Cybersecurity Best Practices Guideline
Industry Comments Table of Responses

No.	Section / Reference	Comments	CBTT Response
1.	**Introduction**	The Introduction appears to need some elaboration and misses some key high level points from which the rest of the guide should pull: 1. **Risk-Based Approach:** Encourage companies to conduct risk assessments tailored to their unique business models, operations, and threat landscape to develop cybersecurity frameworks that address their specific risk profiles. 2. **Consider International Best Practices:** Explore and integrate internationally recognized cybersecurity best practices and standards to enhance the effectiveness of the guideline.	The introduction was amended to reinforce a risk-based approach in conducting the self-assessment. Words were included in the Introduction that indicate that the principles are consistent with international best practice.
2.	**Introduction - Scope of Application** First paragraph, last line Second paragraph, first line	Full name of the Central Bank should be included in the first paragraph (not the second) Central Bank of Trinidad and Tobago (Central Bank/Bank)	Amended
3.	**Scope of Application**	The Scope of application provides a little ambiguity: 1. **Clarify Relationships with Other Guidelines:** Clearly define how the Cybersecurity Best Practices Guideline interacts with the Bank's Corporate Governance Guideline and the Guideline for the Management of Outsourcing Risks. Explain the dependencies, overlaps, or specific areas	The section stipulates that companies should also have regard to guidelines listed in the section when establishing their cybersecurity frameworks. Companies are therefore required to review these guidelines in tandem with any new guidelines being issued. No change required.

No.	Section / Reference	Comments	CBTT Response
		where they complement each other. At least a marker can be placed here for reference in an index. 2. **Provide Adaptation Guidelines:** For institutions not regulated by the Central Bank, offer guidance on how they can adapt the provisions of the guideline to suit their specific industry and risk profiles. This will help ensure consistency and effective risk management across various sectors. 3. **Consider Adoption Incentives:** Explore providing incentives for companies, both regulated and non-regulated, to adopt the guideline voluntarily. This could include public recognition for compliance, access to resources or funding for cybersecurity initiatives, or reduced insurance premiums for companies that meet specific cybersecurity standards.	Note that this guideline is a compulsory requirement for institutions licensed or registered by the Central Bank. The guideline was established in collaboration with other domestic regulators. Accordingly, institutions regulated under a separate legislative ambit should obtain guidance from their respective regulator. This is not in the purview of the Central Bank. The incentives for a company to adopt robust cybersecurity is protecting their customers and themselves from the risk of loss of data / information with potentially devastating impact on the company's reputation.
4.	**1 – Scope of Application –** "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	**Consider adding**: Electronic Transfer of Funds Crime Act, 2000, Data Protection Act *CHAPTER 22:04* ... Act. 13 of 2011 Cybercrime Bill No. 15 of 2017/Computer Misuse Act	The Bank's Guideline on Security Systems for Safeguarding Customer Information has been included in the paragraph. Note that the Bank expects all companies to consider any other related pieces of legislation not under the ambit of the Central Bank.

No.	Section / Reference	Comments	CBTT Response
	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."	CBTT'S Guideline on Security Systems for Safeguarding Customer Information	
5.	**Scope of Application**	It is noted that other institutions not regulated by CBTT are encouraged to adopt the guideline, would these institutions need to report to CBTT in relation to this guideline?	No. Companies not regulated by the Central Bank will not be required to report to the Central Bank.
6.	**Introduction - Supervision and Enforcement**	In respect of annual self-assessments against the Guideline, it is noted that the Guideline states that Companies should attach detailed action plans to remedy any material deficiencies uncovered. It may be helpful to state specifically that action plans or details should be in attached in cases of "partially compliant" or "not compliant" areas. Alternatively, state that the Central Bank may request additional details in cases of "partially compliant" or "not compliant" areas.	The guideline already facilitates the Central Bank's review of the self-attestation, independent reviews and any other relevant information submitted. Additionally, as part of its monitoring function, the Central Bank will discuss developments and periodically conduct risk based on-site examinations to verify compliance with the Guideline.
7.	**Introduction - Supervision and Enforcement** Second to last paragraph	Consider including a full stop after the "2.A" reference From "2.A" to "2.A."	Amended
8.	**Supervision and Enforcement**	The Supervision and Enforcement Section is short and misses some major plots: 1. **Frequency of Supervision:** The section mentions that companies should conduct	The Central Bank utilises a risk-based approach to supervision. Consequently, the frequency of onsite

No.	Section / Reference	Comments	CBTT Response
		annual self-assessments and submit them to the Central Bank by the following January. However, it does not specify how often the Central Bank will conduct risk-based on-site examinations. Clearly define the frequency of risk-based on-site examinations conducted by the Central Bank to ensure consistent and timely oversight of companies' cybersecurity practices.	examinations will depend on the risk profile of the institution based on self-assessments and other information.
		2. **Clarity on Material Deficiencies:** The guideline requires companies to attach detailed action plans to remedy any material deficiencies uncovered during self-assessments. However, it doesn't clearly define what constitutes "material deficiencies." This lack of clarity could lead to inconsistent interpretations by companies. Provide a clear and concise definition of "material deficiencies" to ensure companies have a uniform understanding of the severity of issues that need to be addressed promptly.	A definition for "material deficiency" has been added in Appendix I to provide clarity.
		3. **Include Third-Party Assessments:** Encourage companies to obtain independent third-party assessments regularly and submit those reports to the Central Bank along with their self-assessments. This can enhance objectivity and reliability in evaluating cybersecurity measures.	Section 2A. 4th bullet point already requires the company to perform independent reviews through their internal audit department, as well as, outsource the conduct of an independent review to a third party.

No.	Section / Reference	Comments	CBTT Response
		4. **Establish Escalation Protocol:** Develop an escalation protocol for serious or urgent cybersecurity concerns identified during self-assessments or on-site examinations, ensuring that critical issues are addressed promptly.	As part of its onsite examination process including any review of the assessments, the Central Bank provides recommendations to the institution on identified deficiencies with specific timeframes and ongoing follow-up for remedial action.
		5. **Incorporate Incident Reporting:** Require companies to report any major cybersecurity incidents to the Central Bank promptly. This will help the regulator stay informed about emerging threats and take appropriate actions if necessary. There should be a statement here also and not just the section later in the document.	Incident reporting should be part of the company's incident management framework, which we believe is clearly outlined in section 2F and which also clearly articulates reporting to the Central Bank in the second bullet point.
		6. **Provide Feedback and Support:** The Central Bank should offer feedback and support to companies after reviewing their self-assessments and independent reviews. This could include providing guidance on addressing identified deficiencies or offering resources to help improve cybersecurity practices.	The Central Bank as the regulator is not in a position to offer resources to assist in improving cybersecurity practices. However, as part of its onsite examination process including any review of the assessments, the Central Bank provides recommendations to the institution to address identified deficiencies with specific timeframes for action.
9.	**Introduction – Supervision and Enforcement**	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	The suggested re-wording is noted however the Bank opines that the current wording adequately reflects the requirements.

No.	Section / Reference	Comments	CBTT Response
		other relevant information, discuss developments and periodically conduct risk based on-site examinations to verify compliance with the Guideline. **Consider Re-wording:** Licensees are expected to perform an assessment of the Cyber Security Best Practices Guideline ("the guideline") against their current cyber security framework to identify any gaps and to develop and execute a plan of action to ensure compliance with the guideline. Periodic risk based on-site examinations will be carried out to verify compliance with the Guideline and during this verification any related independent reports will be requested for review.	
10.	**Section 1 - 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."	To avoid companies performing self-assessments so early that the results submitted are outdated, The Guideline should include a period during which the self-assessment should be conducted e.g. 4th quarter or 2nd half of each calendar year. The Guideline should also specifically state by "January 31st the following year" for avoidance of doubt.	The wording has been amended for clarity.
11.	**Supervision and Enforcement -** "Companies should conduct annual self-assessments against the Guidelines and submit these to the Central Bank by the following January."	Our understanding is that the first self-assessment will be due in January following the official promulgation of this 'draft' Cybersecurity Guidelines document by CBTT – Please confirm that mean earliest by Jan 2024?	The submission timeframe for the self-assessment has been amended to March 31st of each year.

