CENTRAL BANK OF
TRINIDAD & TOBAGO

INSTRUCTIONS AND RATING FOR CYBER RISK QUESTIONNAIRE

The Central Bank requests that in selecting responses, financial institutions rate their current degree of maturity on a 1 to 4 scale and provide sufficient justification in all circumstances under the comments section. A definition of each of the ratings is provided below.

4 – Fully Agree The financial institution ('FI') has fully implemented the measures outlined under the sub-categories. There is evidence to substantiate the assessment. There are no outstanding issues identified (e.g. issues raised through self-assessment, or by groups such as operational risk management, Internal Audit, supervisors or other third parties).

3 – Largely Agree The FI has largely, but not fully implemented the measures outlined under the sub-categories, or there may be some minor outstanding issues identified (e.g. issues raised through self-assessment, or by groups such as operational risk management, Internal Audit, supervisors or other third parties).

2 – Partially Agree The FI has partially implemented the measures outlined under the sub-categories, major aspects of the implementation remain, and there may be some significant outstanding issues identified (e.g. issues raised through self- assessment or by groups such as operational risk management, Internal Audit, supervisors or other third parties).

1 – Disagree The FI has not yet implemented the measures outlined under the sub-categories.

N/A If the FI determines the rating 1 to 4 is not applicable, the FI is encouraged to provide sufficient justification for this selection.

Financial institutions are encouraged to provide comments where most applicable which will assist in our assessment of the information gathered.

CENTRAL BANK OF
TRINIDAD & TOBAGO

CYBER-RISK QUESTIONNAIRE[1]

Function	Category	Sub-Category	4	3	2	1	N/A	Comments
IDENTIFY	**Asset Management –** The data, personnel, devices, systems, and facilities that enable the licensee to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the licensee's risk strategy.	Physical devices and systems within the licensee are inventoried						
		Software platforms and applications within the licensee are inventoried						
		Licensee's communication and data flows are mapped						
		External information systems are catalogued						
		Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value						
		Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established						
	Business Environment – The licensee's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	The licensee's role in the supply chain is identified and communicated						
		The licensee's place in critical infrastructure and its industry sector is identified and communicated						
		Priorities for the licensee's mission, objectives, and activities are established and communicated						
		Dependencies and critical functions for delivery of critical services are established						
		Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)						
	Governance – The policies, procedures, and processes to manage and monitor the licensee's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Licensee's cybersecurity policy is established and communicated						
		Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners						
		Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed						
		Governance and risk management processes address cybersecurity risks						
	Risk Assessment – The licensee understands the cybersecurity risk to its operations (including mission, functions, image, or reputation), assets, and individuals.	Asset vulnerabilities are identified and documented						
		Cyber threat intelligence is received from information sharing forums and sources						
		Threats, both internal and external, are identified and documented						
		Potential business impacts and likelihoods are identified						
		Threats, vulnerabilities, likelihoods, and impacts are used to determine risk						
		Risk responses are identified and prioritized						

[1] NIST framework, ISO 27000 series

Function	Category	Sub-Category	4	3	2	1	N/A	Comments
	Risk Management Strategy – The licensee's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk management processes are established, managed, and agreed to by its stakeholders						
		Licensee's risk tolerance is determined and clearly expressed						
		The licensee's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis						
	Supply Chain Risk Management – The licensee's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The licensee has established and implemented the processes to identify, assess and manage supply chain risks.	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by its stakeholders						
		Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process						
		Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of the licensee's cybersecurity program and Cyber Supply Chain Risk Management Plan.						
		Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.						
		Response and recovery planning and testing are conducted with suppliers and third-party providers						
PROTECT	**Identity Management and Access Control –** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes						
		Physical access to assets is managed and protected						
		Remote access is managed						
		Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties						
		Network integrity is protected (e.g., network segregation, network segmentation)						
		Identities are proofed and bound to credentials and asserted in interactions						
		Users, devices, and other assets are authenticated (e.g. single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other risks to the licensee)						
	Awareness and Training – The licensee's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements	All users are informed and trained						
		Privileged users understand their roles and responsibilities						
		Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities						
		Senior executives understand their roles and responsibilities						
		Physical and cybersecurity personnel understand their roles and responsibilities						

Function	Category	Sub-Category	4	3	2	1	N/A	Comments
	Data Security – Information and records (data) are managed consistent with the licensee's risk strategy to protect the confidentiality, integrity, and availability of information.	Data-at-rest is protected						
		Data-in-transit is protected						
		Assets are formally managed throughout removal, transfers, and disposition						
		Adequate capacity to ensure availability is maintained						
		Protections against data leaks are implemented						
		Integrity checking mechanisms are used to verify software, firmware, and information integrity						
		The development and testing environment(s) are separate from the production environment						
		Integrity checking mechanisms are used to verify hardware integrity						
	Information Protection Processes and Procedures – Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among the licensee's other entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)						
		A System Development Life Cycle to manage systems is implemented						
		Configuration change control processes are in place						
		Backups of information are conducted, maintained, and tested						
		Policy and regulations regarding the physical operating environment for the licensee's assets are met						
		Data is destroyed according to policy						
		Protection processes are improved						
		Effectiveness of protection technologies is shared						
		Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed						
		Response and recovery plans are tested						
		Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)						
		A vulnerability management plan is developed and implemented						
	Maintenance – Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance and repair of the licensee's assets are performed and logged, with approved and controlled tools						
		Remote maintenance of the licensee's assets is approved, logged, and performed in a manner that prevents unauthorized access						
	Protective Technology – Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy						
		Removable media is protected and its use restricted according to policy						

