



CENTRAL BANK OF
TRINIDAD & TOBAGO

Cybersecurity Best Practices Guidelines

June 2023 (Draft)

TABLE OF CONTENTS

1. INTRODUCTION.....	2
2. CYBERSECURITY GUIDELINES.....	2
3. OTHER RECOMMENDED CYBERSECURITY PRACTICES.....	6
APPENDIX I - DEFINITIONS / ABBREVIATIONS.....	8
APPENDIX II - CYBERSECURITY INCIDENT REPORTING	10
APPENDIX III - RELEVANT REFERENCE MATERIAL	14

DRAFT

1. INTRODUCTION

This Cybersecurity Best Practices Guideline (Guideline) seeks to provide companies with guiding principles for establishing adequate cybersecurity frameworks to ensure cyber resilience. The cybersecurity framework to be established should be proportional to the company's business model, complexity of operations and risks.

Scope of Application

This Guideline is established in accordance with section 10(b) of the Financial Institutions Act, 2008, (FIA) and section 278(1) of the Insurance Act, 2018 (IA) in respect of companies authorized under these Acts. This Guideline should be read in conjunction with the Bank's Corporate Governance Guideline (2021) and Guideline for the Management of Outsourcing Risks (2022) which are on the Bank's website.

Other institutions not regulated by the Central Bank of Trinidad and Tobago (Central Bank/Bank) are encouraged to adopt the provisions in this Guideline to manage their cyber risks.

Supervision and Enforcement










Companies should conduct annual self-assessments against the Guidelines and submit these to the Central Bank by the following January. Companies should attach detailed action plans to remedy any material deficiencies uncovered.

Reports of independent reviews referred to in section 2.A of the Cybersecurity Guidelines should also be submitted. The Central Bank will review the self-attestation, the independent reviews and any other relevant information, discuss developments and periodically conduct risk based on-site examinations to verify compliance with the Guideline.

2. CYBERSECURITY GUIDELINES

The Cybersecurity Guidelines are set out in the following self-assessment tabular format. Companies should record their level of compliance using the traffic signal format. This self-assessment/attestation should be submitted annually to the Central Bank and signed by the Chief Executive Officer or his/her designate. Section 3 contains complementary actions that are recommended, but not essential to comply with the Guidelines. The Appendices should be read in conjunction with the Guidelines and provide several definitions, the Incident Management Reporting Template and useful references.

<p>A. GOVERNANCE – The Board, senior management and all ‘internal lines of defense’ - Business, Internal Audit, and Risk Departments--must be formally involved in implementing a defined cybersecurity plan:</p>	
<ul style="list-style-type: none"> • 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. • The Board should approve the cybersecurity strategy and be kept informed of developments on a quarterly basis. • Senior Management is responsible for implementing the strategy as well as the accompanying policies, procedures, and standards. • The Internal Audit and Risk Departments 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. 	
<p>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.</p>	
<ul style="list-style-type: none"> • 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, operations procedures, and people. • The company should assure that adequate attention is placed to outsourcing risks, notably the possibility of problems related to third-party providers of IT services. • Policies should be implemented to assure that IT security is updated, including patch management, and more generally an appropriate approach to the implementation of major IT changes. • An explicit incident management framework should be developed, encouraging reporting by staff and incorporating regular, systematic reviews of incidents and measures for improvement. 	

<p>C. AWARENESS AND TRAINING – Regular and appropriate cybersecurity training must be provided to employees and customers in an understandable way.</p>	
<ul style="list-style-type: none"> • Security awareness training should be provided to all employees 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. • Higher level security training should be provided for managers and those responsible for information technology. • Customers should receive adequate training/communication to allow them to utilize the company’s IT tools relevant to their needs, understand their privacy and other rights, and the avenues for redress in case of problems. 	  
<p>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.</p>	
<ul style="list-style-type: none"> • The company should establish IT systems’ recovery time objectives and recovery point objectives aligned to its business resumption and system recovery priorities. • 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. • Where information assets are managed by third party service providers, companies should assess the service provider’s disaster recovery capability. • Business continuity and disaster recovery plans should be tested regularly to validate their effectiveness. 	   
<p>E. TESTING – Regular testing of IT systems that simulate potential threats and failures should be carried out.</p>	
<ul style="list-style-type: none"> • 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. • The company should consider commissioning penetration testing (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems. 	 

