Subject Area no. 28 Cyber security			
Principle: The company has a programme to design and operate IT and digital process control systems to manage risk to system and information integrity, availability and confidentiality.			
Level	**Expectations**	**Targets**	**Suggested objective evidence**
Basic	The company has documented policy and procedures covering cyber security. The company has carried out cyber security assessments, and has developed a cyber security plan. The company has procedures in place for responding to and recovering from cyber incidents. The company has designated appropriate shore based and ship based personnel with responsibility for cyber security.	The policy, which is signed by senior management, includes a commitment to minimising the impact of cyber incidents. The assessment could include: identification of external and internal cyber security threats, identification of onboard IT and OT with communications links, identification of the consequences of a cyber security threat on these systems. The plan includes measures to: reduce the likelihood of vulnerabilities being exploited, reduce the potential impact of a vulnerability being exploited.	Policy and procedures Cyber security assessments Cyber security plan Procedures to recover from incident Responsibility designated ashore and aboard Training and qualifications.

Subject Area no. 28 Cyber security			
Level	**Expectations**	**Targets**	**Suggested objective evidence**
Intermediate	The company has documented procedures on the control of physical access to shipboard IT/OT systems, and use of personal devices aboard.	Procedures may include:- Protection of critical equipment from attacks.- Controlled access to communication ports, including USB ports.- Control of access to all IT/OT terminals including servers- Access for 3rd parties - Use of personal devices.	Procedures/KPIs
	The company provides cyber security training to all staff.	All shore and vessel staff should be made aware of the cyber security policy and its requirements, how they contribute to cyber security and the implications of not conforming to the policy.Initial and refresher training will be provided.	All staff trained & records kept
	The company carries out internal audits of the cyber security procedures to verify its effectiveness.	Cyber internal audits are covered by a procedure.The company develops an audit plan.	Cyber security audits
	The company has formalised sources for receiving information enabling it to respond to potential cyber security events.		

Subject Area no. 28 Cyber security			
Level	**Expectations**	**Targets**	**Suggested objective evidence**
Advanced	The company reviews effectiveness of its cyber security plan to ensure its suitability, adequacy and effectiveness. The company enforces third party access management.	Management reviews should be carried out at least annually in order to follow-up the implementation and development of the plan. The company takes appropriate precautions for third party access to IT and OT. The company performs due diligence audits or uses independent auditors reports before granting access to systems. The company has a formal process before employing new technology aboard its fleet	Documented management reviews 3rd party access precautions. Due diligence audits. Cyber security assessments for new equipment.

Subject Area no. 28 Cyber security			
Level	**Expectations**	**Targets**	**Suggested objective evidence**
Excellence	The company uses external resources to perform regular audits to confirm compliance with the cyber security plan.	Audits are used to: - Understand compliance with external regimes that the company must comply with. - Verify internal compliance with cyber procedures. - Verify cyber risk assessments and risk conditions.	External audits of cyber security plan.
	The company has adopted a cyber security notation for all the vessels in its fleet.	The company has adopted ISO27032 and/or classification notation for its vessels.	Certification
	The company employs network intrusion monitoring & other advanced cyber security monitoring services to provide defence in depth to protect critical systems.	The company uses technology which limits the exposure of critical systems to network attack and monitors network traffic to detect and react to attempted or actual network intrusions. Vessel and equipment are designed and engineered to minimise cyber vulnerabilities.	Use of cyber security monitoring services.

Notes: