JHC Cyber Risk Assessment Guidance

Background checks:

- 1 Cyber security should be owned at Board level within the company, and there should be a demonstration of commitment to employees from the highest levels of the company to effective cyber security.
- The company should have carried out a thorough threat assessment, contemplating the following;
 - 2.1 The current level of actual or attempted security breaches recorded by the IT Manager
 - 2.2 The current level of compliance with internal controls linked to the use of computer systems
 - 2.3 The current level of compliance with international security standards (ISO 27001/2, NERC 1300, ISA/IEC-62443.)
 - 2.4 The current level of compliance with the Critical Security Controls promoted by the Council on Cyber Security.
 - 2.5 The company's current reputation on social media
- The company should have established a coherent IT policy describing how IT will be used on board ship, and how it will be structured and supported.
- 4 The company should be able to provide a rationale for the design and arrangement of on board systems in the context of the Critical Security Controls.
- 5 The company should be able to demonstrate links between recruitment, training and vetting policies for sea staff and the company security policy as it relates to cyber security.

Control checks:

- There should be clear links between ISM, ISPS and cyber security measures on board. Cyber security on board should be included in the scope of internal ISM/ISPS audits. The security measures should be fit for purpose and contemplate;
 - 6.1 The age, vulnerabilities and arrangement of electronic equipment on board
 - 6.2 The implementation of IT security policies and procedures
 - 6.3 An acceptable use policy for the use of shipboard IT for social or recreational purposes.
 - 6.4 A social media policy for crew members

- If the company is not in compliance with an acceptable external standard, there must be an achievable action plan in place to achieve compliance within the policy year.
- There should be sufficiently qualified and experienced people on board to implement the control measures that mitigate cyber risk.
- 9 The company should be able to demonstrate that it has assessed the cyber risk controls of sub-contractors and others in the supply chain that might impinge upon the risk on board ship.
- The company should be able to demonstrate that it has assessed the personnel vetting standards of sub-contractors and partners placing people on board ship.
- 11 The company should be able to provide a written security declaration from telecommunications providers on board.