<p>F. INCIDENT MANAGEMENT AND REPORTING – Information on key system changes and cybersecurity incidents that affect customers should be transparently communicated to them and to the relevant regulator.</p>	
<ul style="list-style-type: none"> 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. 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. In the case of a material incident, affected consumers should be promptly informed in easy to understand language of the incident, implications and remedial measures. 	
<p> Full Compliance Partial Compliance Not Compliant </p>	
<p>Name of Institution:</p>	
<p>Period of Assessment:</p>	
<p>Name of Board Member/ Representative:</p>	
<p>Designation:</p>	
<p>Signature:</p>	
<p>Date:</p>	

3. OTHER RECOMMENDED CYBERSECURITY PRACTICES

- **IT Asset Management** – The company should establish the responsibilities to analyse all IT assets, determine their sensitivity and importance to the institution, and their vulnerability to potential cyber threats.
- **Third Party Service Providers’ Due Diligence** - The company should assess and manage its exposure to cyber risks that may affect the confidentiality, integrity, and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership.
- **Configuration Management** - The company should implement a configuration management process to maintain accurate information of its hardware and software, to have visibility and effective control of its IT systems.
- **Patch Management** – The company should establish a patch management process to ensure applicable functional and non-functional patches (such as fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with the criticality of the patches and the company’s IT systems.
- **Change Management** - The company should establish a change management process to ensure changes to information assets are assessed, tested, reviewed, and approved before implementation.
- **Problem Management** - The company should establish appropriate problem management processes and procedures to determine and resolve the root cause of incidents to prevent the recurrence of similar incidents.
- **User Access Management** – The company should develop a user access program to implement and administer physical and logical access controls to safeguard the institution’s information assets and technology.
- **Remote Access Management** – The company should develop policies to ensure that remote access by employees, whether using company or personally-owned devices, is provided in a safe and sound manner.
- **Data Security** - The company should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data.
- **Network Security** - The company should deploy effective security mechanisms to protect information assets.
- **Cloud Services** – The company’s plans for the use of cloud computing services should align with its overall business and IT strategy, architecture, and risk appetite. The company should develop a policy document governing the use of cloud computing.

Companies' risk management frameworks should facilitate the conduct of appropriate due diligence to manage the risks associated with Cloud Service Providers, as well as their material sub-contracting arrangements.

- **Customer Authentication** - Multi-factor authentication should be deployed at login for online financial services to secure the customer authentication process, including end-to-end encryption for the transmission of customer passwords.
- **Information Sharing** - In the absence of formal structures, companies are encouraged to form an informal, open, self-organized group, where members publish timely threat information to the group on a voluntary, ad hoc basis to facilitate prevention of cyberattacks, thereby contributing to its own cyber resilience and that of the broader financial sector.
- **Remediation Management** - A comprehensive remediation process should be established to track and resolve issues identified from the cyber security assessments or exercises.

DRAFT

APPENDIX I - DEFINITIONS¹ / ABBREVIATIONS

For the purpose of this Guideline, the following definitions are provided:

asset	refers to information and data, hardware, software, documents, communication equipment, business processes, buildings and employees
business continuity plan	A plan that focuses on keeping business operational in the face of a threat or a disaster.
cyberattack	An attack, via cyberspace, targeting an institution's use of cyberspace for the purpose of disrupting, disabling, destroying; or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
cyber incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein; or an event during which computer systems and/or computer-embedded systems are attacked by, or on behalf of, adversaries (external or internal to the financial institution), which could lead to the materialization of cyber risk.
cyber risk	The potential for damage resulting from an occurrence of a cyber incident, taking into account its probability and its impact.
cybersecurity	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

¹ Computer Security Resource Centre (CSRC); Federal Financial Institutions Examination Council (FFIEC); National Institute of Standards and Technology (NIST); Bank of Ghana – Cyber and Information Security Directive, October 2018; European Banking Authority – Guidelines on ICT and Security Risk Management, November 2019; Monetary Authority of Singapore – Technology Risk Management Guidelines, January 2021.

cybersecurity strategy

The high-level plan(s) for how an organization will go about securing its assets and minimizing cyber risk. Typically, cybersecurity strategies are developed with a three-to-five-year outlook but should be updated and revisited as frequently as possible. The cyber security strategy should be aligned with the financial institution's overall business strategy and should be adaptable to the threat landscape.

disruption

An unplanned event that causes an information system or major applications, to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

multi-factor authentication

The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number {PIN}); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric).

resilience

Means the ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a timeframe consistent with mission needs.

APPENDIX II - CYBERSECURITY INCIDENT REPORTING

INSTRUCTIONS

Purpose

- The Central Bank is introducing a **Cybersecurity Incident Report** to facilitate its awareness of, and response to, cyber security incidents at all regulated financial institutions.
- All companies have a responsibility to address cybersecurity incidents in a timely and effective manner and are required to provide timely notification to the Central Bank when material incidents relating to their operations occur. This requirement should be reflected in the company's policies and procedures for dealing with cyber security incidents.

