



**FINANCIAL SERVICES
COMMISSION**

**INSTRUCTIONS FOR THE COMPLETION OF THE
MAJOR CYBER INCIDENT REPORTING FORMS**

Table of Contents

1. INTRODUCTION.....	3
2. SCOPE OF APPLICATION.....	4
3. CLASSIFICATION AS A MAJOR INCIDENT.....	5
4. REPORT TEMPLATE DESCRIPTIONS	5
5. INSTRUCTIONS FOR SUBMITTING THE REPORTING TEMPLATES	6
6. DELEGATED REPORTING	9
7. UPDATE TO CYBER SECURITY POLICIES AND PROCEDURES	9
8. INSTRUCTIONS TO POPULATE THE FORMS.....	10
FORM 1 – INITIAL REPORT	10
Access Form 1	10
FORM 2 – INTERMEDIATE REPORT	13
Access Form 2	13
FORM 3 – FINAL REPORT	14
Access Form 3	14
9. APPENDIX – INCIDENT CLASSIFICATION MATRIX.....	15

1. INTRODUCTION

These instructions accompany the Technology and Cyber Risk Management (TCRM) Guideline issued by the Financial Services Commission (FSC).

In view of the increasing number of cyber-attacks in the region and abroad, the importance of reporting major cyber-attacks to regulators cannot be overstated. One of the roles of regulators is to promote the stability of the financial system and ensure its resilience to all types of attacks inclusive of cyber-attacks. The sharing of pertinent information about a cyber-attack with the regulator, assists the regulator in foreseeing and addressing additional issues and concerns that may have major impact to the financial system locally, regionally and possibly internationally. Regulators have a responsibility to carefully consider the information submitted and respond in a manner that assists regulated financial institutions to recover from such an incident or prevent other institutions from being impacted by the same or similar cyber incident.

With the development of the Major Cyber Incident Reporting Template (M-CIRT), FIs can report and document major incidents in a uniform manner that facilitates the review and study of the root causes and potential problems that can result in a cyber incident. The output from the review can provide a learning platform for all stakeholders to improve Cyber Resilience within the financial system by taking steps to further enhance the implementation of Cyber Risk management frameworks.

Further to the above, the purpose of these instructions is to guide the Financial Institution (FI) on how and when to complete the reporting template. FIs are expected to answer all questions as fulsome as possible given the information acquired about the incident.

2. SCOPE OF APPLICATION

These instructions must be applied to the reporting of a major cyber security incident in accordance with the definition in the TCRM Guideline.

These instructions apply to all incidents classified as a "major cyber incident" once it satisfies the criteria for a high or critical incident as defined in the Classification Matrix. These incidents cover both external events which could either be malicious or accidental.

The instructions are also applicable where the major cyber incident originates from an unregistered entity (e.g. when a cyber incident originates in the parent company or in an unregistered subsidiary) and affects the services provided by the registered entity either directly or indirectly (e.g. the capacity of the FI to execute delivery of its products and services activity is jeopardized as a result of the incident).

These instructions also apply to major cyber incidents affecting functions outsourced by FIs to third parties.

3. CLASSIFICATION AS A MAJOR INCIDENT

- 3.1 A major incident can be classified as follows:
- An incident with medium severity but high frequency
 - An incident with high severity
 - An incident with critical severity
- 3.2 View the Incident Classification Matrix in the [Appendix](#).

4. REPORT TEMPLATE DESCRIPTIONS

4.1 The Initial Report Template

This is the first notification that the FI submits to the FSC after it has been established and confirmed that a major cyber incident has occurred.

4.2 The Intermediate Report Template

This report contains a more detailed description of the incident and its consequences. It is an update to the initial report and/or an update to a previous intermediate report on the same incident.

4.3 The Final Report Template

This is the last report the FI will submit on the incident if:

- i. a root cause analysis has already been carried out and estimates can be replaced with real figures or
- ii. the incident is no longer considered major and needs to be reclassified.

An incident can be re-classified as non-major if the incident no longer meets the criteria to be considered major and is not expected to satisfy the criteria before the incident is resolved. FIs must ensure to state the rationale for the re-classification.

