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.

IDENTIFY[20]

Roles and responsibilities[21]			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
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.	Safety and Quality policy exists. Update to include cyber specifics	Introduction of Security Policy SMS/Company & Policies/1.5 S&Q policy SMS/Fleet Ops/ 1.5.1 Purpose SSP /3.3 risk assessment (SAF 02)
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.	SSP and VMS to specifically describe responsibilities for cyber management.	SMS/Fleet Ops/1.5.7 Master responsibility CSP 1.5 roles and responsibilities SSP / 2.2 Responsibilities
ISM Code: 6.5 Industry Guidelines: 5.2 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for: - all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures - company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.	Verify that training is mandatory. Supplement with additional bulletins/posters etc	CRW 23 ; Voyage Pack CSP 2.10

Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
ISM Code: 10.3 Industry Guidelines: 3 & 4 Using existing company procedures, identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.	An approved SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should already have been documented in an approved SMS. However, an approved SMS, which incorporates CRM will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact on safety and protection of the environment as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems, should be supplemented by a list of the data used by those systems and its source(s).	Critical equipment decision flowchart – is cyber critical?	SMS/Fleet Ops/Technical procedures/4.13 Critical equipment Vessel form/Technical forms/TEC18

[20] Identify, Protect, Detect, Respond and Recover as described in the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[21] Functional element from the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[22] For the purpose of this annex, “critical systems” means the OT, IT, software and data the sudden operational failure or unavailability of which is identified by the company as having the potential to result in hazardous situations.

PROTECT

Implement risk control measures			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
ISM Code: 1.2.2.2 Industry Guidelines: 5 and Annex 1 Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.	The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in these guidelines. As a baseline, the following measures should be considered before a risk assessment is undertaken. The baseline consists of the technical and procedural measures, which should be implemented in all companies to the extent appropriate. These measures are: - Hardware inventory – Develop and maintain a register of all critical system hardware on board, including authorized and unauthorized devices on company controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship. - Software inventory – Develop and maintain a register of all authorized and unauthorized software running on company-controlled hardware onboard, including version and update status. The SMS should be updated to include procedures for: • maintaining this inventory when hardware controlled by the company is replaced • maintaining this inventory when software controlled by the company is updated or changed • authorizing the installation of new or upgraded software on hardware controlled by the company • prevention of installation of unauthorized software, and deletion of such software if identified • software maintenance. - Map data flows – Map data flows between critical systems and other equipment/technical systems on board and ashore, including those provided by third parties. Vulnerabilities identified during this process should be recorded and securely retained by the company. The SMS should be updated to include procedures for: • maintaining the map of data flows to reflect changes in hardware, software and/or connectivity • identifying and responding to vulnerabilities introduced when new data flows are created following the installation of new hardware • reviewing the need for connectivity between critical systems and other OT and IT systems. Such a review should be based on the principle that systems should only be connected where there is a need for the safe and efficient operation of the ship, or to enable planned maintenance • controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems. - Implement secure configurations for all hardware controlled by the company – This should include documenting and maintaining commonly accepted security configuration standards for all authorized hardware and software. The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure configurations are included in the SMS. This information should be retained separately and securely by the company. - Audit logs – Security logs should be maintained and periodically reviewed. Security logging should be enabled on all critical systems with this capability. The SMS should be updated to include procedures for:	Shipsure <> VShips Chart provider > ECDIS vessel email <> shore USB Blockers, standing orders	Vessel Risk Assessment SMS/Fleet Ops/Computer Systems 1.5.7 Shipsure/PC Inventory SMS/Fleet Ops/Comp Systems/1.5.7 (Change control) CSP 2.7.3 CSP 2.6.1 SMS/Fleet Ops/Comp System 1.5.9 SMS/Forms: Information Security/IT03 circular – RSQ0502

	• policies and procedures for the maintenance of security logs and periodic review by competent personnel as part of the operational maintenance routine • procedures for the collation and retention of security logs by the company, if appropriate. - Awareness and training – See line 3 above. - Physical security – The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code. Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard.	No current log management	SMS/Fleet Forms/IT03 CSP 2.6 SSP 3. General security

Develop contingency plans			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
ISM Code: 7 Industry Guidelines: 6 Update procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment which rely on OT.	An approved SMS should already address procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment. In general, these plans should be unaffected by the incorporation of CRM into the SMS. This is because the effect of the loss of availability of OT, or loss of integrity of the data used or provided by such systems, is the same as if the OT was unavailable or unreliable for some other reason. Notwithstanding this, consideration should be given to developing instructions on the actions to be taken if disruption to critical systems is suspected. This could include procedures for reverting to back-up or alternative arrangements as a precaution whilst any suspected disruption is investigated. Procedures for periodically checking the integrity of information provided by OT to operators should be considered for inclusion in operational maintenance routines.	No OT equipment/data affects the safety of the crew or vessel	VMS Forms - TEC18
ISM Code: 8.1 Industry Guidelines: 6 Update emergency plans to include responses to cyber incidents.	An approved SMS should already address emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment. In general, these plans should be unaffected by the incorporation of cyber risk management into safety management systems. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by equipment malfunctioning because of a software failure or inappropriate maintenance or operation of the equipment. Notwithstanding the above, consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them. The purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple OT systems required for the safe operation of the ship and protection of the environment. In this more complex situation, additional information on appropriate immediate actions to be taken in response may be necessary.		CSP 4.10; CSP Appendix A.1