Function	Category	Sub-Category	4	3	2	1	N/A	Comments
	with related policies, procedures, and agreements.	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities						
		Communications and control networks are protected						
		Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations						
DETECT	**Anomalies and Events –** Anomalous activity is detected and the potential impact of events is understood.	A baseline of network operations and expected data flows for users and systems is established and managed						
		Detected events are analyzed to understand attack targets and methods						
		Event data are collected and correlated from multiple sources and sensors						
		Impact of events is determined						
		Incident alert thresholds are established						
	Security Continuous Monitoring – The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	The network is monitored to detect potential cybersecurity events						
		The physical environment is monitored to detect potential cybersecurity events						
		Personnel activity is monitored to detect potential cybersecurity events						
		Malicious code is detected						
		Unauthorized mobile code is detected						
		External service provider activity is monitored to detect potential cybersecurity events						
		Monitoring for unauthorized personnel, connections, devices, and software is performed						
		Vulnerability scans are performed						
	Detection Processes – Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Roles and responsibilities for detection are well defined to ensure accountability						
		Detection activities comply with all applicable requirements						
		Detection processes are tested						
		Event detection information is communicated						
		Detection processes are continuously improved						
RESPOND	**Response Planning –** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Response plan is executed during or after an incident						

Function	Category	Sub-Category	4	3	2	1	N/A	Comments
	Communications – Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Personnel know their roles and order of operations when a response is needed						
		Incidents are reported consistent with established criteria						
		Information is shared consistent with response plans						
		Coordination with stakeholders occurs consistent with response plans						
		Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness						
	Analysis – Analysis is conducted to ensure effective response and support recovery activities.	Notifications from detection systems are investigated						
		The impact of the incident is understood						
		Forensics are performed						
		Incidents are categorized consistent with response plans						
		Processes are established to receive, analyze and respond to vulnerabilities disclosed to the licensee from internal and external sources (e.g. internal testing, security bulletins, or security researchers)						
	Mitigation – Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incidents are contained						
		Incidents are mitigated						
		Newly identified vulnerabilities are mitigated or documented as accepted risks						
	Improvements – Licensee's response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response plans incorporate lessons learned						
		Response strategies are updated						
RECOVER	**Recovery Planning –** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Recovery plan is executed during or after a cybersecurity incident						
	Improvements – Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned						
		Recovery strategies are updated						
	Communications – Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Public relations are managed						
		Reputation is repaired after an incident						
		Recovery activities are communicated to internal and external stakeholders as well as executive and management teams						

Function	Category	Sub-Category	4	3	2	1	N/A	Comments
FINANCIAL	Over the period January 1, 2017 to December 31, 2018, the bank either directly or as a result of an incident involving a vendor or other third party, experience the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information.							
	If yes to the question above, please complete the following section below.							

FINANCIAL

For the financial aspect of the survey, the data for the Cyber Incidents have been organized in the table below according to the following four categories:

1) **Data breach**: the unintentional disclosure of personally identifiable information (PII) stemming from loss or theft of digital or printed information. For example, the theft of laptop or desktop computers containing personal information of employees or customers, caused either by a hacker, or malicious employee. This category also includes the improper disposal or disclosure of personal information (i.e. to a dumpster or website).

2) **Security incident**: an incident involving the compromise or disruption of corporate IT systems (computers or networks) or its intellectual property. For example, a denial of service (DoS) attack, the theft of intellectual property, the malicious infiltration (hack) and subsequent cyber extortion of corporate information, or a disruption of business services.

3) **Privacy violation**: the unauthorized collection, use or disclosure of personal information. For example, unauthorized collection from cell phones, GPS devices, cookies, web tracking, or physical surveillance.

The first two categories are differentiated from the third in that the first two relate to incidents *suffered by* the licensee (i.e. PII stolen from the licensee, or the licensee suffering a compromise of business operations because of a hack), while the third category relates to events *caused by* the licensee (e.g. the licensee improperly collecting or selling personal information).

4) **Phishing / Skimming:** The final category relates to instances of individuals committing particular kinds of computer or electronic crimes directly against other individuals or licensees. For example, these crimes would include phishing attacks (wherein criminals seek to harvest account information from users), identity theft (wherein criminals use another person’s information for financial gain), or skimming attacks (where criminals install, for example, a hardware device over ATM machines in order to copy bank account and bank PIN numbers).

Type of Cyber Incidents	2017		2018	
	# of Incidents	Total Loss Incurred ($'000)	# of Incidents	Total Loss Incurred ($'000)
Data Breach				
Security Incident				
Privacy Violation				
Phishing / Skimming				