October 2020

Dear Stakeholders:

Re: Insurance Sector Operational Cyber Risk Management Code of Conduct – Consultation response

The Bermuda Monetary Authority (the Authority) would like to thank stakeholders for their continued support of our key initiatives. The Authority is committed to ensuring the effective operation of Bermuda's regulatory regime as well as being aligned with international standards.

In Q3-2019 the Authority began a consultation process with the insurance sector associations. The Authority is appreciative of the dialogue that ensued and the support it has received regarding this initiative. On 30 December 2019, the Authority published the Insurance Sector Operational Cyber Risk Management Code of Conduct – consultation paper to the wider market.

The Authority received comments on the consultation paper, we summarise below the sections of the Code that were the focus of comments received and the associated changes that we made.

Overall, the Authority would like to draw attention to section 4 of the Code which details the Proportionality Principle and that the Authority will assess the registrant's compliance with the Code in a proportionate manner relative to its nature, scale and complexity.

The key changes resulting from the consultation are as follows:

1. **Section 4 - Staff cyber risk awareness training must be completed and tested at least annually.**
- *Removed the test requirement*

2. **Section 5.10 - Managing Outsourcing and Third-Party Service Provider Cyber Risk**

- *We have clarified the wording to express that we would expect to review outsourcing controls directly with the registrant, not normally with the outsource service providers themselves.*

3. **Section 5.12 - End User Developed Systems – a request to confirm what specific examples this applies to**

- *The BMA do not set out to prescribe details of every type of end user environment, each registrant should assess their own risks from End User Developed Systems and their desired risk response.*

4. **Section 5.14 - Security Review of New Projects and IT systems**

- *We have noted that this is required for projects involving critical assets and that minor changes should be security reviewed as part of the standard change management process.*

5. **Section 6.13 - Encryption of non-public information**

- *We have added that where encryption is not feasible, mitigating controls may be used by exception.*

6. **Section 6.5 - Cyber Risk Reporting Events**

- *We have made the following changes: confirmed which cyber reporting events must be reported, specified that incident investigation logs (not system event logs) be kept for a minimum of five years.*

7. **Section 7.1 - Business Continuity (BCP) and Disaster Recovery (DR)**

- *We have clarified that we require both the BCP and DR tests to be carried out at least annually.*

The Authority would like to thank stakeholders for their comments on the consultation paper. We remain committed to working with the industry and other interested parties to ensure that results achieved are in the best interests of the Bermuda market.

The Code comes into force on 1 January 2021. The enforcement date was originally set to be 30 June 2021 but in recognition of the current pandemic disruption, the Authority has pushed the enforcement date back to the 31 December 2021.

Yours sincerely,

The Bermuda Monetary Authority