Focus Area: Cyber Security Risk (Rev. 7 – 08.05.2020)

This protocol has been developed to support in the focus-based auditing process having the focus on measures and procedures for managing Cyber Security Risks as per the ISM Code, cf. IMO Resolution MSC 428(98) mandating cyber risk to be managed through the ISM Code and the corresponding Safety Management Systems.

- It must be noted that the IMO has decided that: **A risk management approach to cyber risks** should be resilient and **evolve as a natural extension of existing safety and security management practices.**

We do expect Doc-Holders have existing measures in their SMS enabling them to handle Cyber Security as a natural extension. To be effective, the starting point should be the existing SMS measures and a revision of these as need be.

In the audits, we will, as RO:

1. Stick to verifying the effectiveness of the management system in ensuring ongoing compliance and continuous improvement in reaching goals and handling requirements set by the Code and/or required by the flag States. Accordingly, this protocol is **not** intended to cover all issues raised by cyber security experts and we recommend noting the IMO's statement that:

   - *No two organizations are the same...*
     - *Ships with limited cyber-related systems may find a simple application of the IMO Guidelines to be sufficient (Cf. IMO MSC-FAL.1/Circ.3)*
     - *Ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners*

2. Follow audit systematics as in DNVGL instructions as RO and have cyber security as a focus area in 2020 and 2021 DOC audits, seek information on amendments for review in advance of the audit, suggest to have cyber security as a natural focus area in shipboard audits in 2021 and in both in DOC and shipboard audits beyond 2021.

3. Stress the importance of SMS measures and audit focus setting being based on DOC holder performance and needs and recommend using existing SMS as a starting point

4. Ensure that we cover scopes and that focus areas are part of the audit as per DNVGL instructions as RO.

In support of the industry and noting the above DNV GL has additional services on cyber security, i.e. from Class (Class notation "Cyber) or from Advisory services (though these will **not** be handled as part of the audits we perform as RO).

Audit question	Comments	Company / Ship Applica-bility	Finding	Action
Objectives for cyber security management				
How does the top management demonstrate compliance with objectives of the Code in respect to cyber security?	Management should demonstrate how they have placed and are handling cyber security in the SMS remembering: *"The objectives of the Code are to ensure safety at sea, prevention of human injury or loss of life, and avoidance of damage to the environment, in particular, to the marine environment, and to property."*	C		

How is the Company handling cyber security in relation to the objective of provide for safe practices in ship operation and a safe working environment?		C/S		
How is the Company handling cyber security in relation to the objective of assessing all identified risks to its ships, personnel and the environment and establish appropriate safeguards?	We will take it that DOC Holders have a systematic for risk assessment and that they have a systematic for implementing appropriate safeguards The auditor shall ensure that this is used also on cyber risk Note that we will not approve the risk evaluation	C/S		
How is the Company handling cyber security in relation to the objective continuously improve safety management skills of personnel ashore and aboard ships, including preparing for emergencies related both to safety and environmental protection?	Management systems skills must also be used to ensure that the safety management system handles cyber security. There are many ways of doing this, but the DOC Holder must be able to document how they are doing this. As examples; courses, training, familiarization, drills and lessons learned	C/S		
How is the Company ensuring compliance with mandatory rules and regulations regarding cyber security?	This is a standard objective and DOC Holders must be able to systematically identify regulations. On cyber security the IMO has adopted Resolution SC.428(98) as a basis for the focus on cyber security and flag States may have additional requirements or guidance. Identify if the DOC Holder has a system for and if they identified the above.	C/S		
How is the Company ensuring that applicable codes, guidelines and standards recommended by the Organization, Administrations, classification societies and maritime industry organizations regarding cyber security are taken into account?	See above	C		
Which policies and measure are in place in the Safety Management System to identify and handle cyber security issues?		C/S		
How is the Company ensuring that the policies and measure regarding cyber security are implemented and maintained at all levels of the organization, both ship based as well as shore based?	Implementation and maintenance of measures and ensuring they are effectively handled is critical. There are many ways of doing this, but the DOC Holder must be able to document how they are doing this. Identifying performance indicators and following up on them is critical. Further follow up, as examples; monitoring, internal audits, inspection routines, information feedback, courses, training, familiarization, drills and lessons learned	C/S		
How is the company ensuring that data privacy measures are developed and implemented?	Note: personal data of persons on EU flagged vessels falls under the General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679	C/S		

