News from the Comité International Radio-Maritime (CIRM)

On 4 February CIRM published two important documents:

- **CIRM Cyber Risk Code of Practice for Vendors of Marine Electronic Equipment and Services**
- **CIRM Guideline GL-002 – Implementing the CIRM Cyber Risk Code of Practice**

Both documents, launched on 4 February, are freely available on the CIRM website in the Publications Section at: [http://cirm.org/publications/index.html](http://cirm.org/publications/index.html)

The Code and Guideline were developed over two years by the CIRM Cyber Risk Working Group and subsequently approved by the Technical Steering Committee.

**The Cyber Risk Code of Practice for Vendors**

This document is intended to be used by vendors of marine electronic equipment and services, including producers of shipboard Information Technology (IT) and Operational Technology (OT) equipment, system integrators, service suppliers and Communications Service Providers in the marine electronics industry (collectively referred to as ‘Vendors’). The Code will enable them to implement effective and cost-efficient cyber security best practice derived from both the marine and other industries. As such, it represents CIRM’s view of cyber security best practice. The Code consists of six guiding principles for vendors to establish their role in the chain of trust for a secure digital maritime environment.

**Guideline GL-002**

The Guideline on implementing the CIRM Cyber Risk Code of Practice for Vendors of Marine Electronic Equipment and Services is a companion document to the Code. It aims to explain how to implement the principles of the Code by directing the audience to appropriate standards, guidelines and best practice, and providing additional guidance where this adds value.

The CIRM’s Secretary-General, Frances Baskerville said: ‘The CIRM Cyber Risk Code of Practice is the result of two years’ work by our organization’s members. It presents CIRM’s view of the measures that can be taken by vendors of marine electronic equipment and services to reduce the risk of cyber security incidents’.


CIRM is a Corresponding Member of IAIN
IAIN is an Observer member of CIRM

1