14 March 2022

Dear Stakeholders,

Re: Consultation Paper: Operational Cyber Risk Management Code of Conduct for Banks, Deposit Companies, Corporate Service Providers, Trust Companies, Money Service Businesses, Investment Businesses and Fund Administration Providers (Code).

The Bermuda Monetary Authority (Authority or BMA) would like to thank stakeholders for their continued support of our key initiatives. The Authority appreciates the feedback received and is committed to ensuring that Bermuda's regulatory regime remains effective and aligned with international standards.

The Authority sought feedback on the proposed duties, standards, procedures and principles for compliance in relation to operational cyber risk management within the sectors noted above.

RESPONSE TO INDUSTRY FEEDBACK

Overall, the Authority would like to draw attention to sections III and IV of the Code. Section III – *Interpretation* clarifies that requirements denoted as 'should' are encouraged but are not mandatory. Section IV – *Proportionality Principle* notes that the Authority will assess a Relevant Licensed Entity's (RLE) compliance with the Code in a proportionate manner relative to its nature, scale and complexity.

The Authority received feedback from three stakeholders and the response to the **key substantive comments** received on the Code are outlined below.

Section III – Interpretation

- *Modified the definition of 'Should' to remove documentation of the reason for deviating from the recommendation*

Section VIII – The Role of the Chief Information Security Officer (CISO)

- *Added guidance to clarify that RLEs may place reliance on group CISO to satisfy the requirement*

Section XV – Managing outsourcing and third-party service provider cyber risk

- *The Authority agrees with stakeholders that the reference to 'cyber-related function' was unclear. As such, the requirement has been updated*

Section XXIV – Notification of cyber risk reporting events to the Authority

- *The Authority will publish on its website a sample reporting guide for RLEs, including relevant contact information*

Section XXXVII – Network Security Management

- *The Authority agrees with stakeholders that reference to demilitarised zone in the requirement was not appropriate and have thus updated the requirement*

Section XLI – Use of Cryptography

- *The Authority modified the requirement in response to stakeholder feedback*
  - *Initially proposed: RLEs should evaluate cryptographic implementations and ensure that only cryptographic modules based on authoritative standards and reputable protocols are included*
  - *Revised requirement: RLEs should evaluate cryptographic implementations and ensure that only cryptographic modules based on authoritative standards and reputable protocols are enabled*

Section XLV – Use of Definitions

- *The Authority modified the definition of 'data loss prevention' as it agrees with stakeholders' response that the originally proposed definition was too restrictive*
  - *Revised definition: A strategy for ensuring that end-users do not inappropriately send sensitive or critical information outside the corporate network*

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

The Code comes into force on 15 March 2022 for Corporate Service Providers, Trust Companies, Money Service Businesses, Investment Businesses and Fund Administration Providers and RLEs are required to become compliant by 15 February 2023. The in-force date for entities licensed under the Banks and Deposit Companies Act 1999 will be communicated at a later date.

Sincerely,

Bermuda Monetary Authority