Critical Equipment: Risk Assessment & Systems to be covered				
How is the company ensuring that cyber security risk assessments are being conducted?	The risk assessment company procedure should contain guidance as to how to perform cyber risk assessments, not only for the office locations but also for the vessels	C/S		
How has the Company identified equipment and technical systems (and cyber risks connected with them) the sudden operational failure of which may result in hazardous situations?	Has the company identified Operational Technology (OT) (and cyber risks connected with them) for which a sudden operational failure may result in hazardous situations? Have risk assessment been performed and appropriate safeguards been taken for such OT: Equipment and systems	C/S		
How is the Company ensuring that critical equipment which may be impacted by cyber security challenges are identified?		C/S		
How is the SMS providing for specific measures aimed at promoting the reliability of such equipment or systems?		C/S		
Are these measures including regular testing of stand-by arrangements and equipment or technical systems that are not in continuous use?		C/S		
Have cyber security issues, at least in relation to the following systems, been assessed: 1. Bridge systems?	Cf. IMO MSC-FAL.1/Circ.3 Company should have identified their bridge systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards As examples; Navigation – e.g. Radar AIS GPS ECDIS Compass Gyro Heading and bearing indicator BNWAS Echo sounder Electronic plotting Speed and distance measuring device Tracking aid Rate of turn indicator & transmitting heading device. Integrated systems/maneuvering systems	C/S		

2. Cargo handling and management systems?	Cf. IMO MSC-FAL.1/Circ.3 Company should have identified their cargo handling systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards As examples: Ballasting – e.g. ballast valves, pumps and levels gauges Cranes/ramps	C/S		
3. Propulsion and machinery management and power control systems?	Cf. IMO MSC-FAL.1/Circ.3 Company should have identified their propulsion and machinery management and power control systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards As examples: Propulsion – e.g. CPP, RPM, electrical thrusters and related electrical drives. Steering – e.g. rudder, azimuth thrusters and related electrical drives. Thrusters not part of propulsion functions – e.g. auxiliary thrusters Power generation supplying essential and important systems – e.g. main and auxiliary engine, generator and electrical power management Auxiliary systems for essential and important systems – e.g. cooling, fuel, lube oil, compressed air and ventilation	C/S		
4. Access control systems?	Cf. IMO MSC-FAL.1/Circ.3 Company should have identified their access control systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards	C/S		
5. Passenger servicing and management systems?	Cf. IMO MSC-FAL.1/Circ.3 Company should have identified their passenger servicing and management systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards	C/S		

6. Passenger facing public networks?	Cf. IMO MSC-FAL.1/Circ.3 Company should have identified their passenger facing public networks and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards	C/S		
7. Administrative and crew welfare systems?	Cf. IMO MSC-FAL.1/Circ.3 Company should have identified their administrative and crew welfare systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards	C/S		
8. Communication systems?	Cf. IMO MSC-FAL.1/Circ. Company should have identified their administrative and crew welfare systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards As examples: Communication – e.g. distress alert, EPIRB, public announcement, general alarm, satellite communication, wireless communication and integrated network communications systems/VSAT/VPN.	C/S		
9. Safety systems	Company should have identified their safety systems and identified whether these are subject to cyber security risks and as necessary implemented appropriate safeguards Watertight integrity – e.g. internal watertight doors and shell doors Fire detection and mitigation – e.g. fire detection & alarm system and fire pumps Fire dampers Smoke extraction systems/sprinkler systems/MES(Marine Evacuation systems)			

