	CIRCULAR 2020-005		
	DEPARTMENT OF MARINE SERVICES AND MERCHANT SHIPPING (ADOMS)		
	Maritime Cyber Risk Management	Ref	**IMO Resolutions: MSC.428(98) ISM Code MSC. FAL.1/Circ.3**

Addressees(s):

- ***Owners and Operators of ships under the flag of Antigua and Barbuda***
- ***All ships registered under the flag of Antigua and Barbuda***

1. Scope

The purpose of this Circular is to provide all ADOMS Clients and Stakeholders with information on the interpretation, expectations and requirements of the Administration in respect of the Maritime Cyber Risk Management

2. Legal Basis

Antigua and Barbuda Merchant Shipping Act (MSA) 2006 and adhering Regulations

3. Summary / Excerpt

IMO has decided that safety management system audits, under ISM Code, are to include cyber security as an identified risk.

The handling of the risks is to be verified in the audits carried out from the 1st January 2021, under IMO Res. MSC.428(98) ISM Code.

Recognized Organizations (ROs) have full authorization to carry out this work, under requirements of the ISM Code, on behalf of Antigua and Barbuda flag.

The list of our Recognized Organizations (ROs) is on our website, who have published guidance on this. https://www.abregistry.ag/technical-services/recognised-organisation/

4. ADOMS Policy

Cyber security is key to ensuring safe operation of vessels and safeguarding people, cargo and the environment and IMO has adopted Resolution MSC. 428(98). This stipulates that an approved safety management system should consider cyber risk management, as part of the requirements under ISM Code.

Companies must, no late than the first annual verification of their ISM Document of Compliance (DOC), after 1st January 2021, demonstrate that cyber security is an integral part of the safety management system.

IMO has also issued guidelines on their website for maritime cyber risk management under MSC. FAL.1/Circ.3 and it is recommended that ISM DOC holders carefully consider this guidance.It recommends a risk management approach to cyber risks, that is resilient and evolves as a natural extension of existing safety and security management practices.