No.	Section / Reference	Comments	CBTT Response
12.	**Introduction – Supervision and Enforcement**	If the intention is to implement the timeline for reporting as January 2024, consider revising this timeline as this may be a bit aggressive for institutions to complete and submit in time due to the timeliness of awareness of the requirements. Recommendation: Include contact information or instructions for submission of assessments.	See previous comment.
13.	**Supervision and Enforcement**	1. Submission date of January for the self-assessment is vague; kindly provide a more definite date. Eg. January 31st 2. For most if not all FIs, the first portion of the calendar year is exceptionally busy. Can consideration be given to move the date for submission of the self-assessment to later in the year? Possibly May or June? 3. We note that there is a requirement for both an annual review and a self-assessment. The requirement for both seems counterproductive and adds to the increasing demands by the CBTT to FIs. Can consideration be given to having a reporting requirement for the annual review alone? The suggested self-assessment format can be used as a guide/standard format for the annual review.	The guideline currently states January 31st as the official submission date. The submission date for the self-assessment has been amended to March 31st of each year. The Central Bank expects companies to conduct the exercises simultaneously since the self-assessment is intended to assist in the company's annual review of its cybersecurity practices.
14.	**1 – Supervision and Enforcement** - "Reports of	Self-assessment? Consistency needed	The only annual requirement is for submission of the self-assessment. However, if the company has also conducted an independent review, either through its

No.	Section / Reference	Comments	CBTT Response
	independent reviews referred to in section 2.A of the Cybersecurity Guidelines should also be submitted"		internal audit department or another third party, this report should also be submitted to the Central Bank. It is noted that section 2A states that the independent reviews should be performed **regularly**, which does necessarily mean annually. The Internal Audit department will determine the frequency for such reviews in alignment with the company's complexity and risk profile.
15.	**2 - Cybersecurity Guidelines**	First paragraph states that the self-assessment/attestation should be signed by the Chief Executive Officer or his/her designate. However, the signature section of the attestation form states "Name of Board Member/ Representative". Ensure that the self-assessment/attestation is consistent regarding the person required to sign.	Amended to: Name of Chief Executive Officer / Designate):
16.	**2: Cybersecurity Guidelines -** "…and signed by the **Chief Executive Officer** or his/her designate."	To underscore the significance of cybersecurity and the self-assessments/attestations to both the Bank and the financial *services* community, *I suggest that the Chairperson of the financial institution's Board of Directors (or their designate) be included as a signatory*	Amended to: Name of Chief Executive Officer / Designate):
17.	**2 - Cybersecurity Guidelines -** "This self-assessment/attestation should be submitted annually to the Central Bank and signed by the Chief Executive Officer or his/her designate"	We believe that, given the effort & cost involved in self-assessment and independent review, a once in 2- or 3-years self-assessment would be more effective instead of an 'annual' on	The Central Bank acknowledges the comment. However, given the rapid changes occurring and increasingly associated risks in digitalization of products and services, it is the Central Bank's expectation that companies will implement a more robust review of its cybersecurity practices. The annual assessment is therefore not considered

No.	Section / Reference	Comments	CBTT Response
			unreasonable. Please note that there is no requirement for an annual independent review, the frequency of which should be determined by the Board/ Audit Committee/ Internal Audit based on the institution's size, complexity and risks.
18.	**2 - Cybersecurity Guidelines – page 5**	1. Shouldn't the heading read "Name of Chief Executive Officer/Designate" instead of "Name of Board Member/Representative" as per heading No. 2 – "Cyber Security Guidelines"? 2. There should be a designated area on the self-assessment form where the FI can provide any additional comments if applicable	Amended to: Name of Chief Executive Officer / Designate): Any additional comments can be provided in a separate document and submitted with the self-assessment to the Central Bank.
19.	**2 - Cybersecurity Guidelines –** "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."	**Recommendation:** An annual date should be specified (e.g. Jan 31 reporting on the prior year)	The submission date is stated in the introductory section (Section 1) under "Supervision and Enforcement"
20.	**2 – Cybersecurity Guidelines –** "This self-assessment/attestation should be submitted annually to the Central Bank and signed by the Chief Executive Officer or his/her designate."	It is suggested that the designate should be CISO (Chief Information Security Officer) or CCO (Chief Compliance officer), as per global best practices (NIST, FFIEC, ISO270001)	This has been amended to: Name of Chief Executive Officer / Designate): The designate may include the CISO or CCO, once the individual is an approved officer of the Bank in accordance with the Financial Institutions Act.

No.	Section / Reference	Comments	CBTT Response
21.	**Cybersecurity Guidelines**	We think perhaps for each of the 20 requirements being assessed, to include an area for comments/remarks to explain the rating of Green, or Amber, or Red. The document is very comprehensive thus, no further feedback warranted.	Any additional comments can be provided in a separate document and submitted with the self-assessment to the Central Bank.
22.	**2 - Cybersecurity Guidelines**	For ease of reference, consider inclusion of 'traffic signal key' at the beginning, rather than the end of self-assessment questionnaire.	Dropdown boxes have been inserted to replace the traffic signal key.
23.	**2 - Cybersecurity Guidelines**	The standard cybersecurity rating follows a five-stage maturity process as CMMI rather than a traffic signal format which would provide greater objectivity.	The comment is noted. Capability Maturity Model Integration (CMMI) is a process level improvement training and appraisal program, which is not the Central Bank's objective in issuing this guideline. This assessment is a simple process to measure compliance with cybersecurity best practices.
24.	**2A – Governance -** "The Internal Audit and Risk Departments should perform **regular independent reviews** of compliance…"	As "regular" is a vague timeframe, I suggest that the guidelines be more specific. Also, to mitigate potential biases and ensure independent cybersecurity reviews, I suggest that supervised entities undergo mandatory reviews by external third-party auditors at least once every 2-3 years, *with the larger firms (based on employee count, and/or gross annual revenue, and/or already established criteria) having to perform this review annually. Larger firms may already be performing similar annual reviews, especially if they utilise payment systems such as SWIFT and international credit cards.* The resulting reports and action plans could also be submitted to the Bank *as part of the annual submission, if desired.* Comparing these third-party reports with the firm's own assessments should enhance transparency and	The frequency of these reviews should be determined by the company in collaboration with its Board and/or Audit committee and should be in accordance with the complexity and risk profile of the company.

No.	Section / Reference	Comments	CBTT Response
		contribute to the entity's cybersecurity maturity, benefiting the local financial system.	
25.	**Cybersecurity Guidelines - Section 2 A - Governance**	**Lack of Incident Reporting Protocol:** The section discusses regular independent reviews by the Internal Audit and Risk Departments, but it doesn't explicitly emphasize the importance of establishing an incident reporting protocol within the company. Develop and implement a clear and accessible incident reporting protocol that allows all staff to report cybersecurity incidents promptly and securely. The protocol should define the types of incidents to be reported and the relevant channels for reporting.	Refer to section F which treats with Incident Management and Reporting. It is noted that the document is a principles based document outlining the best practice requirements. Companies are expected to adopt such best practices for incident reporting and include in its policies and procedures, the details of the reporting protocol within the business.
26.	**Cyber Security Guidelines – 2 A. Governance**	"The Internal Audit and Risk Departments should **perform regular independent reviews** of compliance with the cybersecurity strategy and policies and make relevant recommendations." **Feedback:** Clarification is required on the expectation of the frequency re: the performance of "**regular independent reviews".** Please note that the information and cyber security annual planning process is conducted at the bank level and uses a risk-based approach. Our annual coverage is risk based, driven by our assessment of inherent risk and effectiveness of controls, which is informed by audit work, issues management and continuous monitoring of the business. The audit cycle is to cover entities / RAD (Risk Assessment Database) evaluated as higher risk every 28 months, moderate risk every 36 months,	The Central Bank clarifies that the only annual requirement is for submission of the self-assessment. The frequency of the independent reviews should be determined by the company in collaboration with its Board and/or Audit committee and should be in accordance with the complexity and risk profile of the company.

