BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

# Operational Risk Integrated Online Network (ORION)

Policy Document

Applicable to:

1. Licensed banks
2. Licensed Investment banks
3. Licensed Islamic banks
4. Licensed International Islamic banks
5. Licensed insurers
6. Licensed takaful operators
7. Licensed international takaful operators
8. Prescribed development financial institutions
9. Approved issuers of a designated payment instrument
10. Approved issuers of a designated Islamic payment instrument

Issued on: 25 February 2021

## TABLE OF CONTENTS

## LIST OF TABLES

# PART A: OVERVIEW

## 1. Introduction

1.1 The sound operational risk management requires a comprehensive identification and assessment of Operational Risk as well as monitoring of Operational Risk exposures through indicators such as Loss Event Data, Key Risk Indicators and Scenario Analysis.

1.2 The objective of this policy document is to require reporting entities (REs) to submit information to the Bank with regard to operational risk exposure.

1.3 This policy document sets out the requirements for the reporting of Loss Event Data, Key Risk Indicators and Scenario Analysis to the Bank through the ORION.

## 2. Applicability

2.1 This policy document is applicable to REs as defined in paragraph 5.2.

## 3. Legal provisions

3.1 This policy document is issued pursuant to:

(a) sections 47(1) and 143(2) of the Financial Services Act 2013 (FSA);

(b) sections 57(1) and 155(2) of the Islamic Financial Services Act 2013 (IFSA); and

(c) section 41(1) and constitutes a notice under section 116(1) of the Development Financial Institutions Act 2002 (DFIA).

3.2 The guidance in this policy document is issued pursuant to section 266 of the FSA, section 277 of the IFSA and section 126 of the DFIA.

## 4. Effective date

4.1 This policy document comes into effect on 1 March 2021.

## 5. Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA or DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For the purpose of this policy document:

**“S”** denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action;

**“G”** denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

**“BDSF”** refers to business disruption and system failure;

**“CRO”** means the Chief Risk Officer of a RE;

**“Financial group”** refers to a financial holding company approved by the Bank or a licensed institution, and a group of related corporations under such financial holding company or licensed institution primarily engaged in financial services or other services which are in connection with or for the purposes of such financial services which includes at least one licensed person;

**“Financial institutions” or “FIs”** means**:**

(a) licensed banks, licensed investment banks and licensed insurers under the FSA;

(b) licensed Islamic banks which includes licensed international Islamic banks, and licensed takaful operators which includes licensed international takaful operators under the IFSA; and

(c) prescribed institutions under the DFIA;

**“GCRO”** means the Group Chief Risk Officer of a RE;

**“Loss Event Data” or “LED”** refers to information required for assessing an entity’s exposure to operational risk and the effectiveness of its internal controls. The purpose of the analysis of LED is to provide insight into the causes for large losses and whether control failures are isolated or systematic in nature. Identifying how operational risk may lead to credit risk and market risk-related losses also provides a more holistic view of the operational risk exposure;

**“Key Risk Indicators” or “KRIs”** refer to information that will provide insight into the operational risk exposure and are used to monitor the main drivers of exposure associated with the key risks;

**“Operational Risk”** has the same meaning assigned to it under the Policy Document on Operational Risk issued by the Bank on 10 May 2016[1]and includes any amendments made thereof from time to time. For ease of reference, Operational Risk refers to the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Operational risk is inherent in all activities, products and services of financial institutions and can transverse multiple activities and business lines within the financial institutions. It includes a wide spectrum of heterogeneous risks such as fraud, physical damage, business disruption, transaction failures, legal and regulatory breaches[2] as well as employee health and safety hazards. Operational risk may result in direct

[1] Paragraph 1.1 of the Policy Document on Operational Risk.

[2] Including fiduciary breaches and Shariah non-compliance by Islamic financial institutions.

financial losses as well as indirect financial losses (*e.g.* loss of business and market share) due to reputational damage;

**"ORION"** refers to the Operational Risk Integrated Online Network;

**"Payment instrument issuers" or "PIIs"** mean:
(a) approved issuers of a designated payment instrument under the FSA; and
(b) approved issuers of a designated Islamic payment instrument under the IFSA;

**"Reporting entities" or "REs"** refer to financial institutions and payment instrument issuers;

**"Scenario Analysis" or "SA"** refers to an assessment made by an entity to identify potential operational risk events and assess potential outcomes including identifying potential significant operational risks and the need for additional risk management controls or mitigation solutions;

**"SNC"** refers to **Shariah Non-Compliance**;

**"Control function"** refers to the definition as provided in the policy document on *Corporate Governance* issued by the Bank and includes any amendments made to thereof from time time**;** and

**"Officer within the control function"** means an officer that meets the following criteria:
(a) Performs one of the control functions under Shariah governance (i.e. Shariah risk management, Shariah review or Shariah audit);
(b) Independent from the business lines and not involved in revenue generation activities; and
(c) Possesses sound understanding of relevant Shariah requirements applicable to Islamic financial business.

## 6. Policy document superseded

6.1 This policy document supersedes the policy document on Operational Risk Reporting Requirement – Operational Risk Integrated Online Network (ORION) issued on 22 June 2018.

## 6A. Related legal instruments and policy documents

6A.1 This policy document must be read together with other relevant legal instruments and policy documents that have been issued by the Bank, in particular –

(a) Operational Risk issued on 10 May 2016 ;

(b) Corporate Governance issued on 3 August 2016 for FSA and IFSA;

(c) Corporate Governance issued on 13 December 2019 for DFIA;

(d) Shariah Governance Policy Document issued on 20 September 2019;

(e) Risk Management in Technology (RMiT) issued on 19 June 2020;

(f) Management of Customer Information and Permitted Disclosures issued on 17 October 2017;

(g) Guidelines on Business Continuity Management (Revised) issued on 3 June 2011;

(h) Guidelines on Handling of Suspected Counterfeit Malaysian Currency Notes issued on 2 September 2014;

(i) Letter on the 'Implementation of Financial Stability Board's Cyber Lexicon and Bank Negara Malaysia's Cyber Incident Scoring System for the Financial Institutions' issued on 28 September 2020; and

(j) ORION Frequently Asked Questions (FAQ) document[3].

## 7. Enquiries and correspondence

7.1 All enquiries and correspondences relating to this policy document shall be addressed to:

Pengarah<br>
Jabatan Pakar Risiko dan Penyeliaan Teknologi<br>
Bank Negara Malaysia<br>
Jalan Dato' Onn<br>
50480 Kuala Lumpur<br>
Fax No: 03-26970086<br>
Email: oprisku@bnm.gov.my

[3] For avoidance of doubt, REs must refer to the FAQ document in its entirety notwithstanding any direct reference made in this policy document to a specific paragraph in the FAQ document.

# PART B: POLICY REQUIREMENTS

## 8. Overview of the responsibilities of reporting entities

S 8.1 The REs must prepare and submit data and information on LED, KRIs and SA to the Bank through ORION in accordance with the requirements specified under section 12 entitled "ORION Reporting Requirements" of this policy document.

S 8.2 The REs must ensure that the data and information is consolidated and centralised at the entity level prior to submitting the information to the Bank.

S 8.3 The REs must put in place appropriate internal governance and processes to ensure completeness, accuracy and timeliness of the data and information submission to the Bank, including processes for consolidation, validation as well as reconciliation of such data and information with the RE's internal database, system and financial accounts.

## 9. Roles and responsibilities of ORION users

### GCRO

S 9.1 The GCRO or any other officer authorised by the RE to act in that capacity, is required to ensure the RE's compliance with the reporting requirements set out in this policy document.

### CRO

S 9.2 The CRO or any other officer authorised by the RE to act in that capacity, must ensure the RE's compliance with the reporting requirements set out in this policy document.

S 9.3 The CRO shall:

(a) appoint a Submission Officer to perform the functions set out in paragraph 9.4; and

(b) ensure that the reporting requirements in this policy document are complied with at all times, including in the absence of the Submission Officer.

### Submission Officer

S 9.4 The Submission Officer shall:

(a) prepare the data and information for submission to the Bank through ORION;

(b) ensure that the data and information to be submitted to the Bank is accurate, complete and have been consolidated at the entity level and reconciled with internal reports and databases;

(c) ensure the successful transmission of the data and information to the Bank within the timeline specified under each data category;

(d) perform corrections, make amendments and provide updates on the submitted data and information upon having knowledge of any inaccuracy in the data; and

(e) liaise with the Bank on matters pertaining to the data and information to be submitted or generally on the ORION.

## 10. Access to ORION

### Financial group structure

G 10.1 In the case of REs operating as financial groups, access to ORION will be granted to the GCRO, CRO and Submission Officer.

### Single entity structure

G 10.2 In the case of REs operating on stand-alone basis, access to ORION will be granted to the CRO and Submission Officer.

### Adoption of structure

S 10.3 The REs must notify the Bank in writing on the type of reporting structure that it intends to adopt.

