CENTRAL BANK OF TRINIDAD & TOBAGO

SELF-ASSESSMENT:
Best Practices on Cybersecurity

A. GOVERNANCE – The Board, senior management and all 'internal lines of defense' - Business, Risk, and Internal Audit Departments must be involved in the implementation of a defined cybersecurity plan. Roles, responsibilities and reporting lines for all functional areas or person involved in the cybersecurity strategy should be clearly defined.	
• A **formal risk-based cybersecurity strategy** should be developed--covering issues of identification, protection, detection, response and recovery--accompanied by consistent policies, procedures and standards that allow for appropriate tracking and monitoring.	Choose an item
• The **Board should approve the cybersecurity strategy** and be kept informed of developments at least annually or more frequently if material issues arise.	Choose an item
• **Senior Management is responsible for implementing** the strategy as well as the accompanying policies, procedures, and standards.	Choose an item
• The **Internal Audit Department should perform regular independent reviews** of compliance with the cybersecurity strategy and policies and make relevant recommendations. Companies may also outsource the conduct of the independent review to a third party.	Choose an item
B. RISK MANAGEMENT – A clear risk management framework should be established that assesses the company's potential cybersecurity vulnerabilities and incorporates identification, monitoring, analysis, and reporting of cybersecurity incidents.	
• The risk management framework should identify the **cyber security threats and vulnerabilities** applicable to the IT environment, including internal and external networks, hardware, software applications, systems interfaces, data, operations procedures, and people.	Choose an item
• The company should assure that adequate attention is placed to **outsourcing risks**, notably the possibility of risks related to third-party providers of IT services.	Choose an item
• The company should ensure that policies and procedures for **information security** are implemented and regularly reviewed and updated.	Choose an item
• An **explicit incident management framework** should be developed, encouraging reporting by staff and incorporating regular, systematic reviews of incidents and measures for improvement.	Choose an item
C. AWARENESS AND TRAINING – Regular and appropriate cybersecurity training must be provided to employees and customers in an understandable way.	
• Security awareness **training should be provided to all employees and Board members at least annually** along with measures to assure participation and compliance with the training recommendations. Staff training should at least cover identification of malicious dangers, key safety practices, and the company's cybersecurity policies.	Choose an item
• **Tailored security awareness training** should be provided to Managers and IT Staff, reflecting their varying levels of responsibility.	Choose an item
• **Customers should receive adequate communication** to allow them to utilize the company's customer facing and accessible applications and tools relevant to their needs, understand their privacy and other rights, how to report suspicious activities, and the avenues for redress in case of problems.	Choose an item

D. BUSINESS CONTINUITY AND DISASTER RECOVERY – The company should have business continuity and recovery plans which incorporate dealing with cyber-related occurrences, including information technology system failures and unavailability.	
• The company should establish IT systems' **recovery time objectives and recovery point objectives** aligned to its business resumption and system recovery priorities.	Choose an item
• The company should establish a **system and data backup strategy**, and perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted.	Choose an item
• Where information assets are managed by third party service providers, companies should **assess the service provider's disaster recovery capability**.	Choose an item
• Business continuity and disaster recovery plans should be reviewed and **tested regularly** to validate their effectiveness.	Choose an item
E. TESTING – Regular testing of IT systems that simulate potential threats and failures should be carried out at a frequency commensurate with the complexity and risk profile of the company.	
• The company should establish processes to conduct **regular vulnerability assessments** of its IT assets, including IT systems, network devices and applications, to identify security vulnerabilities and ensure risks arising from these gaps are addressed in a timely manner.	Choose an item
• The company should carry out **penetration testing** (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.	Choose an item
F. INCIDENT MANAGEMENT AND REPORTING – Information on material system changes and cybersecurity incidents that affect customers should be transparently communicated to them and to the relevant regulator.	
• The company should establish an **incident management framework** with the objective of restoring an affected IT service or system to a secure and stable state as quickly as possible. The goal is to minimise impact to the company's business and customers.	Choose an item
• The company should **report all incidents considered to have a material impact** on its business operations and consumers to the Central Bank or relevant regulator.	Choose an item
• In the case of a material incident, **affected consumers and the Central Bank should be informed promptly** of the incident, its implications and remedial measures taken. Communication to the public should be in plain language.	Choose an item
Name of Institution:	
Period of Assessment:	
Name of Chief Executive Officer / Designate:	
Designation:	
Signature:	
Date:	

ALL ASSESSMENTS MUST BE SUBMITTED VIA EMAIL TO cyberguides@central-bank.org.tt