No.	Section / Reference	Comments	CBTT Response
		and lower risk every 60 months. Audit work is determined according to a defined audit universe and cycle approach with the objective to cover all critical processes and controls related to the NIST CSF in cycles of three years. As the majority of processes, controls, and technology for management of information and cyber security risk are centralized in Canada, the assessment of centralized controls and exceptions identified as part of the audits conducted by the Audit team at Executive Offices have a global impact which includes IT operations in Trinidad and Tobago. Based on the above, is there a requirement to have a Trinidad and Tobago specific report or can this Global reporting that includes Trinidad and Tobago Operations suffice?	
27.	**2.A.2 – Governance -** "The Board should approve the cybersecurity strategy and be kept informed of developments on a quarterly basis."	The Guideline should require the Cybersecurity Strategy to be reviewed and updated on at least an annual basis.	The statement was amended as follows: *"The Board should approve the cybersecurity strategy and be kept informed of developments* ***in accordance with the complexity and risk profile of the company."*** Section 6.4 of the Corporate Governance Guideline states that *"Senior management should keep the Board regularly and adequately informed of material matters, including proposed changes in business strategy, risk strategy/risk appetite…"* Consequently, the frequency of review/ update of the strategy should be determined by the Board/ Sen Mgmt. The Central Bank will comment however if there are material developments taking place and

No.	Section / Reference	Comments	CBTT Response
			there is no evidence of review/ update of the strategy.
28.	**2.A.4 – Governance –** "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."	Why would both Internal Audit and Risk Departments need to perform these reviews? That could result in duplication of effort, which could be disruptive, particularly in smaller organizations. Is there a minimum frequency for these reviews?	Agreed. The statement has been amended to state that the Internal Audit Department should perform regular independent reviews. The frequency of the independent reviews should be determined by the company in collaboration with its Board and/or Audit committee and should be in accordance with the complexity and risk profile of the company. However, companies are not restricted from allowing their risk departments to conduct a similar independent review. Section 8.5 of the Corporate Governance Guideline states that *"Key activities of the risk management function should include inter alia:* *a) identifying and assessing material individual, aggregate and emerging risks, and measuring the financial institution's exposure to them."*
29.	**2-A Governance**	Recommendation: inclusion of a clause indicating that boards should include members with cybersecurity expertise or experience to provide effective oversight of cyber risk management	The Central Bank advises that as stated under "Scope of Application" this guideline should be read in conjunction with the Bank's other issued guidelines including the Corporate Governance Guideline. Sections 4.1 and 4.5 of the Corporate Governance Guideline provides further guidance.

No.	Section / Reference	Comments	CBTT Response
30.	**2A – 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:"	Internal Audit is the 3rd line and Risk is the 2nd Line of Defense. Therefore, realign when using the IIA profession language of lines of defense. Role of IA does not include implementing a defined cybersecurity plan. IA is an independent objective assurance activity that reports to the Board and Senior Management. IA provides assurance to the Board and Senior Management of effectiveness and efficiency of Management designed controls. **Remove and Reword Internal Audit from: "must be formally involved in implementing a defined cybersecurity plan"** The statement can result in IA no longer being independent and objective.	Noted and re-ordered to align with their positions in the line of defense model. The Central Bank notes that the statement does not directly require Internal Audit to implement the plan. Rather, it states that they should be formally involved. Consequently, the wording has been amended slightly for clarification. The input of Internal Audit is not uncommon for providing feedback on best practice, prior to implementation of the initiative.
31.	**2-A – Governance - 4th Bullet point –**	There should be a cross reference to CBTT's Outsourcing Guideline in this sentence	A statement is already provided in section 1 under "Scope of Application", which references the Outsourcing Guideline.
32.	**2-A – Governance -** "The Board should approve the cybersecurity strategy and be kept informed of developments on a quarterly basis."	**Query:** Based on the Group Corporate structure for GKMS, the security strategy is approved at a divisional level and covers the GKMS Group, which covers GKTT. Would this be considered satisfactory to be compliant for GKTT? **Recommendation:** Quarterly updates may be too frequent as this may imply updates at every Board meeting. GKTT recommends the following: - Board approval of the strategy and at least one subsequent update in the calendar year.	The institution must be able to demonstrate how the Group policy is relevant for the financial institution and how it satisfies the requirements of this Guideline for each regulated entity in the group. Section 7.4 of the Bank's Corporate Governance Guideline provides further guidance. advises The statement was amended to read as follows: *"The **Board should approve the cybersecurity strategy** and be kept informed of developments at least annually or more frequently* at least annually or more frequently if material issues arise.

No.	Section / Reference	Comments	CBTT Response
33.	**2-A – Governance -** "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. "	**Query:** Such reviews may be done at the GKMS parent company level covering technology resources leveraged across multiple countries including Trinidad and Tobago. Will such annual reviews be considered satisfactory to meet the GKTT compliance requirements?	See response above.
34.	**2-A –Governance -** Board Approval of Cyber Security Strategy	Can consideration be given for informing the Board at a minimum at each Board meeting or more frequently, if necessary?	The statement was amended to read as follows: *"The **Board should approve the cybersecurity strategy** and be kept informed of developments* at least annually or more frequently if material issues arise.
35.	**2-A – Governance -** Internal Audit and Risk Department	We assume that "regular reviews" would be defined by the FI. Despite this can a more definite time frame be established for reporting to CBTT? E.g. Within 30 days of the date of the report?	The frequency of the independent reviews should be determined by the company in collaboration with its Board and/or Audit committee and should be in accordance with the complexity and risk profile of the company.
36.	**2-A – Governance –** "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."	Is there an opportunity for this to be Group based or for the provision of Group support where the entities belong to a Conglomerate? What is the position where the business is also governed by IT security policies of key stakeholders with whom they interact? What is the timeline for implementation? This would give adequate time for gap analysis, resourcing, development, training, cost allocation and implementation	The institution must be able to demonstrate how the Group policy is relevant for the financial institution and how it satisfies the requirements of this Guideline for each regulated entity in the group. Section 7.4 of the Bank's Corporate Governance Guideline provides further guidance. advises The first self-assessment against the Guideline must be submitted by March 31, 2024 and annually thereafter.

No.	Section / Reference	Comments	CBTT Response
37.	**2-A - Governance**	The IT /IT Security department is the centre of cybersecurity however is excluded in the governance line.	The IT Department has not been excluded. Companies are expected to determine all of the necessary departments required to assist in implementing the defined cybersecurity plan.
38.	**2-A - Governance**	Organizational setup of IT Security Governance function should be separate to those executing it.	Agreed. The Central Bank considers that approach as best practice.
39.	**2.B. - Risk Management**	The risk management and incident management framework should have well defined roles, responsibilities, and reporting lines across the different functions/entities. This was not mentioned in the Guideline. Consider including.	The Central Bank advises that as stated under "Scope of Application" this guideline should be read in conjunction with the Bank's other issued guidelines including the Corporate Governance Guideline. This guideline outlines best practices regarding the specific roles and responsibilities within your corporate governance structure.
40.	**2 B - Risk Management**	**Inadequate Attention to Outsourcing Risks:** The guideline mentions outsourcing risks, but it doesn't provide specific details on how companies should assess and manage these risks effectively. Elaborate on the specific aspects of outsourcing risks that companies should assess, such as third-party provider reliability, data security practices, and contractual arrangements to ensure robust risk management.	Refer to section 1 which states that the Guideline should be read in conjunction with the Outsourcing Guideline which treats with those issues.
41.	**Cybersecurity Guidelines – Risk Management** – "The risk management framework should identify the cyber security threats and vulnerabilities applicable to the IT environment, including internal and external	Suggested re-wording as follows: The risk management framework governs an organization that identifies cyber security threats and vulnerabilities applicable to the IT environment, including internal and external networks, hardware, software applications, systems interfaces, operations procedures, and people.	Noted. The Central Bank opines that it is implicit for a risk management framework to be part of the governance structure of an organization. No change is required.

