CENTRAL BANK OF TRINIDAD AND TOBAGO
Eric Williams Plaza, Independence Square, Port-of-Spain, Trinidad, Trinidad and Tobago
Postal Address: P.O. Box 1250
Telephone: (868) 621-CBTT (2288), 235-CBTT (2288); Fax: 612-6396
E-Mail Address: info@central-bank.org.tt
Website: www.central-bank.org.tt

August 10, 2022

CIRCULAR LETTER TO ALL COMMERCIAL BANKS LICENSED UNDER THE FINANCIAL INSTITUTIONS ACT, 2008

REF: CB-OIFI-1935/2022

THEMATIC REVIEW OF CYBERSECURITY RISK MANAGEMENT PRACTICES

Cyber incidents pose risks to financial institutions and to financial stability. The increasing frequency and severity of cyber threats and use of digitalisation of financial products and services led to the Central Bank's commencement of a Thematic Review of Cybersecurity Risk Management Practices ("thematic review") in the banking sector that commenced in 2020, just prior to the start of the pandemic. The thematic review was conducted across seven of the eight commercial banks to gather information on their cybersecurity framework/practices and cyber resilience.

The thematic review was aligned with the Federal Financial Institutions Examination Council's[1] ("FFIEC") 2017 Cybersecurity Assessment Tool (CAT), which consisted of two parts; (1) an Inherent Risk Profile, which was determined by each commercial bank's self-assessment of its inherent risk, and (2) a Cybersecurity Maturity assessment.

There are **five** domains in FFIEC's assessment tool, which cover the following areas:-

- **Domain 1** covers the adequacy of **Cyber Risk Management and Oversight**, which addresses the board of directors' (board's) oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight. It also includes the allocation of the FI's resources for cyber risk, as well as, training and culture.

- **Domain 2** captures the quality of **Threat Intelligence and Collaboration**, which includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties. It also incorporates monitoring and analysis, as well as, information sharing.

[1] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB); the Federal Deposit Insurance Corporation (FDIC); the National Credit Union Administration (NCUA); the Office of the Comptroller of the Currency (OCC); and the Consumer Financial Protection Bureau (CFPB) in the USA. It makes recommendations to promote uniformity in the supervision of financial institutions and raises the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

- **Domain 3** looks at the adequacy of **Cybersecurity Controls**, which are the practices and processes used to protect assets, infrastructure, and information by strengthening the institution's defensive posture through continuous, automated protection and monitoring. It includes preventative controls, detective controls, and corrective controls.

- **Domain 4** reviews the quality of the **Management of External Dependency**, which involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution's technology assets and information.

- **Domain 5** looks at the adequacy of **Cyber Incident Management and Resilience**, which includes establishing, identifying, and analyzing cyber events; prioritizing the institution's containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber- incident.

The Bank's assessment comprised of a review of the responses from the assessment tool and an off-site review of documents submitted by each financial institution. The review also included the conduct of virtual interviews with key personnel from the financial institutions. Heavy reliance was also placed on the institutions' assessments of the complexity of their technological and business operating environments.

We are now pleased to submit the final report for your information and consideration. The Report contains valuable information that can be used to improve cybersecurity risk management practices across the industry and should be tabled at the next meeting of your Board of Directors.

Yours sincerely

Patrick Solomon
INSPECTOR OF FINANCIAL INSTITUTIONS