5. INSTRUCTIONS FOR SUBMITTING THE REPORTING TEMPLATES

5.1 The Notification Process

- When a cyber incident occurs, the FI is required to classify the incident in a timely manner but no later than within **24 hours** of its detection. A cyber incident is classified as major if it satisfies the criteria for **high** or **critical** as defined in the Classification Matrix. If the incident cannot be classified within 24 hours, the FI should inform the Relationship Officer and/or Relationship Manager immediately and communicate the reason for this in the **Initial Report**.
- Notwithstanding the above, the FSC should also be contacted promptly pending the submission of the report, as applicable:
 - Where a matter is classified as major within twenty-four (24) hours; or
 - Where a matter reaches the media or social platforms.
- The report date and time refer to the exact date and time the report was submitted to the regulator.
- FIs should be prepared to submit any additional documents required by the FSC, to complement the information submitted in the template, as well as follow up on any requests or clarifications made by the regulator.
- All additional information contained in the documentation provided by the FI to the FSC should be documented in the template.
- FIs should at all times preserve the confidentiality and integrity of the information exchanged between them and the FSC.

The completed template should be submitted via email to the requisite sub-division as follows:

Credit Union Division	CreditUnions@fsc.gov.bb
Insurance Division	Insurance@fsc.gov.bb
Pensions Division	Pensions@fsc.gov.bb
Securities Division	Securities@fsc.gov.bb

5.2 The Initial Report (Form 1)

- Once a cyber incident has been classified as major, the FI is required to complete the **Initial Report Form (Form 1)** with the information available, and submit it to the relevant sub-division.
- The initial report should be submitted within **four (4) hours** from the moment the cyber incident has been **classified as major**. If the email service is down, the FI should communicate this by telephone (or any other reliable back-up communication method) to the Relationship Officer and/or Relationship Manager and email the report once the email service is operational again.
- Once received by the FSC, an Incident Reference Code (IRC) will be assigned to the incident and will be communicated to the FI. The purpose of the IRC is to uniquely identify the incident. The FI would be required to populate the slot provided for this code at the top of each form.
- The initial report should also be submitted to the regulator when a previous non-major cyber incident has been classified as a major incident. FIs are required to email the report to the requisite Division immediately after the change of status is confirmed.
- The initial report requires FIs to provide basic characteristics about the cyber incident and foreseen consequences based on the information available at the time. FIs are also expected to resort to estimations in instances where actual data are not available.

5.3 The Intermediate Report (Form 2)

- If the cyber incident has not been resolved **5 days** after the submission of the Initial Report, the FI is required to populate the **Intermediate Report Form (Form 2)** with the information available and email it to the requisite Division. Any updates to the **Initial Report Form** should also be included in the second submission of the M-CIRT.
- In the case where the cyber incident has not been resolved in five (5) working days after the first Intermediate report, the FI is required to submit an additional Intermediate report.
- However, notwithstanding the above, at any point after the Initial Report and the first submission of the Intermediate Report, and the issue remains unresolved, the FI will be expected to submit an additional Intermediate Report upon the request of the regulator. This request may occur before the previously identified five (5) day period has passed and could be a daily request as long as the cyber incident remains unresolved.
- The FI's submission of the additional Intermediate Report should always be accompanied by an updated Initial Report.
- FIs should also submit Intermediate Reports when regular business activities have been recovered and business is back to normal. FIs should consider

business has resumed to normal when operations are restored with the same level of service/conditions as defined by the FI or defined externally by a service level agreement (e.g. processing times, capacity, security requirements). The resumption of business as normal also means that contingency measures are no longer in place. The Intermediate Report should contain a more comprehensive description of the cyber incident and its consequences and be accompanied by an updated Initial Report.

- As in the case with the Initial Reports, when actual data is not available, FIs are required to make use of estimations.