## 11. Registration of ORION users

### Details to be registered

S 11.1 The REs must register the following details of the GCRO, CRO and Submission Officer at FI@KijangNet portal at www.bnm.gov.my:

(a) Name
(b) Designation
(c) Email address
(d) Phone number

Refer to **FAQ No. 2.**

### Changes in GCRO, CRO and Submission Officer

S 11.2 The REs must notify the Bank in writing of any changes to the GCRO, CRO or Submission Officer and to update such details accordingly at FI@KijangNet portal. Please refer to **FAQ No. 2.**

S 11.3 The REs must ensure that any changes to the GCRO, CRO or Submission Officer will not impact the timeliness of data and information submission to the Bank.

# PART C: REPORTING REQUIREMENTS

## 12. ORION reporting requirements

S 12.1 The REs must submit information to the Bank through ORION in accordance with **Table 1: ORION reporting requirements**.

**Table 1: ORION reporting requirements**

| Appendices | Description | Applicability |
|---|---|---|
| **Appendix 1** | ORION user guide & technical specifications | REs |
| **Appendix 2** | Operational risk event reporting requirements | REs |
| **Appendix 3** | Cyber threat reporting requirements | FIs |
| **Appendix 4** | BDSF event reporting requirements | FIs |
| **Appendix 5** | Boundary event reporting requirements | FIs except Licensed Insurers & Takaful Operators |
| **Appendix 6** | Customer information breaches reporting requirements | REs |
| **Appendix 7** | Insurance-related event reporting requirements | Licensed Insurers & Takaful Operators |
| **Appendix 8** | SNC event reporting requirements | FIs |
| **Appendix 9** | Payment-related fraud event reporting requirements | REs except Licensed Insurers & Takaful Operators |
| **Appendix 10** | Aggregate reporting requirements | REs |
| **Appendix 11** | Overseas loss event reporting requirements | FIs |
| **Appendix 12** | Business lines taxonomy | FIs |
| **Appendix 13** | Event types taxonomy | FIs |
| **Appendix 14** | Causal categories taxonomy | FIs |
| **Appendix 15** | Key risk indicators taxonomy | FIs |

## 13. Scope of reporting

S 13.1 The REs must report all operational risk events in accordance with the requirements and timeline set out in **Table 2: ORION Reporting types and timelines**. The reporting must also include the operational risk events of foreign and offshore subsidiaries or branches of the REs which resulted in financial-related losses.

S 13.2 The REs shall submit to the Bank the LED module for events that occurred from 22 September 2014 onwards and the KRI module data for events that occurred from 1 October 2014 onwards.

S 13.3 For reporting of the operational risk events of foreign and offshore subsidiaries or branches of the REs, REs must notify the Bank of challenges faced by the REs in meeting the reporting requirements of this policy document. A waiver must be obtained from the Bank for failure by REs to comply with reporting requirements under such circumstance.

## 14. Reporting currency

S 14.1 All amounts must be reported by REs in Ringgit Malaysia (RM).

S 14.2 REs must use its applicable internal exchange rate to convert loss amounts to RM in the instance where a financial loss is in a foreign currency.

## 15. Classification and quantification

### Financial related operational risk event

S 15.1 REs must classify financial-related events in accordance with the following:

(a) **Actual Loss** – Actual Loss refers to an event that resulted in a measurable loss in the RE's Profit and Loss account. Accounting treatment must be applied in accordance with the RE's accounting policies.

(b) **Potential Loss** – Potential Loss refers to a conservative estimate of the loss amount until actual loss can be determined. Accounting treatment must be applied in accordance with RE's internal policy.

(c) **Near Miss** – Near Miss refers to an event which financial losses have been averted by controls or mitigating actions.

S 15.2 Where a provision is made in the Profit and Loss account for the measurable loss of an on-going event, the amount must be classified by the REs as 'Actual Loss' in ORION. The 'Actual Loss' amount must be adjusted by the REs if the amount for the provision is subsequently changed.

S 15.3 Indirect Loss which was resulted from an Operational Risk event must not be included by REs in the calculation of the actual and potential loss amount reported in ORION.

### Non-financial related operational risk event

S 15.4 REs must classify Non-Financial-related events in accordance with the following:

(a) **High impact** - which caused severe damage to reputation that resulted in long term effect on business credibility;

(b) **Medium impact** - which caused moderate damage to reputation that resulted in medium term effect on business credibility; or

(c) **Low impact** - which caused insignificant damage to reputation that did not result in any damage on business credibility.

## Table 2: ORION reporting types and timelines

| Reportable operational risk events | | Classification | Timeline |
|---|---|---|---|
| Critical event | **Robbery and theft**<br>• Self Service Terminals (SST)[4] robbery<br>• Robbery and theft events ≥ RM 200k | • Actual<br>• Potential<br>• Near miss | By T+1 working day, T being the date of event confirmation |
| | **Cyber threat**<br>• As defined in Appendix 3 | • Actual<br>• Near Miss | |
| | **Reputational Impact**<br>• High impact events as defined by REs internal policy | • Actual | |
| | **All operational risk events ≥RM 1mil** | • Actual<br>• Potential | By T+2 working days, T being the date of event confirmation |
| | **Critical BDSF**<br>• As defined in Appendix 4 | • Actual | |
| | **New modus operandi (MO)**<br>• New type of fraud MO committed and impacted the REs for the first time | • Actual<br>• Potential | |
| | **Customer information breaches**<br>• As defined in Appendix 6 | • Actual | By T+1 working day, T being the date of investigation is tabled to the Board |
| SNC event | **Actual SNC**<br>• As defined in Appendix 8 | • Actual | By T+1 working day, T being the date of SNC confirmation by Shariah Committee (SC) |
| | **Potential SNC**<br>• As defined in Appendix 8 | • Potential | By T+1 working day, T being the date of event confirmation by an officer within the control function |
| Fraud event | **All fraud types**<br>• Payment-related fraud is defined in Appendix 9<br>• Other fraud events | • Actual<br>• Potential<br>• Near miss | By the 15th calendar day of the following month or earlier |
| Other loss event | **Aggregate reporting**<br>As defined in Appendix 10<br>• All card fraud (Credit Card, Debit Card, Charge Card) with amount involved ≤ RM 5k | • Actual<br>• Potential<br>• Near miss | |
| | • All actual loss ≤ RM 1k<br>• Physical cash shortages | • Actual | |
| | **Overseas loss events**<br>• As defined in Appendix 11 | • Actual | |
| | **All other loss events**<br>• All events other than specified above with financial losses | • Actual | |

[4] Self Service Terminals (SST) are Automated Teller Machines (ATMs), Cash Deposit Machines (CDMs) and Cash Recycler Machines (CRMs).

## 16. Additional reporting requirements

S 16.1 All submission to ORION must not contain any customer information or employee data to satisfy data secrecy and data privacy.

S 16.2 All on-going Operational Risk events must be re-assessed and updated to reflect changes to event classification and latest information.

S 16.3 Notwithstanding the timeline for reporting of critical events as stated in **Table 2**, the REs must notify the Bank on the occurrence of critical events through other communication channels at the earliest opportunity upon the detection of the event.

## 17. Key risk indicators

S 17.1 FIs must submit information on the KRIs according to the applicability, description and frequency set out in **Appendix 15 – Key risk indicators Taxonomy.**

G 17.2 The Bank may define the KRIs at the following levels:

(a) entity level, *i.e.* generic KRIs that can be aggregated on an enterprise-wide basis;

(b) specific to a business line; or

(c) shared across multiple business lines.

S 17.3 The FIs must report the KRIs to the Bank within the timeline specified in **Table 3** below.

**Table 3: Timeline for KRI reporting to ORION**

| KRI frequency | Reporting deadline |
|---|---|
| Monthly | By the 10th calendar day of the following month |
| Quarterly | By the 15th calendar day of the following month |
| Semi-annually | By the 15th calendar day of the following month |
| Annually | By the 15th of January of the following year |

## 18. Scenario analysis

G 18.1 Scenario Analysis (SA) is a systematic process in the creation of plausible operational risk events and has become an essential element in the operational risk management and measurement. It is one of the operational risk management tools[5], however, unlike the others, it is a forward-looking tool that examines and explores predominantly emerging risks and rare tail-end events which are usually low frequency high impact events. Subsequently, the FIs will be able to incorporate the controls on these events to mitigate the risk exposures of those scenarios. By thinking

[5] Operational Risk Management tools are LED, RCSA, KRI and SA

through the impact of various scenarios, FIs can enhance its contingency plans or business continuity management plans.

**S** 18.2 As part of the Bank's mandate to promote the safety and soundness of FIs in the financial system, the FIs shall respond to the SA exercise which is executed through ORION *via* the SA modules where the Bank requires for the FIs to do so.

**S** 18.3 FIs must conduct SA as and when it may be required by the Bank and submit the results of the SA and other information to the Bank within prescribed time.

# APPENDICES

## APPENDIX 1 ORION user guide and technical specifications

1. Please refer to the attached document.

## APPENDIX 2 Operational risk event reporting requirements

### ORION data fields requirements

1. REs must report the following information for each operational risk event as guided in **Table 4** below. Additional data fields for SNC, payment-related fraud and aggregate operational risk related events are provided in **Appendix 8**, **Appendix 9** and **Appendix 10** respectively.

