BMA Releases Insurance Sector Operational Cyber Risk Management Code of Conduct

9 October 2020

The Bermuda Monetary Authority ("BMA") has released its Operational Cyber Risk Management Code of Conduct ("the Code") for the insurance sector. The purpose of the Code is to promote the stable and secure management of information technology systems of registered insurers, insurance managers and intermediaries (collectively, "registrants"), highlighting the critical nature of a registrant's confidentiality, integrity and availability of information to its daily operations.

Registrants must ensure there is adequate board visibility and governance of cyber risk. The Chief Information Security Officer ("CISO") will be responsible for the delivery of the cyber risk management programme, whilst the three lines of defence model should be utilised for the implementation of the cyber risk management programme. Registrants must implement a cyber-risk policy, a staff vetting process and ensure cyber risk awareness training is completed at least annually.

The cyber risk management programme must include a risk assessment process, which includes the identification, measurement, response, monitoring and reporting of cyber related risks. Registrants should ensure that the effectiveness of controls are independently audited and the control environment is monitored and evaluated on a continuous basis. Where a registrant outsources functions either externally or internally to an affiliate, there must be clear accountability and oversight of these outsourced functions and the service agreement must include terms that define the governing roles and relationships and must also allow the BMA to have oversight of relevant outsourced functions.

From a compliance perspective, the Code states that registrants will be assessed in a proportionate manner, with the understanding that registrants have varying risk profiles relative to their nature, scale and complexity.

The release of the Code will provide registrants with the tools needed to construct their cyber risk management programme, enabling them to conduct their business in a sound and prudent manner. The Code will become operative on 1 January 2021 and registrants must be compliant by 31 December 2021.The Insurance Sector Operational Cyber Risk Management Code of Conduct can be viewed here.

>>

Walkers Regulatory and Compliance team of compliance professionals and regulatory lawyers are able to assist with preparing and reviewing policies and procedures and outsourcing agreements, providing staff training and providing assurance that your cyber risk management framework is legally sound and operationally effective from a legal and compliance perspective. Should you require any further information or wish to discuss further the impact of the Code, please do not hesitate to contact Natalie Neto, Melanie Fullerton or Michael Wynne.

Contacts

For more information please speak with your usual Walkers contact or one of the following:

Natalie Neto
Partner
T: +1 441 242 1533
E: natalie.neto@walkersglobal.com

Melanie Fullerton
Senior Associate
T: +1 441 242 1537
E: melanie.fullerton@walkersglobal.com

Michael Wynne
Senior Vice President
T: +1 441 242 1542
E: michael.wynne@walkersglobal.com