster recovery scenarios do not include cyber attacks
- Firewall mounted in engine performance monitoring cabinet, but not connected





Rules are based on IEC 62443 series

DNV GL Cyber Secure class notation

Cyber Secure (Basic)

Target: Operational vessels

Security: Level **1** *(Marinized IEC 62443-3-3)*

Protection: Minimum

Rationale: Security via people, processes & existing systems (technology)

Cyber Secure (Advanced)

Target: New building vessels

Security: Level **3** *(Marinized IEC 62443-3-3)*

Protection: Higher

Rationale: Security via people, processes & integration of systems into the design

Cyber Secure (+)

Can be combined with Basic and Advanced

Target: Operational & new building vessels

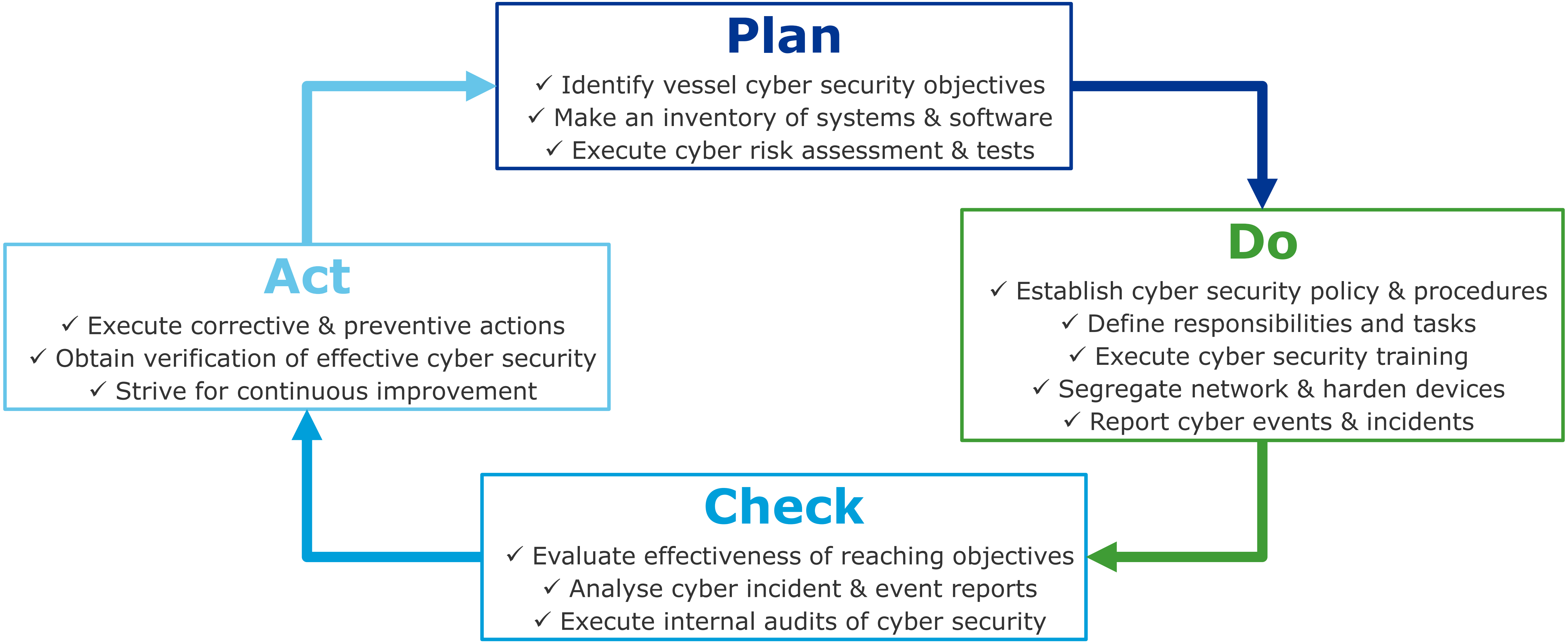
Security: defined by risk assessment

Protection: defined by risk assessment

Rationale: Security of additional target system(s) based on client needs

SL1	Protection against casual or coincidental violation	**SL3**	Protection against intentional violation using sophisticated means, moderate resources, OT system specific skills, moderate motivation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation	**SL4**	Protection against intentional violation using sophisticated means, extended resources, OT system specific skills, high motivation

How to manage your cyber risks



Plan

- ✓ Identify vessel cyber security objectives
- ✓ Make an inventory of systems & software
- ✓ Execute cyber risk assessment & tests

Do

- ✓ Establish cyber security policy & procedures
- ✓ Define responsibilities and tasks
- ✓ Execute cyber security training
- ✓ Segregate network & harden devices
- ✓ Report cyber events & incidents

Check

- ✓ Evaluate effectiveness of reaching objectives
- ✓ Analyse cyber incident & event reports
- ✓ Execute internal audits of cyber security

Act

- ✓ Execute corrective & preventive actions
- ✓ Obtain verification of effective cyber security
- ✓ Strive for continuous improvement

Thank you for your attention!

For further information please contact:

Svante Einarsson

Team Leader Cyber Security

Svante.einarsson@dnvgl.com

www.dnvgl.com

SAFER, SMARTER, GREENER