**Table 4: Data fields for operational risk event reporting**

| Data fields | Mandatory field | Description |
|---|---|---|
| **Reporting Entity Name** | Yes | • To select the respective reporting entity for operational loss event *(Note: Applicable to Financial Group structure)*<br>• Reporting entity name will be automatically displayed for a 'Single' entity |
| **Nature of Event** | Yes | • **New** - New type of MO impacted the REs for the first time.<br>• **Repeated** - MO that has occurred previously at REs<br>Refer to **FAQ No. 35.** |
| **Event Classification** | Yes | Operational risk events must be classified as either one of the following:<br>• Actual loss<br>• Potential loss<br>• Near miss |
| **Islamic Business** | Yes (if the event is related to Islamic product / business) | (√) – If the operational risk event is relating to Islamic business or product<br>*(Note: If the event is no longer classified as SNC, Islamic Business box must remain checked (√) because the operational risk event is related to Islamic business or product)* |
| **Shariah Non Compliance** | Yes | FIs must select one:<br>(a) **Yes**<br>• Event reported as 'actual' SNC or 'potential' SNC<br>(b) **No**<br>• Event classified as non-SNC<br>*(Note: For specific Shariah related fields, please refer to Appendix 8)* |

| Data fields | Mandatory field | Description |
|---|---|---|
| **Loss Event Name** | Yes | Clear and concise name that summarise the nature of the loss event |
| **Internal Loss Event ID** | Yes | REs are required to generate its own internal ID for each loss event reported in ORION |
| **Business lines*** | Yes | Must be reported up to Level 3 (banking) and Level 2 (insurance) in accordance with the taxonomy in Appendix 12 |
| **Product / Services** | Yes | Conditionally populated; please select one |
| **Delivery Channel** | Yes | Conditionally populated; please select one |
| **Event categories*** | Yes | Must be reported up to Level 3 in accordance with the taxonomy in Appendix 13 |
| **Causal categories*** | Yes | Must be reported up to Level 3 in accordance with the taxonomy in Appendix 14 |
| **Country of Events** | Yes | Country where the loss was incurred |
| **State of Events** | Yes | Conditionally populated for operational risk event occurred in Malaysia |
| **District of Events** | Yes | Conditionally populated for operational risk event occurred in Malaysia |
| **Date of Event Occurrence** | Yes | The date of the operational risk event took place |
| **Date of Event Detection** | Yes | The date of operational risk event confirmation is obtained |
| **Loss Event Description** | Yes | **1. General operational risk event**<br>An executive summary of the loss event and shall include the following details:<br>(a) Chronology of the loss event<br>• Where the event took place<br>• How the event occurred<br>• The modus operandi involved<br>• Parties involved in the event (e.g. customer / staff / outsourced service provider / affiliates, etc.)<br>• Number of customers affected by the event<br>• Number of business lines affected<br>• The root cause of the event<br>(b) Remedial actions to resolve the event<br>(c) Mitigating action plans to prevent recurrence of similar incident in the future |

***** *Those marked with asterisks are not applicable to PIIs*

| Data fields | Mandatory field | Description |
|---|---|---|
| | | (d) Indication of timeline when the event can be resolved<br>(e) Progressive update of the event post-reporting to ORION<br>The executive summary must not include customer / individual confidential information e.g. Name, I/C number, account number and other personal information<br>**2. Aggregate operational risk event**<br>For further description and reporting format on aggregate reporting, please refer to Appendix 10 |
| **Event Valid Till** | No | To remove existing operational risk event in ORION; this field is only applicable for **genuine duplicated reporting in ORION** |
| **Reason** | Yes (if the above is selected) | The reason for the removal of the loss event must be provided |
| **Event Impact** | Yes | Please choose one event impact from the following:<br>• **Financial impact** - There is an actual or potential financial loss<br>• **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc.<br>• **Both financial and non-financial** – as defined above |
| **Financial Impact >> Event For** | Yes | RE must select whichever applicable:<br>• Event for Banking<br>• Event for ATM Acquirer<br>• Event for Payment Instrument<br>• Event for Payment Channel<br>• Event for Insurance & Takaful Operator |
| **Financial Impact >> Event For** | Yes | **>>Banking**<br>• REs must identify whether the operational loss event have boundary implications in accordance with Appendix 5<br>• If the loss event is identified as a boundary event, REs must categorise either as Credit Risk or Market Risk related |
| **Financial Impact >> Event For** | Yes | **>> ATM Acquirer**<br>Please refer to Appendix 9 |
| **Financial Impact >> Event For** | Yes | **>> Payment instrument**<br>Please refer to Appendix 9 |

| Data fields | Mandatory field | Description |
|---|---|---|
| **Financial Impact<br>>> Event For** | Yes | **>> Payment channel**<br>Please refer to Appendix 9 |
| **Financial Impact<br>>> Event For** | Yes | **>>Insurance &Takaful Operator**<br><br>REs must identify the insurance category impacted from:<br>• Assets<br>• Claims<br>• Premium<br>• Re-insurance<br>• Intermediaries<br>• Others |
| **Amount Involved** | Yes | This field must have a value to reflect the overall financial amount associated with the operational risk event reported |
| **Financial Impact (for Banking, ATM Acquirer and Payment Channel)<br>>> Actual Loss / Potential Loss / Recoveries** | Yes | REs to record the actual loss / potential loss / recovery amount incurred according to the following categories:<br>• Reporting Entity^<br>• Customer^^<br>• 3rd Party<br><br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field<br><br>*(Note:*<br>*^ Please input the date of write-off or provision recognised in P&L in the "Comments" column.*<br>*^^ Please input the loss amount borne or partially borne by the customer)* |
| **Financial Impact (for Payment Instrument)** | Yes | >> Loss Incurred by Malaysian Entities<br><br>Please refer to Appendix 9 |
| **Financial Impact (for Payment Instrument)** | Yes | >> Loss Incurred by Foreign Entities<br><br>Please refer to Appendix 9 |
| **Non-Financial Impact<br>>> Impact** | Yes | REs must select the severity of the non-financial impact either as:<br>• High<br>• Medium<br>• Low |
| **Non-Financial Impact<br>>> Comments** | Yes | The detailed description of the non-financial impact must be provided to justify the selection of High / Medium / Low |

**">>"** represents sub-data fields

## APPENDIX 3 Cyber event reporting requirements

1. Cyber is defined as relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data and information systems.

2. Cyber threat is a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security. Vulnerability can be defined as a weakness, susceptibility or flaw of an asset (e.g. network devices, endpoints) or control that can be exploited by one or more threats.

3. Cyber security is preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

**Table 5: Types of cyber threats**

| Types | Description | Example |
|---|---|---|
| **Malicious Software (Malware)** | Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems. | • Adware<br>• Bots<br>• Bugs<br>• Rootkits<br>• Spyware |
| **Virus** | A type of malware that is capable of duplicating itself with the intention of stealing information or disrupt the device or system. | • MyDoom<br>• Stuxnet |
| **Ransomware** | A type of malware that installs on a victim's device, encrypting or locking the victim's systems or files. A request for payment is made to unlock the affected systems or files. Ransomware is considered to be a form of extortion. | • CryptoLocker |
| **Distributed Denial of Service (DDoS)** | DDoS is the prevention of authorised access to information or information systems; or the delaying of information system operations and functions, resulting in the loss of availability to authorised users. DDoS is normally carried out using numerous sources simultaneously. | • Network attack<br>• Application attack |
| **Hacking** | Hacking is an unauthorised intrusion into a computer or a network. | N/A |
| **Web defacement** | Website defacement is an attack on a website that changes the visual | N/A |

| | | |
|---|---|---|
| | appearance of the website or a webpage. | |

**Note:** If there are any new modus operandi of cyber-attacks experienced in overseas subsidiaries or branches, please notify the Bank  via email to the respective Supervisor of the Bank.

**Cyber event reporting types**

4. REs must report **all** cyber events that occurred as stipulated below to ORION in accordance with the requirements set out in **Table 2: ORION reporting types and timelines** within **1 working day** upon confirmation.

(a) Cyber incident

Defined as a cyber event that:

(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or

(ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

(b) Cyber event

Defined as any observable occurrence of cyber threat in an information system. Cyber threat events may also provide an indication that a cyber incident is occurring (i.e. cyber threat which could potentially compromise REs' IT equipment, system, operations, data, services or users).

5. Examples of reportable cyber incidents

(a) Ransomware that has affected corporate PCs / laptops and encrypted the files within.

**Event Classification:** Actual Loss<br>
**Event type**: BDSF**>>** System **>>** Security breach – virus / malware

(b) DDoS attack on the REs network that caused network downtime

**Event Classification:** Actual Loss<br>
**Event type**: BDSF**>>** System **>>** Security breach – Distributed Denial of Service

6. Examples of reportable cyber events

(a) Persistent DDoS attempt coming from the same IP address defined as 'high risk' by REs internal monitoring system.

**Event Classification:** Near Miss

**Event type**: BDSF**>>** System **>>** Security breach – Distributed Denial of Service

(b) Virus infection successfullly blocked by REs antivirus software defined as 'high risk' by REs internal monitoring system.