No.	Section / Reference	Comments	CBTT Response
	networks, hardware, software applications, systems interfaces, operations procedures, and people."		
42.	**Cybersecurity Guidelines – Risk Management –** "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."	Suggested re-wording as follows: 'Policies should be implemented to ensure that the organization implements a controlled change management process which includes effective management of security concerns including patches	Section 3 provides guidance on other recommended cybersecurity practices including change management.
43.	**Cybersecurity Guidelines – Risk Management –** "An explicit incident management framework should be developed…"	Suggested re-wording as follows: An incident management policy governs an organization, that encourages reporting by staff, incorporates regular, systematic reviews of incidents and measures for improvement ….	Further guidance on incident management reporting is expressed in Appendix II
44.	**2-B - 2nd bullet point - Risk Management -** "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."	Consider including the word risks rather than problems.	Agreed and amended.
45.	**2-B – Risk Management**	The implementation of both an explicit cybersecurity incident management framework and risk management framework would be deemed as onerous. One risk management framework to	Companies should weigh the efficiency of including the cybersecurity incident management framework in a standalone document versus embedding it in one risk management framework.

No.	Section / Reference	Comments	CBTT Response
		include/address cybersecurity would be suitable based on best practice.	
46.	**2-B – Risk Management –** "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.	Revision needed. Data should be included as well.	The word "data" has been included.
47.	**2-B – Risk Management – "**Policies should be implemented to assure that IT security is updated……."	How is IT security defined here. What is updated?	The section has been amended to read as follows: *"The company should ensure that policies and procedures for **information security** are implemented and regularly reviewed and updated."*
48.	**2-B – Risk Management –** "An explicit incident management framework should be developed, encouraging reporting by staff and incorporating regular, systematic reviews of incidents and measures for improvement."	Companies may also have a 24-hr incident monitoring system, like SIEM. Who is the staff? Is it the IT staff? or employees?	Further guidance on incident management has been included in Section 3. It includes the following wording: *"Incident Management - The incident management framework should cover at a minimum:* • *the process and procedure for handling IT incidents, including cyber related incidents;* • *maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and*

No.	Section / Reference	Comments	CBTT Response
			• *the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents."*
49.	**2.C. - Awareness and Training**	Consider including training for the Board of Directors and service providers, and regular review of the training program to ensure that its content remain current and relevant. *<u>Below is an extract from the Draft Technology and Cyber Risk Management Guideline on the Barbados Financial Services Commission website for reference</u>* *Section 1. (F)* *(3) A training program should be undertaken annually for all staff, contractors and service providers who have access to the FI's information assets.* *(4) The board of directors should undergo training to raise their awareness of risks associated with the use of technology and enhance their understanding of technology and cyber risk management practices.* *(5) The training program should be reviewed regularly to ensure its contents remain current and relevant. The review should take into consideration changes in the FI's IT security policies, current and emerging risks, and the evolving cyber threat environment.*	Included in bullet point 1 – Training for Board of Directors is included. The company's due diligence of the service provider should ensure that it possesses the requisite competencies and provides for regular training of its staff. Refer to the Central Bank's Guideline for the Management of Outsourcing Risk section 5.4.
50.	**2C – Awareness and Training** 1. "Security awareness training should be provided to all employees…"	1. I suggest modifying the statement to: "Security awareness training should be provided to all employees **annually**, and the training records should	Statement was amended as follows: *"…training should be provided to all employees and Board members at least annually"*

No.	Section / Reference	Comments	CBTT Response
		be documented, and summary training reports should be made available to the Bank upon request."	
	2. “Higher level security training should be…” 3. Awareness training should also be mandated for Board Directors.	2. I suggest revising the phrase "Higher level security training" to clarify the different levels and types of training expected to be provided: "Tailored security awareness training should be provided to Managers and IT Staff, reflecting their varying levels of responsibility, as distinct from that provided to non-Management and non-IT staff." I suggest mandating Security Awareness training for Board Directors, as they bear the "ultimate responsibility for promoting, approving, and overseeing management's implementation of the financial institution's business and strategic objectives, governance, risk management and compliance frameworks, control functions, and corporate culture,"(3.1, pg. 9) and the “tone at the top” (3.9, pg. 11) of the Bank's March 2021 "Corporate Governance Guideline." The training provided to the Board should also be documented in a similar manner as outlined before in #1 of this part.	Statement was amended as follows: *“**Tailored security awareness training** should be provided to Managers and IT Staff, reflecting their varying levels of responsibility.”* Addressed in first statement above.
51.	**2 C - Awareness and Training**	**Insufficient Customer Awareness:** Without clear and effective customer training, there is a risk that customers may not understand the potential risks associated with using the company's IT tools, leading to security incidents or data breaches. Define the key elements that should be included in customer	Statement was rephrased as follows: *“**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.”*

No.	Section / Reference	Comments	CBTT Response
		training, such as privacy rights, security best practices, and how to report suspicious activities.	
52.	**Cyber Security Guidelines – 2C. Awareness and Training**	**1. AWARENESS AND TRAINING –** Regular and appropriate cybersecurity training must be provided to employees and customers in an understandable way. **Consider Re-wording:** **AWARENESS AND TRAINING –**Regular and appropriate cybersecurity training and awareness must be provided to employees in an understandable way. For customers' reasonable awareness should also be provided. **2. Higher level security training** should be provided for managers and those responsible for information technology. **Feedback:** Clarification required on what Higher **level security training** means. 3. **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. **Consider Re-wording:** **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, and the avenues for redress in case of problems.	See response above

No.	Section / Reference	Comments	CBTT Response
53.	**2.C.1 – Awareness and Training -** "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".	The Guideline should provide a minimum frequency for security awareness training, e.g. at least once a year.	Frequency of annually was added.
54.	**2.C.2 – Awareness and Training –** "Higher level security training should be provided for managers and those responsible for information technology."	The Guideline should provide a minimum frequency for security awareness training, e.g. at least once a year.	See response above
55.	**Cybersecurity Guidelines – Awareness and Training** – "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**,	Please Clarify what is defined as "key safety practices"	These would include practices implemented by the company to mitigate against any cybersecurity risks.

No.	Section / Reference	Comments	CBTT Response
	and the company's cybersecurity policies."		
56.	**Cybersecurity Guidelines – Awareness and Training –** "**Higher level security** training should be provided for managers and those responsible for information technology."	Please Clarify what is defined as "higher level security"	This statement was amended as follows: *"**Tailored security awareness training** should be provided to Managers and IT Staff, reflecting their varying levels of responsibility."*
57.	**2-C Awareness and Training –** this refers to cybersecurity training for employees and customers.	Recommendation: include the Board as a stakeholder that should receive regular and appropriate Cybersecurity training. E.g. "The company should offer ongoing training, education, and awareness programs for the board members to enhance their cybersecurity knowledge and skills."	The statement was amended to include training for board members.
58.	**Cybersecurity Guidelines - Section C - Awareness and Training – "**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."	We use social media channels, website notices and email blasts/advisories to advise clients on protecting themselves and their accounts while banking electronically. What additional tools are we expected to use to strengthen training for clients?	This statement was amended as follows: *"**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."*
59.	**2-C – Awareness and Training –** "Customers should receive adequate	More specificity is required here as customers are not compelled to attend training. Is training a requirement to accessing goods and services?	See response above