Reportable Incidents

- Companies should define priority and severity levels within their incident management framework.
- A reportable incident may have **one or more** of the following characteristics of a material nature:
 - ❖ Impact has potential consequences for other companies or the domestic financial system;
 - ❖ Impacts the company's systems affecting financial market settlement, confirmations or payments (e.g., Financial Market Infrastructure), or impact to payment services;
 - ❖ Impacts operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity or availability of customer information;
 - ❖ Disrupts business systems and/or operations, including but not limited to utility or data centre outages or loss or degradation of connectivity;
 - ❖ Causes the disaster recovery teams or plans to be activated or a disaster declaration has been made by a third party vendor that impacts the company;
 - ❖ Impacts a number of external customers and/or negative reputational impact is imminent (e.g., public and/or media disclosure);
 - ❖ An incident assessed by a company to be of high or critical severity, or ranked Priority/Severity/Tier 1 or 2 based on the company's internal assessment; or
 - ❖ Incidents that breach internal risk appetite or thresholds as per the cybersecurity strategy or policy.

- For incidents that do not align with or contain the specific criteria listed above, or when a company is uncertain, notification to the Central Bank is encouraged.

Initial Notification Requirements

- As soon as possible but within **24 hours** of becoming aware of a cyber-incident, the company shall alert the Central Bank, that a cyber-incident has occurred.
- The company should complete the Cyber Incident Reporting Template below and submit to the Central Bank within **48 hours** of the incident.
- Where specific details are unavailable at the time of the initial report, the company must indicate 'information not yet available.' In such cases, the company must provide best estimates and all other details available at the time including their expectations of when additional information will be available.

Subsequent Reporting Requirements

- The Central Bank expects the company to provide regular updates (e.g., daily) as new information becomes available, and until all details about the incident have been provided.
- Until the incident is contained/resolved, the Central Bank expects the company to provide situation updates, including any short term and long-term remediation actions and plans.
- Following incident containment, recovery and closure, the company should report to the Central Bank on its post-incident review and lessons learnt.

Failure to Report

- Failure to report incidents as outlined above may result in increased supervisory oversight including, but not limited to, enhanced reporting by the company, and/or the issuance of compliance directions as relevant.

CENTRAL BANK OF TRINIDAD AND TOBAGO	
CYBER INCIDENT REPORTING TEMPLATE	
<i>Particulars and Details of Incident</i>	
Name of Financial Institution:	
Reporting Officer's Name:	
Reporting Officer's Position:	
Reporting Officer's Email & Phone Number:	
Date and Time of Notification:	
Date and Time Incident Discovered / Detected:	
Incident Level or Priority:	
Type of Incident that occurred (e.g. Ransomware, Phishing, Data Breach / Leak, Insider Threat, DDoS):	
Provide the Indicators of Compromise (IOCs):	
Indicate Actions Taken:	
<i>Impact Assessment (examples are given but not exhaustive)</i>	
Business Lines Impacted (including availability of services – Treasury Services, Cash Management, ATM, Internet / Mobile Banking, etc.):	
Stakeholders Impacted:	
Financial and Market Impact (trading activities, liquidity impact, transaction volumes and values etc.):	
Reputational Impact:	
<i>Detailed chronological order of events</i>	
Date of Incident, Start Time and Duration (DD/MM/YY):	
Escalation Steps Taken:	
Stakeholders Informed or Involved:	
Channels of Communication Involved:	

CENTRAL BANK OF TRINIDAD AND TOBAGO	
CYBER INCIDENT REPORTING TEMPLATE	
<i>Root Cause Analysis</i>	
Factors that caused the problem / reason for occurring:	
Interim measures to mitigate / resolve the issue:	
<i>Final Assessment and Remediation</i>	
Current state of incident:	
Actions completed and pending:	
Conclusion on cause and effects of incident:	
List the corrective actions taken to prevent future occurrences of similar types of incident:	
Estimated timelines to address the remediation of the incident (DD/MM/YY)	

DRAFT

APPENDIX III - RELEVANT REFERENCE MATERIAL

- Banks for International Settlements, Financial Stability Institute (“FSI”) Insights on policy implementation No 50 – Banks’ cyber security – a second generation of regulatory approaches – June 2023: <https://www.bis.org/fsi/publ/insights50.pdf>;
- Federal Financial Institutions Examination Council (“FFIEC”) Information Technology Examination Handbook: Information Security - September 2016: https://www.ffiec.gov/press/pdf/ffiec_it_handbook_information_security_booklet.pdf;
- FFIEC Cloud Computing Statement, April 2018: https://www.ffiec.gov/press/pdf/FFIEC_Cloud_Computing_Statement.pdf
- Financial Stability Board (“FSB”) Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence – October 2021: <https://www.fsb.org/wp-content/uploads/P191021.pdf>;
- G-7 Fundamental Elements for Threat-Led Penetration Testing, October 2018: <https://www.bundesbank.de/resource/blob/764690/792725ab3e779617a2fe28a03c303940/mL/2018-10-24-g-7-fundamental-elements-for-threat-led-penetration-testing-data.pdf>;
- NIST Framework for Improving Critical Infrastructure Cybersecurity – April 2018: <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>;
- NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations – September 2020: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>;
- NIST Special Publication 800-150 - Guide to Threat Information Sharing – October 2016: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf>.