**Event Classification:** Near Miss
**Event type**: BDSF**>>** System **>>** Security breach – virus / malware

**Reporting a cyber incident and cyber event in ORION**

7. Cyber incident and cyber event

**Category:** Cyber incident and cyber event
**Event Classification:** Actual Loss or Near Miss

| Data fields | Description |
|---|---|
| Reporting Entity Name | To select the respective reporting entity for operational loss events |
| Event Classification | • **Actual Loss** – Any cyber incident that has been confirmed<br>• **Near Miss** – any high risk cyber event detected and confirmed<br>*(Note: The event classification above is not referring to the status of financial impact resulted from the cyber incident or event)*<br>Refer to **FAQ No. 68.** |
| Nature of Event | • **New** - New type of MO that impacted the REs for the first time.<br>• **Repeated** - MO that has occurred previously at REs<br>Refer to **FAQs No. 35 and 67.** |
| Islamic Business | (√) – If the operational risk event is relating to Islamic business or product |
| Loss Event Name | Clear and concise name that reflects an overall summary and nature of the loss event |
| Business Lines | Must be reported up to Level 3 (banking) in accordance with the taxonomy in Appendix 12 |
| Products / Services | Please choose where applicable |
| Delivery Channel | Please choose where applicable |

| Data fields | Description |
|---|---|
| Event Category | Please categorise the cyber incident or event using **ONLY** the following selection of event types:<br>**OPTION 1**<br>**Level 1**: Internal Fraud<br>**Level 2**: Unauthorised Activity<br>**Level 3**: Select one:<br>• Unauthorised changes to programmes, data or transactions<br>• Hacking / Cracking<br>• Misuse of system access (e.g. Powerful system ID)<br>• Computer virus / malware injection<br>**OPTION 2**<br>**Level 1:** External Fraud<br>**Level 2:** System Security<br>**Level 3:** Select one:<br>• Hacking damage<br>• Theft of information<br>• Unauthorised changes to programmes by external parties<br>• Misuse of system access by external parties<br>• Sabotage by external parties<br>**OPTION 3**<br>**Level 1 :** BDSF<br>**Level 2 :** Systems<br>**Level 3 :** Select one:<br>• Security breach – virus / malware<br>• Security breach – DDoS<br>• Security breach – hacking / cracking<br>• Security breach – Web defacement |
| Causal Category | Must be reported up to Level 3 in accordance with the taxonomy in Appendix 14 |
| Date of Occurrence | The date cyber incident / event occurred |
| Date of Detection | The date of cyber incident / event confirmation is obtained |

| Data fields | Description |
|---|---|
| Loss Event Description | An executive summary of the incident / event and shall include the following details:<br>(a) Chronology of the cyber incident / event:<br>• What type of cyber event occurred<br>• What type of system or service impacted from the attack<br>• How long was the system or service downtime (if any)<br>• Where is the cyber event coming from<br>• For DDoS attack, please specify the IP address<br>• How the cyber incident / event occurred i.e. root cause<br>• Number of customers affected<br>• Number of business lines affected<br>(b) Remedial actions to resolve the incident / event<br>(c) Mitigating action plans to prevent recurrence of similar event in the future<br>(d) Indication of timeline when the incident / event can be resolved<br>(e) Progressive update of the incident / event post-reporting to ORION<br><br>The executive summary must not include customer / individual confidential information e.g. Name, I/C number and other personal information |
| Event Impact | Please choose one event impact from the following:<br>• **Financial Impact** - There is an actual or potential financial loss<br>• **Non-Financial Impact** – No loss amount involved but has an impact on reputation, non-compliance etc.<br>• **Both Financial and Non-Financial** – as defined above |
| Financial Impact >> Events For | REs must select one:<br>• Event for Banking<br>• Event for Insurance & Takaful Operator |
| Financial Impact >> Events For | **>> Banking**<br><br>• REs must identify whether the operational loss event have boundary implications in accordance with Appendix 5 |

| Data fields | Description |
|---|---|
| | • If the loss event is identified as a boundary event, REs must categorise either as Credit Risk or Market Risk related |
| Financial Impact<br>>> Events For | **>>Insurance &Takaful Operator**<br>REs must identify the insurance category impacted from:<br>• Assets<br>• Claims<br>• Premium<br>• Re-insurance<br>• Intermediaries<br>• Others |
| Amount Involved | This field must have a value to reflect the overall financial amount associated with the operational risk event reported |
| Actual Loss / Recoveries | REs to record the actual loss / recovery amount incurred to the following categories:<br>• Reporting Entity^<br>• Customer^^<br>• 3rd Party<br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, the recovered amount must be recorded in the 'Recovery Amount' field<br>*(Note: ^ Please input the date of write-off or provision recognised in P&L in the "Comments" column.*<br>*^^ Please input the loss amount borne or partially borne by the customer)* |
| Non-Financial<br>>>Impact | Please choose either:<br>Low / Medium / High |
| Non-Financial<br>>> Comments | The detailed description of the non-financial impact must be provided to justify the selection of Low / Medium / High |

**">>"** represents sub-data fields

## APPENDIX 4 BDSF event reporting requirements

1. BDSF is an event or a series of events related to business disruptions or system failures.

2. FIs must report all actual critical BDSF events to ORION in accordance with the requirements set out in **Table 6: BDSF event reporting types** within **2 working days** of event confirmation regardless of whether the events are translated into a financial / non-financial impact.

**Table 6: BDSF event reporting types**

| Category | Definition |
|---|---|
| **Critical BDSF event** | • Any business disruption of LoD 1 event involving failure at main branch or processing hub irrespective of breaching or not breaching MTD timeline including network.<br>• Any business disruption of LoD 2[6] and above irrespective of breaching or not breaching MTD timeline including network.<br>• Any system failure or system execution failure occurred at REs or outsourced service provider affecting the critical business functions or systems irrespective of breaching or not breaching RTO timeline. The minimum critical business functions or systems are set out in the **FAQ No. 61.**<br>• Any acceptance of counterfeit Malaysian currency notes by deposit-accepting SST. |

3. A BDSF event may affect several lines of business. FIs must select only one line of business which is most affected by the incident. Some factors that could be taken into account to determine the business line includes (based on priority sequence):
   (a) If the core banking system (deposit) or core insurance system (underwriting and claims processing) is one of the systems affected, this is always the priority above other systems. To also indicate channels such as ATM or Internet if they are also affected;
   (b) Materiality of the impact (financial and non-financial);
   (c) Criticality of the business / service / system;
   (d) Transaction volume processed by the system and availability of manual workaround processes; and
   (e) Duration of system downtime (in cases where systems are recovered in phases)

[6] LoD 2 – affect a number of branches or departments. Probability of exceeding MTD/RTO is moderate.

## APPENDIX 5 Boundary event reporting requirements

1. A boundary event is a loss event that has both operational risk and credit or market risk components. REs must identify events that incur operational losses with credit or market risk implications and report these as boundary events.

### Credit related operational risk event

2. A boundary event with credit risk components is a loss event resulting from operational risk events or failures that led to credit risk implications. This type of event is treated as credit risk loss and is therefore excluded from operational risk capital charge. However, REs must report the event in ORION and flag this as Credit Risk Boundary Event.

Example:
**Event type:** External fraud **>>** Theft & fraud **>>** Fraudulent application by banking products / facilities **>>** Boundary event: Credit risk.

A customer has deliberately overstated his income, subsequently provided misleading credit exposure and resulted in loan credit approval. The customer later defaulted as he was unable to service his loan. Fraud is an operational event and default is a credit risk event.

### Market related operational risk event

3. A boundary event with market risk components is a loss event resulting from operational risk events or failures, but has market risk implications. This type of event is treated as operational risk loss and is therefore subject to operational risk capital charge. REs must report the event in ORION and flag this as a Market Risk Boundary Event.

Example:
**Event type:** Execution delivery & process management **>>** Transaction capture, execution & maintenance **>>** Data entry, maintenance or loading **>>** Boundary event: Market risk.

A desk dealer transacts a Spot FX trade. The trader input a transaction as “sell” MYR 20 Million against USD when it should have been “buy”. When the trader realised the erroneous input, the exchange rate between MYR and USD has moved against the trader.
In this scenario, the error made by the dealer is an operational error. However, the loss incurred was due to market movements and hence has market risk implications.

## APPENDIX 6 Customer information breaches reporting requirements

1. Reporting of customer information breaches must be done in line with the requirements stipulated in Management of Customer Information and Permitted Disclosures policy document issued by the Bank on 17 October 2017.

2. The reporting as 'Actual Loss' to ORION must be done **within 1 working day** upon **tabling report to the Board** with the summary of the event including the modus operandi involved, the root cause(s) of **the customer information breach** and the number of customers affected.