5.4 The Final Report (Form 3)

- FIs should deliver the final report, based on an independent assessment to the FSC within **twenty (20) working days** after business is deemed back to normal. FIs in need of an extension of this deadline (e.g. when there are no actual figures on the impact available or the root causes have not been identified yet) should contact their Relationship Officer and/or Relationship Manager before the time has elapsed and provide an adequate justification for the delay, as well as a new estimated date for the final report.
- FIs should include in their final report, full information on the following:
 - actual figures on the impact instead of estimates (as well as any other updates needed in form 1 and 2); and
 - if already known, the root cause and a summary of measures adopted or planned to be adopted to resolve the problem and prevent its reoccurrence in the future.
- FIs should also send a final report when, as a result of the continuous assessment of the incident, they identify that an already reported incident no longer fulfils the criteria to be considered major and is not expected to fulfil them before the incident is resolved. In this case, FIs should send the final report as soon as this is determined and, within the deadline for the submission of the next report. In this particular situation, instead of filling out form 3, FIs should check the box '**incident reclassified as non-major**' and provide an explanation of the reasons justifying this reclassification.
- FIs should ensure that the final report is accompanied by the most up-to-date versions of the Initial and Intermediate Reports.

6. DELEGATED REPORTING

- FIs wishing to delegate reporting obligations of cyber incidents to a third party, must formally write the FSC to obtain approval.

- In order to be eligible for approval, the following conditions must be met:
 - Irrespective of the possible delegation of reporting obligations, the affected FI remains fully responsible and accountable for the content of the information provided to the regulator.
 - FIs will monitor to ensure that the service is being delivered in the manner expected and in accordance with the terms of the contract or outsourcing agreement.
 - The FI should ensure and confirm the confidentiality and quality of sensitive data, as well as the consistency, integrity and reliability of the information to be provided to the FSC.

- FIs are required to inform the FSC of any material developments affecting the designated third party and its ability to fulfil the reporting obligations.

- FIs are required to diligently fulfil their reporting obligations without any recourse to external assistance whenever the designated third party fails to inform the FSC of a major cyber security incident.

7. UPDATE TO CYBER SECURITY POLICIES AND PROCEDURES

FIs should ensure that their cyber security policies clearly define all the responsibilities for cyber incident reporting as well as the processes implemented in order to fulfil the requirements defined in these Instructions.

8. INSTRUCTIONS TO POPULATE THE FORMS

FORM 1 – INITIAL REPORT

[Access Form 1](#)

Form 1 – Initial Report	
General Details	
Type of Report	<ul style="list-style-type: none"> • <u>Solo</u>: the report refers to a single FI • <u>Consolidated</u>: the report refers to a FI and its branches and subsidiaries that are also licensed institutions and are governed under the same Enterprise Cyber Security Framework • <u>List of Entities in Consolidated Report</u>: Applicable only if Consolidated reporting is selected and refers to the FIs affected by the incident that are branches or subsidiaries of the parent entity affected.
Name of Entity	<ul style="list-style-type: none"> • FI that is experiencing the cyber incident
Name of parent entity, if applicable	<ul style="list-style-type: none"> • In the case of groups of entities, please indicate the name of the parent entity.
Country/countries affected by the incident	<ul style="list-style-type: none"> • Country or countries where the impact of the incident has materialized (<i>e.g. several branches of the FI located in different countries are affected</i>), irrespective of the severity of the incident in the other country/countries. • If the country is not listed, select other and type the name of the country in the space provided
Primary Contact Person	<ul style="list-style-type: none"> • Name and surname of the person responsible for reporting the incident. • <u>Email</u>: email address to which any requests for further clarifications could be addressed, if needed. It ought to be a corporate email address. • <u>Telephone</u>: telephone number through which any requests for further clarifications could be addressed, if needed. It ought to be a corporate telephone or cell number.

