key'point

CBB releases draft rules on cyber security for consultation

In a possible sign of things to come, the Central Bank of Bahrain has proposed changes to Volume 4 of its Rulebook (investment firms), revising the authorisation module, drafting a new module on digital financial advice and adding a chapter on cyber security risk measures, as well as adding to Volume 4's glossary.

Released for consultation on 22 January 2019 (with comments due by 21 February 2019), the chapter on cyber security risk requires licensees to establish clear ownership and management accountability for risks associated with cyber-attacks and to put risk management processes commensurate with their size, activities and risk profile in place. In addition, cyber security measures must be part of each licensee's IT security policy. As well as stipulating responsibilities for the board and senior management – including approving and creating a cyber risk framework – the chapter requires cyber security risk to be an agenda item at board meetings.

A clear reporting line to the board must be established for cyber security incidents and a dedicated IT security officer must be appointed with responsibility for cyber and information security.

Cyber security risk defense strategies must be defined and documented and cyber security risk policies established, including objectives, structures, frameworks, effectiveness matrices and reporting. Licensees must report any significant cyber-attacks – whether internal or external – to the CBB immediately.

The new cyber security chapter also requires all licensees providing internet services to test their systems twice every year – and to report the findings to the CBB within two months. These tests must be conducted by external, independent security professionals, such as ethical hackers.

The proposed rules are available on the CBB website in the 'open consultations' section.

Contact us

Srikant Ranganathan
Senior Director
IT consulting
+973 1720 6827

Sagar Rao
Senior Consultant
IT consulting
+973 1720 6834