### Reporting customer information breaches in ORION

3. Customer information breaches in Financial Institutions

**Category:** Customer information breaches
**Event Classification:** Actual Loss

| Data fields | Description |
|---|---|
| Reporting Entity Name | To select the respective reporting entity for operational loss events |
| Event Classification | **Actual Loss** |
| Nature of Event | • **New** - New type of MO that impacted the REs for the first time.<br>• **Repeated** - MO that has occurred previously at REs<br>Refer to **FAQ No. 35.** |
| Islamic Business | (√) – If the operational risk event is relating to Islamic business or product |
| Loss Event Name | Clear and concise name that reflects an overall summary and nature of the loss event |
| Business Lines | Must be reported up to Level 3 in accordance with the taxonomy in Appendix 12 |
| Products / Services | Please choose where applicable |
| Delivery Channel | Please choose where applicable |
| Event Category | Please categorise the customer information breach event as follows:<br>**Level 1**: Client, products and business practices<br>**Level 2**: Suitability, disclosure and fiduciary<br>**Level 3**: Breach of Privacy |

| Data fields | Description |
|---|---|
| Causal Category | Must be reported up to Level 3 in accordance with the taxonomy in Appendix 14 |
| Date of Occurrence | The date that the event took place |
| Date of Detection | The date of event confirmation is obtained |
| Loss Event Description | An executive summary of the loss event and shall include the following details:<br>(a) Chronology of the loss event<br>• Where the event took place<br>• How the event occurred<br>• The modus operandi involved<br>• The categories of parties involved in the event (e.g. customer / staff / outsourced service provider / affiliates, etc.)<br>• Number of customers affected by the event<br>• Number of business lines affected<br>• The root cause of the customer information breach<br>(b) Progressive update of the event post-reporting to ORION<br>The executive summary must not include customer / individual confidential information e.g. Name, I/C number, account number and other personal information |
| Event Impact | Please choose one event impact from the following:<br>• **Financial Impact** - There is an actual or potential financial loss<br>• **Non-Financial Impact** – No loss amount involved but has impact on reputation, non-compliance etc.<br>• **Both Financial and Non-Financial** – as defined above. |
| Financial Impact >> Events For | Choose: Banking<br>• REs must identify whether the operational loss event have boundary implications in accordance with Appendix 5<br>• If the loss event is identified as a boundary event, REs must categorise either as Credit Risk or Market Risk related |

| Data fields | Description |
|---|---|
| | Choose: Insurance and takaful operator<br>REs must identify the insurance category impacted from:<br>• Assets<br>• Claims<br>• Premium<br>• Re-insurance<br>• Intermediaries<br>• Others |
| Amount Involved | This field must have a value to reflect the overall financial amount associated with the operational risk event reported |
| Actual Loss / Potential Loss / Recoveries | REs must record the actual loss / potential loss / recovery amount incurred to the following categories:<br>• Reporting Entity^<br>• Customer^^<br>• 3rd Party<br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field<br>*(Note:*<br>*^ Please input the date of write-off or provision recognised in P&L in the "Comments" column.*<br>*^^ Please input the loss amount borne or partially borne by the customer)* |
| Non-Financial >>Impact | Please choose either:<br>Low / Medium / High |
| Non-Financial >> Comments | The detailed description of the non-financial impact must be provided to justify the selection of Low / Medium / High |

**">>"** represents sub-data fields

## 4. Customer information breaches in Payment Instrument Issuers

**Category:** Customer information breaches
**Event Classification:** Actual Loss

| Data fields | Description |
|---|---|
| Reporting Entity Name | To select the respective reporting entity for operational loss events |
| Event Classification | **Actual Loss** |
| Nature of Event | • **New** - New type of MO that impacted the REs for the first time.<br>• **Repeated** - MO that has occurred previously at REs<br>Refer to **FAQ No. 35.** |
| Loss Event Name | Clear and concise name that reflects an overall summary and nature of the loss event |
| Event Category | Please categorise the customer information breach event as follows:<br>**Level 1**: Client, products and business practices |
| Date of Occurrence | The date that the event took place |
| Date of Detection | The date of event confirmation is obtained |
| Loss Event Description | An executive summary of the loss event and shall include the following details:<br>(a) Chronology of the loss event<br>• Where the event took place<br>• How the event occurred<br>• The modus operandi involved<br>• The categories of parties involved in the event (e.g. customer / staff / outsourced service provider / affiliates, etc.)<br>• Number of customers affected by the event<br>• Number of business lines affected<br>• The root cause of the customer information breach<br>(b) Progressive update of the event post-reporting to ORION<br>The executive summary must not include customer / individual confidential information |

| Data fields | Description |
|---|---|
| | e.g. Name, I/C number and other personal information |
| Event Impact | Please choose one event impact from the following:<br>• **Financial Impact** - There is an actual or potential financial loss<br>• **Non-Financial Impact** – No loss amount involved but has impact on reputation, non-compliance etc.<br>• **Both Financial and Non-Financial** – as defined above |
| Amount Involved | This field <u>must</u> have a value to reflect the overall financial amount associated with the operational risk event reported |
| Actual Loss / Potential Loss / Recoveries | REs must record the actual loss / potential loss / recovery amount incurred to the following categories:<br>• Reporting Entity^<br>• Customer^^<br>• 3rd Party<br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field<br>*(Note:*<br>*^ Please input the date of write-off or provision recognised in P&L in the "Comments" column.*<br>*^^ Please input the loss amount borne or partially borne by the customer)* |
| Non-Financial >>Impact | Please choose either:<br>Low / Medium / High |
| Non-Financial >> Comments | The detailed description of the non-financial impact must be provided to justify the selection of Low / Medium / High |

**">>"** represents sub-data fields

## APPENDIX 7 Insurance-related event reporting requirements

### Insurance / Takaful Fraud

1. Insurance / Takaful fraud occurs when someone knowingly lies to obtain some benefit or advantage to which he / she is otherwise not entitled or someone knowingly lies to deny some benefit that is due and to which another person is entitled. The main motive for committing the insurance / takaful fraud (*i.e.* in the form of premiums / contributions and claims fraud) is to attain financial gain.

2. Insurance / takaful fraud can be in the form of:

   (a) **Internal fraud**
   Fraud against the insurer / takaful operator committed by an employee or director whether on his / her own or in collusion with other parties which are internal or external to the insurer / takaful operator.

   (b) **External fraud**
   Fraud against the insurer / takaful operator committed by other than an employee or director of the insurer / takaful operator, such as the policyholder / participant, third party claimant, outsourced service provider, medical provider, beneficiary, workshop, supplier and contractor in the purchase and / or execution of an insurance policy / takaful contract.

3. Fraud committed by intermediaries such as an agent, loss adjuster or broker must be classified under external fraud, unless the fraud is committed in collusion with an employee or director of the insurer / takaful operator. In such a case, the collusion must be reported as internal fraud.

4. The severity of fraud can range from slightly exaggerating claims to deliberately causing accidents or damages in order to file for claims. The most common form of fraud is to obtain lower premiums / contributions, misappropriation of insurance premiums / contributions and to obtain wrongful financial gain through inflated or fictitious claims. In this regard, fraud can be classified as either hard fraud or soft fraud:

   (a) Hard fraud occurs when a policyholder / participant / claimant deliberately plans or invents a loss, such as a collision, motor theft, or fire that is covered by the insurance policy / takaful contract in order to receive payment for damages. This includes false claims, where the damages claimed actually did not occur; and

   (b) Soft fraud, which is far more common than hard fraud, is sometimes also referred to as opportunistic fraud. This type of fraud is where policyholder / participant / claimant exaggerates an otherwise legitimate claim. For example, when involved in a collision, an insured / participant may claim a higher amount compared to the actual cost of damages.

5. Examples of situations which may indicate fraud is about to be, has been or is being committed includes:
   (a) Making a false entry, omitting, altering, concealing, destroying or causing to omit, alter, conceal or destroy any entry in respect to the documents of an insurer / takaful operator;
   (b) Receiving a proposal for insurance / takaful contract or collecting premium / contributions, on a group policy / takaful contract if it has expired or has been cancelled by the insurer / takaful operator;
   (c) Forging, making use of or holding a false document, purporting to be a policy of an insurer / takaful operator;
   (d) Altering an entry made in a policy of an insurer / takaful operator; or
   (e) Issuing / using a policy / takaful contract which is false or incorrect, wholly or partly, or misleading

6. To perpetrate the fraud, documents may be forged or tampered with and this may include the following examples:
   (a) Unauthorised signature for underwriting and claims approvals;
   (b) Unauthorised issuance and / or tempering of Cover Notes;
   (c) Incomplete or non-disclosure of material facts in the proposal forms;
   (d) Wordings against and / or certificates of insurance / takaful contract;
   (e) Fake / tempered policy document / takaful contract, policy schedule, claims documents or reports.

7. Paragraphs 5 & 6 contain fraud illustrations as a guide to insurers and takaful operators. While insurance / takaful fraud can take place in various forms with different modus operandi, insurers and takaful operators shall be aware of and must be able to identify other scenarios which indicate that fraud is about to be, is being or has been committed.

**Premium / Contribution Fraud**

8. Premium / contribution fraud occurs when someone intentionally conceals or misrepresents information when obtaining insurance / takaful coverage, knowing that it would influence the insurance / takaful contract and premium / contribution calculation.