No.	Section / Reference	Comments	CBTT Response
	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."	Does this mean training re: the product the customer utilizes and not the IT tools? Would this specifically be training re: the software the Customer interacts with e.g. Online banking? Please clarify.	
60.	**2-C - Awareness and Training**	There is no added value to having a 'higher level security training as security can only be as 'strong as its weakest link'. While key personnel can be notified on the risks to the Company, the trainings for management and staff should be equal. Ongoing training for IT personnel on cybersecurity vulnerabilities and threats.	This statement was amended as follows: *"**Tailored security awareness training** should be provided to Managers and IT Staff, reflecting their varying levels of responsibility."*
61.	**2-C – Awareness and Training – "**Regular and appropriate cybersecurity training must be provided to employees and customers in an understandable way."	Mandatory annual cybersecurity training must be provided to all employees and vendors, who do business with companies.	A requirement for annual training has been included.
62.	**2-C – Awareness and Training –** "Security awareness training should be provided to all employees along with measures to assure participation and compliance with the training recommendations."	New employees and business partners are required to complete training within one week of hiring.	The document is principles based and we expect companies to adopt best practices in accordance with its complexity and risk profile.
63.	**2D – Business Continuity…**	"Tested regularly" is a vague timeframe. I suggest specifying a desired timeframe (e.g., annually) for testing to ensure prompt and reasonable compliance	The statement was amended as follows: "Business continuity and disaster recovery plans should be

No.	Section / Reference	Comments	CBTT Response
	"Business continuity and disaster recovery plans should be **tested regularly**…"	with this section of the Guidelines; this will also foster the ongoing improvement of the local financial system's cybersecurity maturity.	reviewed and **tested regularly** to validate their effectiveness.*"*
64.	**2 D - Business Continuity and Disaster Recovery**	**Unvalidated Plans:** Without regular testing, there is a risk that business continuity and disaster recovery plans may not be effective during actual cyber-related occurrences. Emphasize the importance of regularly testing business continuity and disaster recovery plans to validate their effectiveness. These tests should cover different scenarios, including cyber-related incidents.	See response above
65.	**2.D.3. – Business Continuity and Disaster Recovery –** "Where information assets are managed by third party service providers, companies should assess the service provider's disaster recovery capability."	Minimal guidance should be provided on how to assess a third party service provider's disaster recovery capability	The Central Bank advises that as stated under "Scope of Application" this guideline should be read in conjunction with the Bank's other issued guidelines including the Guideline for Management of Outsourcing Risks. Section 5.29 of the Outsourcing Guideline requires a company's senior management to: *"ensure that adequate business continuity and contingency plans are in place in the event that the service provider is unable to fulfil the outsourcing contract"*. Companies should also refer to section 5.6 of the Outsourcing Guideline that addresses Business Continuity and Contingency Plans.
66.	**2.D.4. – Business Continuity and Disaster Recovery –** "Business continuity and disaster recovery plans should be tested regularly to validate their effectiveness."	The Guideline should be provided a minimum frequency for testing of BCPs and DRPs e.g. at least once a year.	The requirement has been rephrased as follows: *"Business continuity and disaster recovery plans should be **reviewed and tested regularly** to validate their effectiveness."*
67.	**2-D – Business Continuity and Disaster Recovery –** "Business continuity and disaster recovery	Consider a defined time such as at least annually.	See response above

No.	Section / Reference	Comments	CBTT Response
	plans should be tested regularly to validate their effectiveness."	The document refers to Supervision and Enforcement Companies should conduct annual self-assessments against the Guidelines and submit these to the Central Bank by the following January.	
68.	**2-D - Business Continuity and Disaster Recovery -** "Business continuity and disaster recovery plans should be tested regularly to validate their effectiveness."	**Recommendation:** Since the Cyber Risk Strategy is risk based, then all components should follow the risk based approach including testing of the BCP. 'Regularly' in this instance is vague, and may create a challenge in guiding the Risk and Audit functions in establishing whether BCP/DRP testing frequency is adequate. The following is recommended: - Language along the lines of "to validate their effectiveness, Business continuity and disaster recovery plans should be tested at a frequency requisite for the risk profile of the entity, documented in the board approved cyber risk strategy."	See response above
69.	**2-D – Business Continuity and Disaster Recovery – "**Business Continuity and Disaster Recovery plans should be tested regularly to validate their effectiveness."	What would be the regular period? Once per year?	See response above
70.	**2-E - Business Continuity and Disaster Recovery** – "Business continuity and disaster recovery plans should be tested regularly to validate their effectiveness."	Define regularly. The best practice is annually. As well, Vendors should submit evidence of their annual test and results of test, and any mitigation plans/strategies, if necessary.	See response above
71.	**2E – Testing**	"Regular" is a vague timeframe. *I suggest specifying a desired timeframe* for the conduct of vulnerability	The frequency of these reviews should be determined by the company in collaboration with its

No.	Section / Reference	Comments	CBTT Response
	"The company should establish processes to **conduct regular** vulnerability assessments…"	assessments (VAs) once every 2-3 years, *using the firm's own Internal Audit and/or Risk Management resources or external consultants*. *I also suggest that the Guidelines be modified to* ***strongly recommend*** *the conduct of threat-led penetration tests (PTs) for* ***all*** *supervised entities.* *For larger firms (based on employee count, and/or gross annual income, and/or already established criteria), I suggest mandating the annual performance of VAs and/or PTs (which they may already be doing).* *The resulting reports and remediation plans arising from the conduct of these assessments and tests should be available to the Bank either as part of their annual submissions or upon request.*	IT Security department and should be in accordance with the complexity and risk profile of the company. Pen test comment – the following change was made: *"The company should* ***carry out*** ***penetration testing*** *(including threat-led penetration testing where appropriate) commensurate to the level of risk identified with the business processes and systems."*
72.	**2.E.1 – Testing –** "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 Guideline should be provided a minimum frequency for conducting vulnerability assessments e.g. at least once a year.	The frequency of these reviews should be determined by the company in collaboration with its IT Security department and should be in accordance with the complexity and risk profile of the company.
73.	**2.E.2 – Testing –** "The company should consider commissioning penetration testing (including threat-led penetration testing where necessary and	The Guideline should be provided a minimum frequency for conducting penetration testing e.g. at least once a year.	The frequency of these reviews should be determined by the company in collaboration with its IT Security department and should be in accordance with the complexity and risk profile of the company.

No.	Section / Reference	Comments	CBTT Response
	appropriate) commensurate to the level of risk identified with the business processes and systems."		
74.	**2-E – Testing - Bullet 2 -** 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.	Observation: 'Threat-led penetration' testing is a growing concept that is not yet well-established outside of the UK and the EU, as evidenced by the reference to the German Bundesbank in the appendix. Recommendation: We recommend excising the bracketed clause on threat-led penetration testing Observation: "should consider" followed by "commensurate to" may introduce too many qualifications Recommendation: We recommend strengthening to "The company should commission penetration testing when commensurate to the level of risk identified with the business processes and systems."	The following change was made: *"The company should **carry out** **penetration testing** (including threat-led penetration testing where appropriate) commensurate to the level of risk identified with the business processes and systems."*
75.	**2 E - Testing**	1. **Frequency of Vulnerability Assessments:** Define the frequency of vulnerability assessments based on the company's risk profile, industry standards, and the evolving threat landscape. 2. **Factors for Threat-led Penetration Testing:** Specify the factors that should determine whether threat-led penetration testing is necessary, such as the company's risk exposure,	The frequency of these reviews should be determined by the company in collaboration with its IT Security department and should be in accordance with the company's complexity and risk profile. Noted

No.	Section / Reference	Comments	CBTT Response
		criticality of assets, and potential impact of a successful cyber attack	
76.	**2-E – Testing** – "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".	Define "timely manner".	In line with the incident management reporting framework, companies should establish protocols and timelines for addressing risks. Further principles based guidance was also added in section 3.
77.	**2.F. - Incident Management and Reporting** Last bullet point	The sentence construction makes it hard to follow. Suggestion to remove the words 'in easy to understand language' altogether OR include the instruction in a separate sentence, see below: In case of a material incident, affected consumers should be promptly informed of the incident, implications and remedial measures. This should be done in an easy to understand language.	We have noted the comments and have amended this section to reflect the following. *"In the case of a material incident,* ***affected consumers should be promptly informed*** *of the incident, its implications and remedial measures taken. This should be communicated in an easy to understand language."*
78.	**2.F. -Incident Management and Reporting**	Would Incident management reporting need to be included in the institution's recovery plan? If yes, this should be mentioned under Section F	Companies should ensure that sufficient resources are available to facilitate and support incident response and recovery.
79.	**2F - Incident Management and Reporting** "In the case of a material incident, **affected consumers** should be promptly informed…"	While the Bank requires reporting of "all (cybersecurity) incidents considered to have a material impact on its business operations and consumers" within 24-48 hours (c.f. Appendix II, page 11), there is no specific guidance *on the*	Noted.