DETECT

Develop and implement activities necessary to detect a cyber-event in a timely manner			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
ISM Code: 9.1 Industry Guidelines: 5.1 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.	An approved SMS should already address procedures relating to non-conformities. When incorporating CRM into the SMS, company reporting requirements for non-conformities may need to be updated to include cyber related non-conformities. Examples of such non- conformities and cyber incidents: - unauthorised access to network infrastructure - unauthorized or inappropriate use of administrator privileges - suspicious network activity - unauthorised access to critical systems - unauthorised use of removable media - unauthorised connection of personal devices - failure to comply with software maintenance procedures - failure to apply malware and network protection updates - loss or disruption to the availability of critical systems - loss or disruption to the availability of data required by critical systems.		VMS Forms: TEC 03 – Superintendent inspection checklist VMS 1.5.4 Standing orders CSP 1.5 Standing orders ITConnectSea – reporting incidents

RESPOND

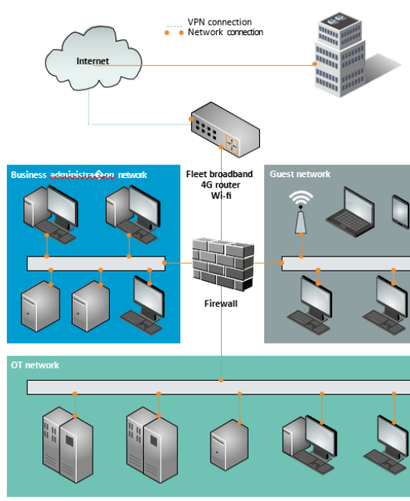
Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
ISM Code: 3.3 Industry Guidelines: 7.1 Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems.	An approved SMS should already be supported by adequate resources to support the DPA. However, the incorporation of CRM into the SMS should require that this resourcing includes appropriate IT expertise. This resource could come from within the company but may also be provided by a third party. In providing the adequate resources, the following should be considered: - company or third party technical support should be familiar with onboard IT and OT infrastructure and systems - any internal response team or external cyber emergency response team (CERT) should be available to provide timely support to the DPA - provision of an alternative means of communication between the ship and the DPA, which should be able to function independently of all other shipboard systems, if and when the need arises - internal audits should confirm that adequate resources, including third parties when appropriate, are available to provide support in a timely manner to support the DPA.		TOM – Vessel Support, IT Support, CSIRT team SSP – 2. Responsibilities VSAT: Email; Collaboration technologies FBB: email; telex Telephone Superintendent audits
ISM Code: 9.2 Industry Guidelines: 7.1 Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.	An approved SMS should already include procedures for responding to non-conformities. In general, these should not be affected by the incorporation of CRM in SMS. However, the procedures should help ensure that consideration of non-conformities and corrective actions involves the personnel with responsibility and authority for CRM. This should help ensure that corrective actions, including measures to prevent recurrence, are appropriate and effective.		SMS IT01 - Vessel cyber risk assessment Shipsure inspection module
ISM Code: 10.3 Industry Guidelines: 7.1 Update the specific measures aimed at promoting the reliability of OT.	An approved SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for: - Software maintenance as a part of operational maintenance routines – Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person. - Authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks – This should include authorizing access in general (including - verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session. - Preventing the application of software updates by service providers using uncontrolled or infected removable media. - inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state. - Trolled use of administrator privileges to limit software maintenance tasks to - competent personnel.		VMS 1.5.7 VMS 1.5.5 Standing orders CSP 1.5 Standing orders

RECOVERY

Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
ISM Code: 10.4 Industry Guidelines: 5.1 and 7.2 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. A SMS, which incorporates CRM, should include procedures for: • checking back-up arrangements for critical systems, if not covered by existing procedures • checking alternative modes of operation for critical systems, if not covered by existing procedures • creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident • maintaining back-ups of data required for critical systems to operate safely • offline storage of back-ups and clean images, if appropriate • periodic testing of back-ups and back-up procedures.		CSP 2.8

