



Cybersecurity requirements for Volume 4 Licensees

KPMG in Bahrain insight on to how to prepare for the new Central Bank of Bahrain (CBB) Volume 4 cybersecurity requirements



August 2019

kpmg.com/bh

The CBB published new cybersecurity requirements as part of the Risk Management module of the Volume 4 Licensee Rulebook.



New regulation highlights

01



Board responsibility

The **Board is accountable** for implementing and monitoring a cyber risk framework and strategy.

IT security officer

The Board must appoint a **dedicated IT security officer** with responsibility for cyber and information security.



02

03



Cyber framework

Entities must **create, measure, and continuously improve** a cyber risk control framework.

Incident response

The entity must have processes to **respond and report security incidents**.



04

05



Cyber assessments

Independent penetration testing required in June and December. Report to be submitted within one month.

Training

Cyber threat training must be provided to all employees on a regular basis.



06

The effectiveness of training must be tested through **simulated cyber-attack scenarios**.



How can KPMG help?

Our cybersecurity team here in Bahrain will walk with you in setting up the required processes and overall framework needed to maintain ongoing compliance. We customize each control and process to fit your organization size and risk appetite profile.

01

We perform an as-is assessment of your cybersecurity processes which are currently being performed.

We provide a recommendation roadmap for remediating any compliance gaps.



02

We assist you in developing a cyber risk framework and strategy to be approved and implemented by the board.

We help you prepare the required policies, technology, and governance processes.



03

We perform penetration testing of your technology systems according to the CBB requirements in June and December.

Our testing includes internal and external to simulate real world cyber threats and attacks.



04

We provide cyber security training at three levels to meet the compliance requirements.

- Board level cyber training
- Technical cyber training
- General employee cyber training





For further information, please contact:



Logan Simpson
Lead Cyber Security
Management Consulting
E : jlsimpson@kpmg.com



Manav Prakash
Director
Management Consulting
E : mprakash@kpmg.com

©2019 KPMG Fakhro, a Bahrain partnership registered with the Ministry of Industry, Commerce and Tourism (MOICT), Kingdom of Bahrain and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks of KPMG International.