<p>Secondary Contact Person</p>	<ul style="list-style-type: none"> Name and surname of an alternative person that could be contacted by the FSC to inquiry about an incident when the primary contact person is not available. In the case of a third-party service provider reporting on behalf of the affected FI, name and surname of an alternative person in the incident management/risk department or similar area. <u>Email</u>: email address to which any requests for further clarifications could be addressed, if needed. It ought to be a corporate email address. <u>Telephone</u>: telephone number through which any requests for further clarifications could be addressed, if needed. It ought to be a corporate telephone or cell number.
<p>Reporting Entity <i>(if reporting entity is a third party)</i></p> <p>Primary Contact Person</p> <p>Secondary Contact Person</p> <p>Email</p> <p>Telephone</p>	<ul style="list-style-type: none"> (primary) In the case of a third-party service provider reporting on behalf of the affected FI, the name and surname of the person responsible for reporting the incident. (secondary) In the case of a third-party service provider reporting on behalf of the affected FI, the name and surname of the alternative person responsible for reporting the incident. <p>(primary & secondary)</p> <ul style="list-style-type: none"> <u>Email</u>: email address to which any requests for further clarifications could be addressed, if needed. It ought to be a corporate email address. <u>Telephone</u>: telephone number through which any requests for further clarifications could be addressed, if needed. It ought to be a corporate telephone or cell number.
<p>Form 1: Incident Detection and Classification</p>	
<p>Date and time of detection of the incident</p>	<p>Date and time when the incident was first identified.</p>
<p>Initial Classification of Incident</p>	<p>Select High or Critical based on the criteria defined in the Classification Matrix.</p>
<p>Date and time of classification of the incident</p>	<p>Date and time when the cyber security incident was classified as major.</p>

<p>The Incident was detected by</p>	<p>Indicate whether the incident was detected by an internal user, (e.g. a general staff member, internal audit) or by another external party (e.g. customer, perpetrator). If it was none of those, please select other and provide an explanation in the corresponding field.</p>
<p>Type of incident</p>	<p>Choose from the list provided, the best indication with the information available, the type of incident that has occurred. If no selection can be made, select other and type the incident and a brief description.</p>
<p>Criteria Triggering the Report</p>	<p>Indicate which of the criteria have triggered the major incident report. Tick all that apply. Select other and state trigger if not observed in the list provided.</p>
<p>Short Description of the Incident</p>	<p>Explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, details of any unusual customer activity, etc.</p>
<p>Please state whether the incident was or will be reported to other regulatory authorities</p>	<p>Indicate whether the cyber incident has been/will be reported to other authorities under separate incident reporting frameworks, if known at the time of reporting. If so, kindly specify the respective authorities.</p>
<p>Reasons for the late submission of the Initial Report (where applicable)</p>	<p>Explain the reasons why you required longer than 24 hours to classify the incident.</p>

FORM 2 – INTERMEDIATE REPORT

[Access Form 2](#)

Form 2 – Intermediate Report - General Details	
Who was the threat actor?	Identify the category of the person or group that orchestrated the incident. Please refer to the table “Threat Actor Types” for further guidance.
What was the motive?	Indicate the reason behind the cyber-attack.
What was the level of internal escalation of the incident?	Detail your incident escalation process including, for example, levels of escalation, persons responsible for escalation, the person to whom the incident is being escalated and any associated time frames.
How did the incident start?	Detail what actions led to the incident and provide a brief overview of the initial impact. Also include relevant details e.g. any unusual customer activity.
How did the incident evolve?	Detail how did the incident spread throughout your network
Was the incident communicated to public, customers and staff? If yes, please specify	Specify the persons to whom the incident was communicated and the communication message.
Was crisis management started (internal and/or external)?	Detail what steps were taken during the crisis and the responders involved both internally and externally.
Form 2 – Intermediate Report – Incident Classification	
Type of incident	Refer to the table “Type of Incidents” for examples.
Cause of Incident	Select from the list of probable causes. Multiple choices may be selected.
Form 2 – Intermediate Report – Incident Scope	
Type of data disruption	Indicate how the data was disrupted. Select all that apply. <ul style="list-style-type: none"> Integrity: the accuracy and completeness of the asset or data. Availability: the accessibility of data according to acceptable predefined levels. Confidentiality: information is not made available to unauthorized persons, entities, or processes.
Functional areas affected	Specify how each applicable functional area was affected. Mentioning any data access challenges, systems malfunction etc.
Service Channels affected	Indicate the channel or channels of interaction with customers that have been affected by the cyber incident. Multiple selections can be made.
Form 2 – Intermediate Report – Incident Severity	
Transactions affected	Impact level: refer to the Classification matrix
Form 2 – Intermediate Report – Incident Mitigation	