No.	Section / Reference	Comments	CBTT Response
		timeframe for reporting customer-affecting cybersecurity incidents to customers and the public. *I suggest incorporating a clear timeline for customer reporting, either in this Guideline or referencing another applicable Bank Guideline with an appropriate timeframe, provided this is possible or practical.* *I also suggest including a recommendation that the Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT) or the TTPS Cyber and Social Media Unit (CSMU) be contacted (if desired) for assistance with the conduct of investigations.*	
80.	**2 F – Incident Management and Reporting (Incident Response)**	1. **Define "Material Incident":** Provide a clear and concise definition of what qualifies as a "material incident." This could include criteria such as the severity of the incident's impact on business operations, customer data, or critical infrastructure. 2. **Establish Incident Notification Timeframe:** Set specific timeframes for notifying affected customers after a material incident occurs. The timeframe should be reasonable, ensuring that customers are informed promptly without compromising the accuracy of information. 3. **Communication Channels:** Clearly outline the communication channels through which customers will be informed of incidents. This may include email notifications, website announcements, or other suitable methods. 4. **Language and Format of Communication:** Ensure that the communication to affected	A definition for material incident has been added to Appendix I Refer to Appendix II Noted, it is expected that companies will have processes for notifying their customers. Noted

No.	Section / Reference	Comments	CBTT Response
		customers is presented in easy-to-understand language, free of technical jargon. Use a format that conveys the necessary information without overwhelming the recipients. 5. **Incident Management Framework:** Provide detailed guidelines on establishing an incident management framework, including incident categorization, escalation procedures, and roles and responsibilities of incident response teams. 6. **Post-Incident Analysis:** Encourage companies to conduct post-incident analyses to understand the root causes of cybersecurity incidents, identify areas for improvement, and implement remedial measures to prevent similar incidents in the future. 7. **Testing Incident Response Plans:** Regularly test incident response plans through simulation exercises (tabletop exercises, red teaming, etc.) to evaluate their effectiveness and identify areas for improvement.	Further guidance has been added to section 3. Note that this is a principles based document. Noted. High level guidance on remedial management is outlined in section 3. Noted
81.	**Cybersecurity Guidelines – Incident Management and Reporting –** "Information on key system changes and cybersecurity incidents that affect customers should be transparently communicated to	Please elaborate on: a. What constitutes an 'Information' or 'Key System Change'? b. Is there a requirement to inform CBTT of an 'information' or 'key system change'?	The word "key" has been changed to "material." This should now be assessed in conjunction with a material incident which has been defined in Appendix I.

No.	Section / Reference	Comments	CBTT Response
	them and to the relevant regulator."		
82.	**2-F – Incident Management and Reporting - Bullet 2 –** "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."	Recommendation: Define the term "material impact" as this may vary based on interpretation. E.g. Impact to financial reporting.	A definition for a material incident has now been included in Appendix I.
83.	**2-F - Incident Management and Reporting -** "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."	**Query and Recommendation:** Will there be guidance on classifying what is a "material impact"? If no, and this is self-determined, the following is recommended: - The use of a risk classification "High Risk" which considers not only the measure of severity, but also the velocity i.e. time to impact and as well the probability of occurrence. A material impact can occur in the short, medium or long term and as such, a risk measure would allow for alignment to the 1st, 2nd and 3rd line methodology of treating with such issues.	A definition for a material incident has now been included in Appendix I.
84.	**2-F - Incident Management and Reporting**	The establishment of an Incident Management Policy is sufficient to fulfil the objective of service restoration within the quickest possible timeframe. As such, an explicit and separate Incident Management framework (already included in the Policy) would not be applicable.	It is acceptable if a company has already combined the elements of its framework within its policy document.

No.	Section / Reference	Comments	CBTT Response
85.	**3 - Other recommended Cybersecurity practices**	Since this area is frequently changing and evolving and new risks are rapidly emerging – I would recommend that a suggestion along these lines be included i.e. For the institution to keep abreast of what's happening in the landscape and identify any emerging risks that may be happening in other countries etc. – this may seem like common sense, but it may be valuable to include it to reiterate that this is not a static area of focus.	Noted. The requirement to keep abreast would be covered under governance as the cybersecurity strategy has to be kept under constant review.
86.	**3 - Other Recommended Cybersecurity Practices**	I suggest sorting the list of recommended practices alphabetically unless there's a specific reason for the current order. *If the list will remain as is,* consider placing the "Cloud Services" *item* near the "Third Party Service Providers' Due Diligence" *item* since many Cloud Services Providers will also be Third Parties *to the firms.*	Section has been rearranged alphabetically.
87.	**3 – Other Recommended Cybersecurity Practices – Data Security**	Consider using "sensitive" instead of "confidential" as data classified as "internal" if lost may adversely affect the organization.	The word "sensitive" has been added.
88.	**3 – Other Recommended Cybersecurity Practices – Data Security – Cloud Services**	We suggest that Procedures and Standards be included.	The words "procedures and standards" have been added.
89.	**3 – Other Recommended Cybersecurity Practices – Data Security – Customer Authentication**	We recommend inserting the phrase "in alignment with industry best practices" immediately after encryption.	The words "industry best practice" have been added.
90.	**3 - Other Recommended Cybersecurity Practices**	Data privacy should be included here. After all, cybersecurity is the security of data in cyber space.	Noted

No.	Section / Reference	Comments	CBTT Response
91.	**3 - 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."	For cybersecurity, physical access is not included.	The words "physical access" have been removed, since the guideline is focused on cybersecurity and not technology risk.
92.	**3.13 – 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."	Is this meant to be an internal group or should we be looking at pushing the Association of Trinidad and Tobago Insurance Companies (ATTIC) to create such a group across the industry?	Industry groups or associations are encouraged to establish such structures to enhance information sharing capabilities for cybersecurity.
93.	**3 - Cybersecurity Guidelines** - The supporting controls section covers many area's some clarity can be given for the **Cloud Section**	**Cloud Services:** Lack of specific guidance on risk management for Cloud Service Providers and sub-contracting arrangements. Develop a policy document governing the use of cloud computing, ensuring alignment with the overall business and IT strategy and thorough risk assessments for Cloud Service Providers and sub-contractors.	The Central Bank advises that as stated under "Scope of Application" this guideline should be read in conjunction with the Bank's other issued guidelines including the Guideline for Management of Outsourcing Risks. Section 10 of the Outsourcing Guideline addresses Cloud Computing Services.