9. However, premium/contribution fraud goes beyond the above definition as illustrated below:
   (a) Avoid paying equitable premium / contribution for risk proposed to be assumed (Premium Avoidance):
   When obtaining a new insurance policy / takaful contract, an individual fraudulently misrepresents previous or existing conditions in order to obtain a lower premium/contribution on his / her insurance policy / takaful contract. For example, he / she may not disclose previous claims experience or health condition which would have resulted in higher premium / contribution charged.

   (b) Siphoning of premium / contribution monies:
   This is also known as misappropriation of premium / contribution. This occurs when the employee of insurer, agent or broker on his/her own; or in collaboration with another party pockets the

premiums / contributions which have been paid and does not remit them to the insurer / takaful operator. The fraudster may also:

(iii) Issue a forged cover note or policy / takaful contract; or

(iv) Write off outstanding agents' balances as bad debts via issuance of credit endorsements to cancel policies / takaful contracts after they have expired.

(c) "Bogus insurer / takaful operator":
This type of fraud occurs when an entity or person who holds out to be a branch or representative office of a licensed insurer or takaful operator or impersonates as a licensed insurer or takaful operator. Although premium / contribution may be paid by the policyholder / participant, the insurance policy / takaful contract is worthless.

(d) "Kick-backs":
An employee receives "kick-backs" by recording the premium / contribution of a "walk-in" customer under "agency" and receives a share of the commission, of which he / she is actually not entitled. In other instances, this may be done through the creation of a "fictitious" agency which is actually owned by the employee to earn commission.

(e) Dual premium / contribution charges or inflated premium / contribution:
The premium / contribution stated in the policy schedule / takaful contract or debit note is lower than the premium / contribution paid. The difference is pocketed by the employee, agent or broker. For example, premium / contribution rates stated in the debit note and payment receipt issued by insurer / takaful operator is lower than the billing note issued by employee, agent or broker where premium / contribution payment is paid in cash. Normally this type of fraud is discovered when insured / participant complains or queries on the differences between the amounts stated in the insurers / takaful operator's debit note or policy schedule and the actual premium / contribution paid.

## Fraudulent Claim

10. Fraudulent claim includes staged or planned accidents, submitting false claim for a loss which has not occurred, faking death or committing an act of arson to collect insurance money, overstating insurance claims to reap profits for personal gain, false reporting to enable claimant to make a claim under a policy which otherwise is not covered, for example, falsifying the date or circumstances of an accident.

11. Fraudulent claim can be perpetrated by an insured / participant, a third party claimant, crime syndicate either on his / her own or in collusion with an employee(s) of an insurer, service provider, an agent and loss adjuster. For example a loss adjuster may exaggerate the quantum of loss or submit misleading, fabricated or untruthful loss report to the insurer / takaful

operator. Collaborators to fraudulent claim may either be given a share of the claim benefit or receive some form of kickbacks or bribery.

(a) Past posting (Back dating of cover notes / policy period):
This happens when an insured/participant who is involved in a motor accident, a victim of a car theft or whose property was damaged, has no insurance / takaful coverage. The insured / participant may decide to take a chance at "past-posting" insurance / takaful contract coverage by creating an elaborate scheme of events including tempering, falsifying or faking claim documents to prove that the policy / takaful contract is in force at the time of the loss.

(b) Deliberate act of arson:
This happens when an owner of a property/vehicle, or someone hired by an owner, deliberately burns a property/vehicle to make a claim.

(c) Fictitious or falsified claim:
This type of fraud occurs when a fraudster makes a claim for a loss that never took place. Example under this classification includes claiming for non-existent injuries or damage to property.

(d) Exaggerated or inflated claim (Overstating the Amount of Loss):
A real loss has occurred, but a third party claimant (e.g. motor workshop) may take the opportunity to incorporate previous minor damages to the vehicle into the repair bill associated with the “real accident” to reap additional profits. The inflated claim is also intended to reap gains for the policyholder / participant, and in some instances to compensate for the “excess” or “deductible” stipulated in the insurance / takaful contract.

(e) Multiple claims (Multiple Policies for Profit):
A fraudster buys numerous insurance policies / takaful contracts on a same property, normally with various insurers / takaful operators and then intentionally damages or destroys the property. Subsequently, the fraudster will claim on all the policies / takaful contracts.

(f) Staged accident through organised crime syndicate:
These are planned accidents normally orchestrated by organised crime syndicate. Accidents are usually pre-planned manoeuvres which involved self-inflicted accidents and at times, involving an innocent party. Examples of staged accident are:

(i) “Swoop and Squat”:
Innocent victims are targeted by organised auto accident rings. These rings orchestrate an accident by using pre-planned manoeuvres to set the innocent party up for a rear end collision.

(ii) “Paper Accident”:
Organised rings actively solicit others to participate in the creation of accidents that only exist on paper. No innocent parties are involved in this type of staged accident.

(g) Disguised suicide:
An insured / participant commits suicide and disguises it as an accident to enable people close to him to benefit from his personal accident insurance / contract. Such action may also constitute fraud in life insurance i.e. where the usual waiting period applying to suicide in a life insurance policy has not yet elapsed.

(h) Faked death:
A fraudster will take out a life insurance policy / family takaful contract on himself and make his spouse the beneficiary. A warning sign might be if a spouse or other family member suddenly asks a person to buy or increase life insurance / family takaful coverage. After the policy / takaful contract has been in effect for several months, the fraudster fakes his death and his spouse is paid the death benefit. In the case of faked death, the fraud may be committed in two ways i.e. presenting to the insurer / takaful operator with the body of a stranger which has been made unrecognisable or claiming the insured/participant has died but for some reason the body cannot be found or produced.

(i) Falsified beneficiary:
Someone other than the policyholder / participant takes control of the insurance policy / family takaful contract and changes the beneficiary through "nefarious" means.

(j) Medical and Health insurance fraud:
Health insurance fraud is described as an intentional act of deceiving, concealing, or misrepresenting information that results in health care benefits being paid to an individual or group. The most common perpetrators of healthcare insurance fraud are health care providers. Examples of medical and health fraud are:

(i) Billing for services not provided;
(ii) Billing for service which is more expensive than what was actually provided;
(iii) Providing and billing for unnecessary services while representing that such services were necessary; and
(iv) Fake disability claim, including submission of forged documents to be eligible for a disability claim.

(k) Fraudulent workmen's compensation claim:
This type of fraud is committed with the intent to obtain some benefit or advantage to which the claimant is otherwise not entitled. Examples of fraud committed under the workmen compensation insurance / contract are:

(i) Working while collecting workmen' compensation benefits;
(ii) Faking injury;
(iii) Claiming to be injured at work when injury occurred elsewhere; and
(iv) Intentionally misclassifying employees' job codes.

## APPENDIX 8 SNC event reporting requirements

1. FIs must submit both potential and actual SNC events to ORION in accordance with the requirements and timeline set out in **Table 2: Reporting types and timelines**.

2. Submission of both potential and actual SNC reports represents an official attestation by the FIs based on the business operations and activities conducted. The officer-in-charge of respective FIs shall be prepared to respond to any query from the Bank as to the details of their submission.

### Shariah Committee (SC)

3. The FI's SC must make decision on events tabled whether it is SNC or non-SNC. This decision must be clearly reflected in the SC's meeting minutes.

4. The event classification of "Actual" or "Potential" is not under the purview of the SC.

### Islamic contracts

5. In relation to the definition of specific Shariah contracts, please refer to the respective policy documents on Shariah contracts issued by the Bank.

### Potential SNC event

6. A potential SNC event is defined as any SNC event detected and confirmed by an officer within the control function but pending decision by the SC. Please refer to ORION **FAQs No. 71.**

7. The FIs must report any potential SNC event to ORION within **1 working day** upon confirmation by an officer within the control function. Please refer to **Table 2: Reporting types and timelines**.

8. The event must be tabled at the SC meeting within **14 working days** of the event confirmation by an officer within the control function.

9. In the event where there is no SC meeting that will be held within the 14-day period, FIs are required to conduct an ad-hoc SC meeting (may consist of the minimum required quorum) specifically to deliberate on the matter.

10. Where there is no submission of potential SNC event by the FIs for any particular period, this is deemed as a declaration that there is no occurrence of potential SNC events at the FIs during the period.

### Actual SNC event

11. Actual SNC event is defined as any SNC event that has been confirmed by the FI's SC. Please refer to ORION **FAQ No. 71.**

12. The FIs must report any actual SNC event to ORION within **1 working day** from the SC's confirmation date. Please refer to **Table 2: Reporting types and timelines**.

13. The FIs must submit to ORION a rectification plan as approved by the Board and the SC within **30 calendar days** from the reporting date of actual SNC to the Bank.

14. In the event where there is no Board meeting that will be held within the 30-day period, FIs must conduct an ad-hoc Board meeting (may consist of the minimum required quorum) to obtain the Board's approval on the rectification plan prior to submission to the Bank.

15. FI must take appropriate remedial rectification measures or follow up to resolve actual SNC and control mechanism to avoid recurrences. Latest facts and actions taken on the case must be updated in ORION.