Which actions/measures have been taken so far or are planned to recover from the incident?	Detail any forensic activity, strategies and resources, both technical and human, used in recovery
---	--

FORM 3 – FINAL REPORT

[Access Form 3](#)

Form 3 – Final Report – General Details	
Updates made to previous initial and intermediate reports	Provide further details on the cyber incident including in particular, any changes made to the information previously provided in the intermediate report.
Are all original controls in place?	Indicate whether or not the FI had to cancel or weaken some controls at any time during the cyber incident. If so, indicate whether these controls are back in place and if not, explain why and outline the steps and timeframe required for restoration.
Form 3 – Final Report – Root Cause Analysis and follow up	
What was the root cause?	Indicate what the root cause of the incident was, or if not known, what it was most likely to have been. Multiple choices may be selected. Description of the selections can be observed under “ Appendix 1: Types of Root causes ”. Also note that the root cause must be distinguished from the impact.
If Other root cause	If the cause of the cyber incident is none of the above, further details should be provided in the free text field.
Other relevant information on the route cause	Provide any other details on the root cause including preliminary conclusions drawn from the analysis
Main corrective actions or measures taken or planned to be taken to prevent the event from reoccurring	Describe the actions that have been taken or planned to be taken in order to prevent a possible reoccurrence of the cyber incident.
Form 3 – Final Report – Additional Information	
Has the incident been shared with other financial institutions for information purposes?	Provide an overview of which FIs have been reached out to and details of the information given to them. Ensure to note what was shared and why.
Has any legal action been taken against the financial institution?	Indicate whether at the time of filing of the report if there has been any legal action due to the occurrence of the cyber incident.
Assessment of the effectiveness of the action taken?	Include a self-assessment of the effectiveness of the actions taken during the duration of the cyber incident, including any lessons learnt.

9. APPENDIX – INCIDENT CLASSIFICATION MATRIX

		SEVERITY			
		Low	Medium	High	Critical
		<ul style="list-style-type: none"> No impact or minimal impact to the delivery of services and products to customer bases Downtime spans minutes Recovery time is predicted and can be handled internally No incident contagion No notification from service providers Data users may encounter none to little inconveniences relating to data integrity and availability Little to no impact on reputation; none to minimal cost and effort to recover Little to no financial loss 	<ul style="list-style-type: none"> Minimal impact to delivery of services and products to customer base Downtime spans 4 hours or less Recovery time is predicted and can be remedied internally with minimal external support Incident is contained within a unit/department Service Provider reports minor incident detected but contained and remedied in under 4 hours Data users may encounter significant inconveniences relating to data integrity and availability which may be corrected at low costs for licensee Reputation moderately affected requiring moderate cost and effort to recover; moderate impact on revenue, customer base and/or staff Financial losses can be absorbed 	<ul style="list-style-type: none"> Material impact to the delivery of services and products to customer base Downtime spans above 4 hours Recovery time is unpredictable and requires internal and extensive external support Incident spans the entire licensee network Service Provider reports material incident detected that has compromised its ability to offer reliable or substantial service to licensee Data users may encounter significant consequences relating to data confidentiality, integrity or availability which may be corrected at great costs for licensee Reputation severely damaged requiring great costs and effort to recover; severe impact on revenue, customer base and/or staff Financial losses compromise liquidity or normal conduct of operations 	<ul style="list-style-type: none"> Unable to deliver services and products to customer base Downtime spans multiple days Critical Systems extensively compromised and threatens recoverability Incident also compromises third party service providers and other financial institutions Service Provider is non-operational Data users may encounter irreversible consequences relating to data confidentiality, integrity or availability, equating to insurmountable financial losses Reputation irrevocably destroyed; critical impact on revenue, customer base and/or staff Financial distress or insolvency
FREQUENCY	Low Occurs on a yearly basis				
	Medium Occurs quarterly to bi-annually				
	High Occurs daily to monthly				