No.	Section / Reference	Comments	CBTT Response
94.	**3.2 – 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."	Minimal guidance should be provided on conducting Third Party Service Provider Due Diligence.	The Central Bank advises that as stated under "Scope of Application" this guideline should be read in conjunction with the Bank's other issued guidelines including the Guideline for Management of Outsourcing Risks. Section 5.4 of the Outsourcing Guideline offers guidance on conducting third party service provider due diligence.
95.	**3.6 – 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."	It is not clear whether this is POST incident review or active incident management.	The wording has been amended to provide greater clarity as follows: *"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. A record of past incidents should be maintained and a trend analysis of past incidents performed to identify commonalities and patterns in the incidents."*
96.	**#3 Bullet 5 – Change Management.**	Consider updating to "IT Change Management" to differentiate from organisational change management.	The guideline is focused on cybersecurity and refers to associated items to be included in the change management process. The statement is considered adequate as stated.
97.	**#3 Bullet 7 – User Access Management**	Consider including the term "role-based access" or "principle of least privilege" to provide clarity and ensure adherence to industry best practices for user access management	The following has been added to the section: *"Companies should enforce the principle of least privilege, so that users are granted the minimum access rights that are strictly required to execute their duties, to prevent unjustified access to a large set of data."*

No.	Section / Reference	Comments	CBTT Response
98.	**#3 Bullet 8 – Remote Access Management**	Consider including the term "authorised third-party – e.g. consultants, support vendors" as employees are not the only ones who may be using company or personally-owned devices to access company resources.	The words *"authorised third-parties"* have been added.
99.	**#3 Bullet 12 – Customer Authentication**	Consider amending the multi-factor authentication recommendation to indicate when necessary, based on risk, availability of PII etc. Consider removing "Financial" as there may be other use-cases requiring MFA for authentication e.g. sensitive Health data administered by regulated entities. Possible wording: "The company should implement multi-factor authentication for all customers accessing online services that process, store, or transmit sensitive data. The company should also ensure that the transmission of customer passwords is encrypted end-to-end."	The paragraph has been amended as follows: *"Multi-factor authentication should be deployed at login for all customers accessing online services that process, store, or transmit sensitive data. The company should ensure that industry best practice end-to-end encryption is utilized for the transmission of customer passwords."*
100	**3 - Customer Authentication**	Multi-Faction Authentication(MFA) should not be for customers only. MFA for employees (email access, remote access, privileged accounts) is just as important.	This section is intended to address customer authentication only. Employees' access is captured under "Remote Access Management. Companies are expected to adopt international best practices when implementing access procedures for employees, which may include MFA.
101	**3 - Other Recommended Cybersecurity Practices**	Remediation Management is embedded and established as part of core incident resolution best practices. There may be no added value for this to be addressed as a separate cybersecurity practice/process.	Companies are expected to treat with cyber-related incidents more urgently than an operational incident which may not have as severe an impact of a cyber event. Companies are therefore encouraged to develop a remediation process that treats with

No.	Section / Reference	Comments	CBTT Response
			cybersecurity issues and does not become shrouded within its wider incident resolution practices.
102	**Appendix I – Definitions/Abbreviations - Disruption**	Would this include unavailability of the service for the end customer? Note that systems may be down but not affect customers.	This should be considered in alignment with the definition of "material deficiency" that has been added to Appendix I. Companies should consider disruptions to refer to a cyberattack or cyber incident that causes an information system or major applications, to become inoperable for a length of time, which has the potential to significantly affect inter alia the financial institution's business operations, reputation or profitability.
103	**APPENDIX I – Cybersecurity Incident Reporting**	We would like clarity that this section relates to reporting of Cyber Attacks and Cyber Incidents only as defined under Appendix I- Definition /Abbreviations. If this statement is yes, we would recommend the removal of the **definition for Disruption** as it creates a conflict of understanding. If the definition of Disruption was meant to relate to disruptions related to Cyber Attacks and Cyber Incidents would recommend the definition be revisited to articulate same. **Definition as extracted from the Guideline** *"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)."*	The guideline is focused on cybersecurity and therefore relates solely to cyber incidents.
104	**Appendix I – Cyberattack definition**	Consider defining "cyberspace" which appears twice in this definition and nowhere else in the document. Alternatively, re-define a cyberattack without using	The first use of the word "cyberspace" has been removed.

No.	Section / Reference	Comments	CBTT Response
		"cyberspace" in the definition (similar to definitions for cyber incident, cyber risk etc.)	
105	**Appendix II - Initial Notification Requirements** (third bullet point)	Consider the change in the placement of apostrophe: … available'. instead of … available.'	Amended
106	**Appendix II - Cybersecurity Incident Reporting**	Who receives the "Cyber Incident Report"? The Guidelines lack an email address or telephone contact. If this information is available in other Bank Guidelines, consider including it here for completeness. *As mentioned in item #7, I also suggest including a recommendation that the Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT) or the TTPS Cyber and Social Media Unit (CSMU) be contacted (if desired) for assistance with the conduct of investigations.*	All regulated institutions are required to address the submission of any reports to the Inspector of Financial Institutions and usually copy their relationship officers.
107	**APPENDIX II – Cybersecurity Incident Reporting -** 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 **Feedback:** The guideline should specify who determine the frequency of regular updates.	Upon notification and review of the initial incident report, the Central Bank will formally advise the company of the frequency of any subsequent reporting requirements.
108	**Appendix II – Cyber Incident Reporting - Purpose**	Please consider including Standards.	Noted. The Central Bank opines that the section's content relates solely to the purpose of the incident reporting.

No.	Section / Reference	Comments	CBTT Response
109	**Appendix II – Cyber Incident Reporting –** Initial Notification Requirement	In the event of a major cyber incident and reporting channels are closed, would there be any special waiver for the notification timeline? Are there other acceptable forms of notification?	Companies are expected to use best efforts to contact the Inspector/Deputy Inspector if regular reporting channels are closed.
110	**Appendix II – Cybersecurity Incident Reporting, Initial Notification Requirements -** Bullet 2	Recommendation: Increase the timeframe for reporting a Cyber Incident to the Central Bank from 48 hours to 72 hours to better align with international practices: US Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) – cyber incident reported within 72 hours EU (ENISA) NIS2 directive Clause 102 – early warning submission within 24 hours and submission of incident notification with 72 hours UK Information Commissioners Office (ICO) – report breaches within 72 hours	Timeline has been amended to 72 hours.
111	**Appendix II – Reportable Incidents**	Bullet #1 Consideration - the statement is a bit vague as it's not specific to cybersecurity incidents. Consider including the term "cybersecurity" before the phrase "incident management framework". •Bullet #2 The term "characteristics of a material nature" may not apply to all scenarios listed. Consider defining what is meant by "material nature."	The guideline is focused on cybersecurity and therefore relates solely to cyber incidents.
112	**Appendix II – Cybersecurity Incident Reporting, Subsequent Reporting Requirements**	"The Central Bank expects the company to provide regular updates (e.g., daily)"	Upon notification and review of the initial incident report, the Central Bank will formally advise the

No.	Section / Reference	Comments	CBTT Response
		•Recommendation – excise bracket item "(e.g., daily)" as our research has not identified a similar precedent in other jurisdictions. E.g. the US SEC's draft guidelines stipulate "A registrant must provide updates as necessary until all material information has been disclosed […]" without implying daily.	company of the frequency of any subsequent reporting requirements.
113	**Appendix II - Cybersecurity Incident Reporting - Initial Notification Requirements** - "The company should complete the Cyber Incident Reporting Template below and submit to the Central Bank within 48 hours of the incident."	**Recommendation:** It should be noted in the guidelines that at the 48-hour mark of an active incident, all information to fully complete the incident report may not be available. However, all available information should be completed; with outstanding areas to be provided in subsequent submission or a further update on the incident.	Timeline has been amended to 72 hours.
114	**Appendix II - Initial Notification Requirements**	1. What is CBTT's preferred method of being "alerted"? 2. The 48-hour time frame seems to be onerous as the report is quite comprehensive. We would assume that if something material does occur the FI should be expending efforts on mitigating the effects. Can consideration be given for a later time frame possibly with regular updates to the CBTT via the designated liaison?	Companies are expected to use best efforts to contact the Inspector/Deputy Inspector directly by phone. Timeline for submission of the report has been amended to 72 hours.
115	**Appendix II - Subsequent Reporting Requirements**	This level of reporting seems excessive given that the FI would be focusing on rectifying issues. Can consideration be given to allow for longer interval times?	Timeline for submission of the report has been amended to 72 hours.
116	**Cyber Incident Report Template - Other recommended**	Regarding the Draft Cybersecurity best practices, the Cyber Incident Reporting Template seems to be	Guidance is provided in the Bank's Outsourcing Guideline to treat with third-party vendors.