ONBOARD NETWORKS

Develop and implement activities necessary to detect a cyber-event in a timely manner			
Action	**Remarks**	**V.Group Comments**	**Evidence location**
A secure network depends on the IT/OT set up onboard the ship, and the effectiveness of the company policy based on the outcome of the risk assessment. Control of entry points and physical network control on an existing ship may be limited because cyber risk management had not been considered during the ship's construction. It is recommended that network layout and network control should be planned for all new buildings. .	Direct communication between an uncontrolled and a controlled network should be prevented. Furthermore, several protection measures should be added: • implement network separation and/or traffic management • manage encryption protocols to ensure correct level of privacy andcommercial communication • manage use of certificates to verify origin of digitally signed documents, software orservices. In general, only equipment or systems that need to communicate with each other over the network should be able to do so. The overriding principle should be that the networking of equipment or systems is determined by operational need.		CSP 2.4
Physical layout	The physical layout of the network should be carefully considered. It is important to consider the physical location of essential network devices, including servers, switches, firewalls and cabling. This will help restrict access and maintain the physical security of the network installation and control of entry points to the network.		VMS 1.5.4 Standing orders CSP 1.5 Standing orders
Network management	Any network design will need to include an infrastructure for administering and managing the network. This may include installing network management software on dedicated workstations and servers providing file sharing, email and other services to the network		

Network segmentation	Onboard networks should normally accommodate the following: 1. necessary communication between OT equipment 2. configuration and monitoring of OT equipment 3. onboard administrative and business tasks including email and sharing business related files or folders (IT networks) 4. recreational internet access for crew and/or passengers/visitors. Effective network segmentation is a key aspect of “defence in depth”. OT, IT and public networks should be separated or segmented by appropriate protection measures. The protection measures used may include, but are not limited to an appropriate combination of the following: • a perimeter firewall between the onboard network and the internet • Network switches between each network segment • internal firewalls between each network segment • Virtual Local Area Networks (VLAN) to host separate segments.		VMS Fleet ops 1.5.1
	In addition, each segment should have its own range of Internet Protocol (IP) addresses. Network segmentation does not remove the need for systems within each segment to be configured with appropriate network access controls and software firewalls and malware detection.  figure 2: example of an onboard network In the example shown above, the network has been segmented using a perimeter firewall, which supports three VLANs: 1. the OT Network containing equipment and systems, that performs safety critical functions 2. the IT network containing equipment and systems, that performs administrative or business functions 3. a crew and guest network, providing uncontrolled internet		

	access. Considerations should be made on how to maximise the security of the switches themselves. To achieve the highest level of security, each network should use a different hardware switch. This will minimise the chance of an attacker jumping between networks due to misconfiguration or by acquiring access to the configuration of a switch. A correctly configured and appropriate firewall is an important element of the proper segmentation of a network installation. The onboard installation should be protected by at least a perimeter firewall to control traffic between the internet and the onboard network. To prevent any unintended communication taking place, the firewall should be configured by default to deny all communication. Based on this configuration, rules should be implemented. The rules should be designed to allow the passage of data traffic that is essential for the intended operation of that network. For example, if a specific endpoint receives updates from the internet, the rule should allow the specific endpoint to connect specifically to the server handling the specific update service. Enabling general internet access to a specified endpoint for updates is not recommended. Uncontrolled networks like a crew or passenger network should not be allowed any communication with the controlled networks. The uncontrolled network should be considered as unsafe as the internet, since the devices connecting to it are unmanaged, their security status (antivirus, updates, etc.) is unknown and their users could be acting maliciously, intentionally or unintentionally.		
Monitoring data activity	It is important to monitor and manage systems to be aware of the networks' status and to detect any unauthorised data traffic. Logging should be implemented in the firewall and ideally in all network- attached devices so that in case of a breach, the responsible person can trace back the source and methodology of the attack. This will help to secure the network from any similar attacks in the future. A network Intrusion Detection System (IDS) or Intrusion Protection System (IPS) can alert the system administrator in real-time of any attacks to the network systems. The IDS and IPS inspect data traffic, entry points or both to identify known threats or to reject traffic, which does not comply with the security policy. An IPS should comply with the latest industry best practices and guidelines. It is recommended to place a sensor on the internet-facing segment, because the public servers are a visible target to attackers. Another sensor should be placed behind the firewall, to monitor traffic between the internet and the internal network. An IDS/IPS sensor could also be placed by a remote- access segment, for instance a Virtual Private Network (VPN).		Epsco-Ra? Gradient Cyber? Dualog Protect?

Protection measures	Protection measures should be implemented in a way that maintains the system's integrity during normal operations as well as during a cyber incident. Every OT network onboard has several endpoints such as workstations, servers, routers, input and output modules, transducers etc. The endpoints are very important as they control the operation and the security of the system. A single security product, technology or solution cannot adequately protect an OT system by itself. A multiple layer strategy involving two (or more) different overlapping security mechanisms is desired, so that the impact of a failure in any one mechanism is minimized (see chapter 5.1 defence-in-depth). In addition, an effective defence-in-depth strategy requires a thorough understanding of possible attack vectors on an OT system. These may include: • backdoors and holes in network perimeter and instruments • vulnerabilities in commonly used protocols • endpoints and sensors • unprotected databases. A secure running environment can be established by using a sandbox, which provides additional protection against cyber threats by isolating executable software from the underlying operating system. This prevents unauthorised access to the operating systems, on which the software is running. The sandbox enables software to be run under a specific set of rules and this adds control over processes and computer resources. Therefore, the sandbox helps prevent malicious, malfunctioning or untrusted software from affecting the rest of the system.		