For each of the systems (above 1 – 8) assessed, which measures are in place to: • **Identify cyber security issues?**	Define personnel roles and responsibilities for cyber risk management Identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations. Cover both Operational Technology (OT) and Information Technology (IT) Cf. IMO MSC-FAL.1/Circ.3	C/S		
For each of the systems (above 1 – 8) assessed, which measures are in place to: • **Protect systems and solutions from cyber security threats**	Implement risk control processes and measures • Anti-virus maintained • Software updates • Access control and authorization • Firewalls • Personal and entertainment systems separated from shipboard system • USB control • Control of interfaces • Back-up and • Contingency planning to protect against a cyber-event and ensure continuity of shipping operations. Cf. IMO MSC-FAL.1/Circ.3	C/S		
For each of the systems (above 1 – 8) assessed, which measures are in place to: • **Detect cyber-events**	Develop and implement activities necessary to detect a cyber-event in a timely manner Cf. IMO MSC-FAL.1/Circ.3	C/S		
For each of the systems (above 1 – 8) assessed, which measures are in place to: • **Respond to Cyber-events**	Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event. Cf. IMO MSC-FAL.1/Circ.3	C/S		
For each of the systems (above 1 – 8) assessed, which measures are in place to: • **Recover**	Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event. Cf. IMO MSC-FAL.1/Circ.3	C/S		
How is the company ensuring that risks related to equipment disposal, including data destruction are mitigated?	e.g.: - handling of data on company cell phones, IT equipment - Deletion of data before disposal of equipment	C/S		

Responsibilities and Authority				
Has the Company defined and documented the responsibility, authority and interrelation of all personnel who manage, perform and verify work relating to and affecting safety and pollution prevention, including for cyber security?	Has the company identified and documented who is responsible for and has the authority in handling measures regarding cyber security? Has the company identified and documented the relations between those who are responsible for and has the authority in handling measures regarding cyber security? As examples: Updating • Authorization matrix • Job descriptions • System Admin rights • Responsibility for log in accounts/authentication; • Responsibilities for updating licences and software updates.	C/S		
How is the Company ensuring that adequate resources and shore-based support are provided to enable the designated person or persons to carry out their functions, also relating to cyber security?	Company should be able to document resources designated for handling SMS measures on cyber security As examples: IT-experts, budget items and time allotted for implementation and maintenance of SMS measures	C		
How is the Company ensuring that there is a link between the company and those on board on cyber security matters?	Company should be able to document SMS measures ensuring needed links on cyber security and who are authorized and responsible for ensuring this ashore and on board Roles and responsibilities and reporting lines should be clearly defined	C/S		
How has the Company defined and documented the Master's responsibility regarding: .1 the cyber security measures in the Safety Management System?		C/S		
How has the Company defined and documented the Master's responsibility regarding: .2 motivating the crew in the observation of the measures?	Safety meetings/during inspection rounds/during cyber security drills/briefings	C/S		
How has the Company defined and documented the Master's responsibility regarding: .3 issuing orders and instructions on cyber security in a clear and simple manner?		C/S		

How has the Company defined and documented the Master's responsibility regarding: .4 verifying that requirements on cyber security are observed?		C/S		
How has the Company defined and documented the Master's responsibility regarding: .5 periodically reviewing the SMS and reporting its deficiencies to the shore based management?		C/S		
Has the Company, in the SMS, established that the master has the overriding authority and the responsibility to make decisions with respect to safety and pollution prevention, including on cyber security, and to request the Company's assistance as may be necessary.	How is the authority identified in the SMS and how is the master supported in using this authority?	C/S		
RESOURCES AND PERSONNEL				
How is the company ensuring that the master is fully conversant with the Company SMS, including on cyber security?		C/S		
How is the company ensuring that the master given the necessary support so that the master's duties can be safely performed?		C/S		
Training and Awareness				
How is the company ensuring that training on cyber-security issues are included in the training plans?	Training should consider the different roles, responsibilities and authorities of the organisation.	C/S		
How is the company ensuring that necessary training resources are defined and made available?	Which training are identified and how are training needs ensured? As examples: Training plans Training budgets Training deliveries Competency requirements for training providers Training goals Verification of training goal achievement	C/S		
How is the company ensuring that training deliveries are documented?		C/S		