No.	Section / Reference	Comments	CBTT Response
	Cybersecurity best practice guideline	more applicable to an insurer who manages their own IT infrastructure and system and will have access to the information which the report is structured to capture. What about the insurers who outsource their IT function? Consider an additional form for IT function (outsourced) or Cloud based support because the insurer will need to liaise with their vendor to get information on the incident to complete the report. The vendor may not be as forthcoming with some information according to nature of the incident. Also some insurers' IT needs and policies are sponsored by the parent company, therefore this must be considered so that the appropriate questions are asked in each case.	
117	**Cyber Incident Reporting Template**	What metrics should be used to define Reputational Impact? Or is it that the organization's thresholds should be used?	Companies should be guided by their internal thresholds.
118	**Cyber Incident Reporting Template - Particulars and Details of Incident – "**Provide the Indicators of Compromise (IOCs)"	We believe that it would be appropriate to move this line item 'Provide the Indicators of Compromise (IOC's)' to the bottom section titled 'Final Assessment & Remediation' since we normally don't know about the IOC's early on.	The line item has been moved as recommended.
119	**Cyber Incident Reporting Template - Impact Assessment – "** Business Lines Impacted (including availability of services – Treasury Services, Cash	Clarity is required on 'Business Lines Impacted' vs. 'Stakeholders Impacted'	Business lines refer to the services provided by the company. The stakeholders include inter alia, the company's clients, service providers, employees etc.

No.	Section / Reference	Comments	CBTT Response
	Management, ATM, Internet / Mobile Banking, etc.):		
120	**Cyber Incident Reporting Template - Impact Assessment –** "Stakeholders Impacted"	Does 'stakeholders impacted' refer to people or groups of people + organizations impacted? (e.g., CMT - Crisis Mgmt Team, Customers, etc.?)	See response above
121	**Cyber Incident Reporting Template - Impact Assessment –** "Reputational Impact"	Please clarify what is the expectation of the regulator with respect to this field? Are we expected to respond - NA, TBD, None, informational/Low/limited Medium/High or leave it blank?	The company is expected to provide details on any issues that have impacted its reputation including inter alia, negative news published, social media comments.
122	**Cyber Incident Reporting Template - Detailed chronological order of events** – "Escalation Steps Taken"	Escalation Steps Taken' includes mitigation, therefore we believe that 'Interim measures to mitigate/resolve the issue' in this section of the form is redundant.	The interim measures to mitigate /resolve the issue is actually part of the Root Cause Analysis section of the report and not part of the Chronological Order of Events section.
123	**Cyber Incident Reporting Template - Detailed chronological order of events** – "Channels of Communication involved"	By 'Channels of Communication' is there an expectation to specify how the 'stakeholders were informed'? i.e., via email, phone, webex/teams, postal letter etc.? Please clarify.	Yes. Companies are expected to identify how stakeholders were informed. This is aligned with requirements in section 10.3 of the Bank's Market Conduct Guideline for Institutions licensed under the Financial Institutions Act, 2008 regarding cyber risks and cybersecurity.
124	**Cyber Incident Reporting Template - Final Assessment and Remediation** – "Current State of Incident"	We believe that it would be appropriate to move the 'Current State of the Incident' to the top under 'Particulars and Details of the Incident' section for chronological flow.	The line item was moved as recommended but placed as the ninth item under the first section.
125	**General Comments -** Clause Numbering & Referencing	To enhance clause identification and referencing in the document, I recommend using numbered lists	Noted

No.	Section / Reference	Comments	CBTT Response
		instead of bullet points, specifically in the following sections: 1. Cybersecurity Guidelines (Sect. 2, pgs. 3-5) 2. Other Recommended Cybersecurity Practices (Sect. 3, pgs. 6-7) 3. Cybersecurity Incident Reporting (Appendix II, pgs. 10-11)	
126	**General Comments**	Language & Style – the draft guideline seems to use US spellings (e.g. organization, minimizing, authorized, utilize etc.). Consider adopting UK English as standard.	Noted
127	**General Comments**	Consider inclusion of a clause for institutions to impose insider trading procedures relating to cybersecurity incidents. Companies should carefully assess that topic during the course of their response to a cybersecurity incident and consider whether and when to suspend any purchases or sales of company securities by the company and by insiders. (SEC Adoption of New Cybersecurity Disclosures for Companies)	The guideline is principles based and expectations are listed at a high level. Companies are expected to consider more comprehensive issues in their own policies and procedures.
128	**General Comments**	End-of-life (EOL) / Unsupported software and hardware (e.g. Windows XP, MO2003) not included. EOL should be segregated from the network, with plans to decommission timely.	The guideline is principles based and expectations are listed at a high level. Companies are expected to consider more comprehensive issues in their own policies and procedures.
129	**General Comments**	As these are guidelines, are there any penalties for organizations that are grossly not following them?	The Central Bank has the power to take stronger action if a regulated entity has not adopted recommendations to implement aspects of the guideline and considers that failure in

No.	Section / Reference	Comments	CBTT Response
			implementation can cause risks to depositors or policyholders.
130	**General Comments**	Recommend that companies have cyber insurance with limits of at least X dollars, as a risk transfer method AND as a means for IT incident response panel.	Noted
131	**General Comments**	Administrative Fines based on the nature of CyberCrime and an Insurer's duty to protect its policyholder information. The Cybercrime Bill includes Penalties and Fines.	Noted
132	**General Comments**	Roles and Responsibilities of the Board and Senior Mgmt should be included in this guideline.	The Central Bank advises that as stated under "Scope of Application" this guideline should be read in conjunction with the Bank's other issued guidelines including its Corporate Governance Guideline. Sections 3 and 6 of the Corporate Governance Guideline outline the role of the board and senior management respectively.
133	**General Comments**	Include a section that addresses independent review and certification/report from Internal Audit on the insurer's cybersecurity governance, risk and controls.	The Central Bank advises that as stated under "Scope of Application" this guideline should be read in conjunction with the Bank's other issued guidelines including its Corporate Governance Guideline. Section 10 of the Corporate Governance Guideline outlines the role of the internal audit function.
134	**General Comment**	Consider the addition of a 'not applicable' section to the 'traffic signal' options for sections A through F of the questionnaire. Additionally, the 'not applicable' option can also include the requirement for the regulated entity to provide an explanation for their selection of the 'not applicable' option.	The Central Bank will appreciate any additional comments in a separate document to complement the self-assessment, which will assist in the Central Bank's own review of the assessment.

No.	Section / Reference	Comments	CBTT Response
		The 'not applicable' option is being suggested to accommodate varying technology and business models. For example, internet facing payment services versus non-internet facing services each contain differing levels of inherent cyber security risk. The associated policies and procedures will be informed by the accompanying model and CBTT's guidance.	
135	**General Comments**	This guideline recommends many policies and procedures to be put in place and implemented. Ample consideration should be given to the timeframes FIs would have to fully comply with the guideline once it is finalized and issued	As stated in the Supervisory and Enforcement paragraph, companies should attach detailed action plans to remedy any material deficiencies uncovered. Action plans should also outline proposed timelines.
136	**General Comments**	Is any consideration being given for Financial Groups that prefer to develop their cyber security protocol at a group level?	The institution must be able to demonstrate how the Group policy is relevant for the financial institution and how it satisfies the requirements of this Guideline for each regulated entity in the group. Section 7.4 of the Bank's Corporate Governance Guideline provides further guidance.