### Determining loss from SNC event

16. In determining the actual loss arising from SNC incidents, the following operational risk impact may serve as a basis in deriving the loss:

    (a) Legal liability – Judgments, settlements and other legal costs;
    (b) Regulatory and compliance – fines or the direct cost of any other regulatory penalties. For example, the regulatory fine as stipulated in Section 28(5) of IFSA;
    (c) Restitution – Payments to third parties on account of operational losses for which the bank is legally responsible;
    (d) Loss of recourse - Losses experienced when a third party does not meet its obligations to the FIs;
    (e) Write-downs – Direct reduction in value of assets due to theft, fraud, unauthorised activity or market and credit losses arising as a result of SNC incidents; and
    (f) Direct purification of income – amount of income that needs to be purified either by channeling it to charity or any other manners as prescribed by the SC.

### SNC KRIs

17. FIs must submit on a monthly basis to the Bank the following leading KRIs pertaining to SNC aspects arising from their business operations and activities:

    (a) **Litigation**
    Any business cases that are currently under litigation that may have potential SNC implications. These include counter-suit by customers claiming the contract is executed not in accordance with Shariah requirement.

(b) **Complaints**
Any complaints that have been lodged by customers pertaining to Shariah compliance aspects of Islamic contracts (including transparency and proper implementation of Islamic contracts by FIs.

**Reporting SNC event in ORION**

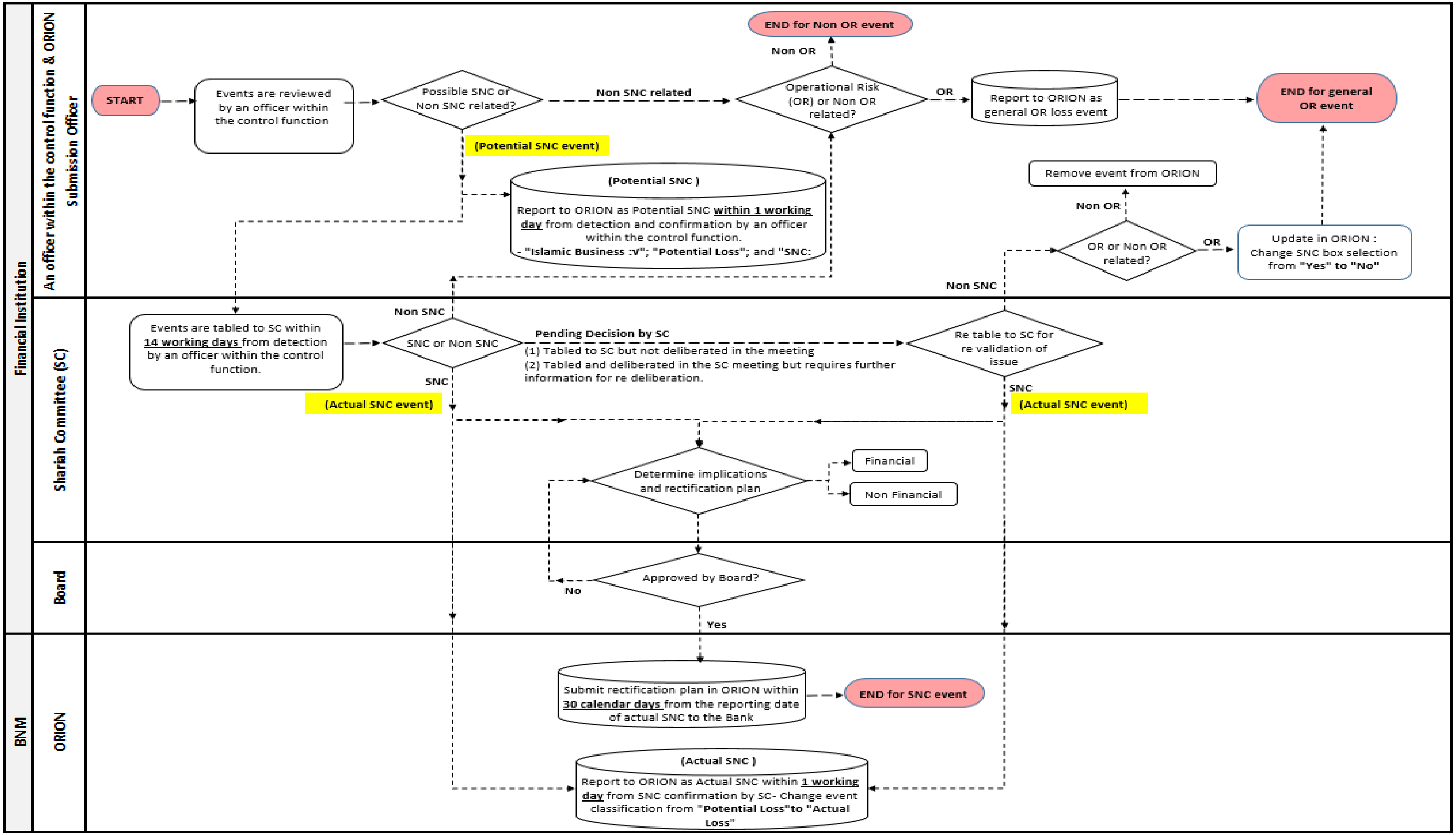
18. In addition to the general reporting requirements specified in **Appendix 2: Operational risk event reporting requirements**, SNC related events must be reported by REs in accordance with **Table 7: SNC Specific data fields**.

**Table 7: SNC specific data fields**

| Data item | Description |
|---|---|
| Event Classification | • **Actual Loss** – Any SNC event that has been confirmed by the FI's SC as SNC<br>• **Potential Loss** – any SNC event detected and confirmed by an officer within the control function but pending decision by the SC<br>*(Note: The event classification above is not referring to the status of financial impact resulted from the SNC event)*<br>*Refer to* **FAQ No. 71.** |
| Shariah Non-Compliance | FIs must select one:<br>(a) **Yes**<br>• Event reported as 'actual' SNC or 'potential' SNC<br>(b) **No**<br>• Event classified as non-SNC<br>In the event where the SC has decided that the event is non-SNC event, FIs are required to amend in ORION the SNC field from "Yes" to "No". The event needs to be reassessed whether it is to be considered under operational risk event |
| Shariah Primary Contract | FIs must select only ONE primary Shariah contract applied to the product<br>If there are several products involved in an event, FI must select more than one main Shariah contract according to the number of products involved<br>The option "Others (please specify)" is meant for transaction that does not involve any Shariah primary contract e.g. advertisement does not comply with Shariah, questionable sponsorship etc. |

| Data item | Description |
|---|---|
| | *(Note: In relation to the definition of specific Shariah contracts, please refer to the respective policy documents on Shariah contracts issued by BNM)* |
| Shariah Supporting Contracts | FIs must provide the type of secondary Shariah contract used under a particular Shariah primary contract (where applicable)<br>If the option “Others (please specify)” is selected, FIs must specify the specific contract used in the ‘Shariah Supporting Contract Comments’ field<br>*(Note: In relation to the definition of specific Shariah contracts, please refer to the respective policy documents on Shariah Contracts issued by BNM)* |
| Shariah Source of Detection | FIs must report the source of detection of the potential and actual SNC e.g. Shariah Compliance Unit, Business Unit, etc. |
| SC Reporting Date | The date the event was tabled to SC for decision |
| Board Reporting Date | The date of tabling the rectification plan of an SNC event to the Board |
| Shariah Date Resolved | Shariah resolution date endorsed by SC |
| No. of Accounts Involved | The number of accounts involved in a particular SNC event |
| Shariah Decision | Entailing Shariah resolutions including the basis of the decision on the SNC event. The decision made by SC must be distinctly documented in the minutes of the meeting |
| Actions Taken | Entailing the rectification plan following SC’s decision. SNC rectification plan approved by the Board must be provided within 30-calendar days after the event has been reported to the Bank.<br>Concurrently, FIs must update ORION on the detailed rectifications and actions taken by FIs |

## Figure 1: Process flow for reporting SNC events


Financial Institution
An officer within the control function & ORION Submission Officer
Shariah Committee (SC)
Board
BNM
ORION
START
Events are reviewed by an officer within the control function
Possible SNC or Non SNC related?
Non SNC related
(Potential SNC event)
Operational Risk (OR) or Non OR related?
Non OR
END for Non OR event
OR
Report to ORION as general OR loss event
END for general OR event
(Potential SNC )
Report to ORION as Potential SNC within 1 working day from detection and confirmation by an officer within the control function.
- "Islamic Business :V"; "Potential Loss"; and "SNC:
Remove event from ORION
Non OR
OR or Non OR related?
OR
Update in ORION : Change SNC box selection from "Yes" to "No"
Non SNC
Events are tabled to SC within 14 working days from detection by an officer within the control function.
Non SNC
SNC or Non SNC
Pending Decision by SC
(1) Tabled to SC but not deliberated in the meeting
(2) Tabled and deliberated in the SC meeting but requires further information for re deliberation.
Re table to SC for re validation of issue
SNC
(Actual SNC event)
SNC
(Actual SNC event)
Determine implications and rectification plan
Financial
Non Financial
Approved by Board?
No
Yes
Submit rectification plan in ORION within 30 calendar days from the reporting date of actual SNC to the Bank
END for SNC event
(Actual SNC )
Report to ORION as Actual SNC within 1 working day from SNC confirmation by SC- Change event classification from "Potential Loss"to "Actual Loss"

## Examples of SNC event

18. Appropriate assessment has to be given in determining SNC events attributed to operational risk loss event types. These types of event may have potential SNC implications. The following examples are provided to illustrate reporting of SNC events:

(a) **Event Type**:Internal fraud **>>** Theft and fraud **>>** Misappropriation of assets

> "When performing Shariah review on Takaful business based on Wakalah model, it is discovered that the Takaful agents have misappropriated the participants' contribution to the Tabarru' (donation) fund. Hence, the claims made by the participants are not able to be paid".
>
> **Conclusion:** The Takaful agent failed to channel the contribution to the donation fund. Therefore, this incident shall be reported under Internal Fraud operational risk loss event type with SNC implications since the Takaful agents did not perform the Wakalah contract as mandated by the Takaful participants.