Shipboard Operations				
How has cyber security been included in procedures, plans and instructions, including checklists as appropriate, for key shipboard operations concerning the safety of the personnel, ship and protection of the environment?	Company should be able to document changes in the mentioned measures and that there is a link to the risk assessment performed Note that the needs may vary As examples: Navigation/engine operations/deck and cargo operations: **physical barriers & procedural barriers** (*patching, access cards, locked cabinets, maintenance scans, "human firewall",..)* ***ship barriers:*** *protect the connection between zones & systems with remote access (VPN, DMZ, …), segregation (firewalls, data diodes, …)* ***system barriers*** *(protect the individual system with barriers such as encryption, user control and authentication, removable devices, event logging, backup and recovery, etc); segregation of your networks*	C/S		
Have various tasks, regarding cyber security in shipboard operations, been defined and assigned to qualified personnel?	Has the Company identified needed tasks, regarding cyber security in shipboard operations? Has the company identified and documented who is responsible for and has the authority in handling the various tasks regarding cyber security in shipboard operations? Has the company assigned these tasks to qualified personnel? Has the company identified requirements for and how to be qualified for handling these tasks? As examples: Updating • Authorization matrix • Training matrix • Job descriptions • System Admin rights • Responsibility for log in accounts/authentication; • Responsibilities for updating licences and software updates.	C/S		
Emergency Response				
Has the Company identified potential emergency shipboard situations, which may be caused by cyber security challenges, and established procedures to respond to them?		C/S		
Has the Company covered cyber security in their programmes for drills and exercises to prepare for emergency actions?		C/S		

Does the Company, in the SMS, have measures ensuring that the Company's organization can respond at any time to cyber security hazards, incidents and emergency situations involving its ships?		C/S		
Reports and Analysis of Non-Conformities, Accidents and Hazardous Occurrences				
Where in the Safety Management System are there procedures ensuring that non-conformities, accidents and hazardous situations, also related to cyber security, are reported to the Company, investigated and analysed with the objective of improving safety and pollution prevention	How is the reporting system revised to ensure reporting of cyber security incidents? How is the SMS revised in order to ensure that staff ashore and onboard know what to report and how to report cyber security incidents? How is the SMS revised to ensure handling of reported cyber security incidents? Who is responsible for handling reports and follow ups? How is the objective of improving the SMS based on the reports and analysis ensured? Statistics on cyber incidents	C/S		
Where in the Safety Management System are procedures for the implementation of corrective action, including measures intended to prevent recurrence?	Who is responsible for this and how is it followed up by management? Master's review Management review			
Documentation				
Has the Company established, and can they document maintenance of procedures to control all documents and data which are relevant to the SMS, including on cyber security?		C/S		
How is the company ensuring that valid documents are available at all relevant locations?		C/S		
How is the company ensuring that changes to documents are reviewed and approved by authorized personnel?		C/S		
How is the company ensuring that obsolete documents are promptly removed?		C/S		
Company Verification, Review and Evaluation				
How is the company ensuring that cyber security is included in the internal safety audits on board and ashore, at intervals not exceeding twelve months to verify whether safety and pollution-prevention activities comply with the safety management system?	Note that: In exceptional circumstances, this interval may be exceeded by not more than three months.	C/S		

How is the company ensuring that cyber security is included when they periodically verify whether all those undertaking delegated ISM-related tasks are acting in conformity with the Company's responsibilities under the Code?		C/S		
How is the company ensuring that cyber security is included when they periodically evaluate the effectiveness of the SMS in accordance with procedures established by the Company?		C/S		
Are the audits and possible corrective actions carried out in accordance with documented procedures?		C/S		
How is it ensured that personnel carrying out audits are; unless this is impracticable due to the size and the nature of the Company, independent of the areas being audited?		C/S		
How is it ensured that the results of the audits and reviews, including on cyber security, are brought to the attention of all personnel having responsibility in the area involved?		C/S		
How is it ensured that the management personnel responsible for the area involved take timely corrective action on deficiencies found?		C/S		