(b) **Event Type**:Clients, products and business practices **>>** Selection, sponsorship and exposure**>>** Failure to investigate client per guidelines

> "During the course of Shariah review, it is discovered that Islamic corporate financing facility has been disbursed to corporate clients who involved in entertainment and tobacco-related industries. Further review revealed that there was no due diligence conducted on the business activities during credit approval process".
>
> **Conclusion:** The failure to investigate client per guidelines led to non-compliance with ruling issued by Shariah Advisory Council of Bank Negara Malaysia (BNM SAC) which prohibits the granting of financing to fund Shariah non-compliant business activities

(c) **Event type**: External fraud >> Theft and fraud >> Forgery / counterfeit (cover notes, policy certificates, currency, cheque, security documents / identifcation documents

> "Credit Administration division failed to assess the authenticity of trade invoices supported by one trade finance customer upon processing financing disbursement. The case had been reported to commercial crime police as it also involved some FIs. Hence, the affected FIs need to recognise this actual loss".
>
> **Conclusion:** This incident may have Shariah concern as the subject matter i.e. the trade invoices are not genuine leading to non-existence of subject matter when performing the financing transaction. Therefore, it should be raised as a potential SNC event.

(d) **Event type**: Execution, delivery and process management >> Transaction capture, execution and maintenance >> Model / system mis-operation

> "When processing financing disbursement to one corporate customer, credit administration unit discovered that commitment fees have been charged on the customer's unutilised financing amount. The unit found out that errors in system-setting caused this incident".
>
> **Conclusion:** The errors in credit processing system caused the above potential SNC occurrence. Hence, this is against the ruling of BNM SAC which prohibits commitment fees to be charged on the unutilised financing amount.

(e) **Event type**: Damage to physical assets **>>** Natural disaster & Other losses **>>** Damage to islamic inventory

> "Some FIs maintain commodity warehouse to facilitate financing transaction with customers. Nevertheless, when Shariah review team performed an on-site review, it is found that the commodity used in the financing transaction is of inferior quality due to improper maintenance of the warehouse. Further, it is found that the warehouse was affected by the recent flash flood caused by poor drainage system. The customer has been purchasing and selling commodity for financing transactions which is of lower quality and not as what have been specified in the Aqad process".
>
> **Conclusion:** This incident has led to potential SNC occurrence as the customers have transacted the inferior quality of commodity not as what has been stipulated in the Aqad process.

(f) **Event type**:Business disruption and system failures **>>** Systems **>>** Software-Inadequate system capacity

> "Claims department discovered that there was no segregation of funds between Takaful participants and Shareholders. This could disrupt Takaful business operations as the participants may dispute in the event of non-payment of claims and no surplus sharing between the Shareholders and the Takaful participants. There is a need to segregate the funds immediately to ensure smooth operations of the Takaful".
>
> **Conclusion:** This incident may lead to SNC as there is no proper channeling of participants' contribution to Participant Risk Fund (PRF) which can be utilised in the event of mishap and claims made by the participants.

## APPENDIX 9 Payment-related fraud event reporting requirements

1. In line with the general reporting requirements specified in **Appendix 2: Operational risk event reporting requirements**, applicable REs must report all payment-related fraud events individually per transaction basis as listed in **Table 8: Payment-related fraud types**.

2. Particularly for payment Card fraud (credit card, charge card and debit card), REs must report based on the following requirements:
   (a) Card fraud with amount involved > RM5,000, REs must report the event individually per transaction basis.
   (b) Card fraud with amount involved ≤ RM5,000, REs must report the event on an aggregate basis as stipulated in **Appendix 10 – Table 14: Aggregate reporting types and threshold**.
   (c) Card fraud with new MO committed and impacted REs for the first time, REs must report the event individually per transaction basis.

**Table 8: Payment-related fraud types**

| Fraud | Type of instruments and channels | REs responsible to report fraud event in ORION |
|---|---|---|
| Payment Instruments | • Credit card<br>• Charge card<br>• Debit card<br>• E-money[7]<br>• Cheque | • Card issuers<br>• Card issuers<br>• Card issuers<br>• E-money issuers<br>• Issuing banks **(Refer to FAQ No. 57.)** |
| Payment channels | • Internet banking (includes desktop banking)<br>• Mobile banking | • Internet banking offering banks<br>• Mobile banking offering banks |
| Unauthorised cash withdrawal | • ATM | • ATM acquirers |

### Description of MO for payment-related fraud

3. The REs must refer to the detailed description of MO in **Table 9** to **Table 13** when reporting loss event arising from specific payment instruments or payment channels.

[7] E-money comprises card-based and network-based e-money schemes. International brand prepaid card is categorised under card-based e-money scheme.

(a) Payment instrument: Credit card, debit card, charge card and card-based e-money schemes

**Table 9: Card-related fraud MO**

| MO | Description |
|---|---|
| **Account Take Over** | Fraudster gains access to existing card account and use them to make fraudulent transactions. This could happen by making fraudulent card replacement request or false change of address request |
| **Counterfeit** | Fraudsters copies data from the card (typically magnetic strip) and illegally reproduced or duplicate the card and make fraudulent transactions |
| **Forged Application** | Fraudster applied for a card under the identity of another person and subsequently uses the card to make fraudulent transactions |
| **Internet**<br>Authenticated internet transaction<br>Unauthenticated internet transaction | Card information obtained illegally and subsequently used to order goods or services through the internet<br>(a) Authenticated internet transaction: Internet transaction that was authenticated by verifying the cardholder's password<br>(b) Unauthenticated internet transaction: Internet transaction where authentication was not performed or could not be performed |
| **Mail and Telephone Order** | Card information obtained illegally and subsequently used to order goods or services through telephone or mail |
| **Loss or Stolen** | (a) Card is misplaced or lost (by accident or other means) and subsequently used fraudulently; or<br>(b) Card is stolen as a result of theft, burglary, robbery or other criminal means and used subsequently used fraudulently. |
| **Wire Tapping** | Card information obtained illegally by tapping the telephone lines. The information is subsequently used to make fraudulent transactions |
| **Non-Receipt** | Card is stolen from the issuer’s delivery system and subsequently used to make fraudulent transactions |

(b) Payment instrument: Network-based e-money scheme

**Table 10: Network based e-money scheme MO**

| MO | Description |
|---|---|
| **Lost or stolen mobile devices** | (a) Mobile phone is either misplaced or lost (by accident or other means) and subsequently used fraudulently<br>(b) Mobile phone is stolen as a result of theft, burglary, robbery or other criminal means and used fraudulently |
| **Stolen or compromised login credentials** | Login credentials obtained illegally, such as via e-mail and short message services (SMS) and subsequently used to access the e-money account of the genuine owner to make payment for goods or services or to transfer fund |
| **Wire tapping** | Account information obtained illegally by tapping the telephone lines and then used to make fraudulent transactions |
| **Illegal e-money value** ***(also applicable to card-based e-money scheme)*** | Manipulation of e-money balance / illegally reload or top-up by fraudster so that the account appears to have a greater monetary value than the amount actually paid by the user |

(c) Payment instrument: Cheque

**Table 11: Cheque fraud MO**

| MO | Description |
|---|---|
| **Cloning** | A wholly fabricated cheque or duplicated copy of a genuine cheque. |
| **Forgery** | A genuine cheque issued without obtaining proper authorisation from the cheque owner, using forged signature. |
| **Alteration** | A genuine cheque of which its details are illegally altered. |

(d) Payment channel: Internet banking fraud

Any fraudulent transactions performed by a third party via internet banking services offered by the REs (including access to internet web browser using mobile devices). Cases whereby beneficiary accounts or mule accounts are maintained at REs shall be excluded.

Any other scams involving customers transferring funds willingly via various social engineering, not classified as an unauthorised transaction (e.g. love scam and telephone scam) must not be captured in this report.

**Table 12: Internet banking fraud MO**

| MO | Description |
|---|---|
| **Phishing**<br>• **Email**<br>• **SMS**<br>• **Telephone** | A method used by fraudsters to access valuable personal information such as username, PIN and passwords by sending 'spoofed' e-mail messages, sending messages via short messaging service (SMS), making telephone calls etc. to lure customers into divulging such information. This information will be used to conduct unauthorised internet banking transactions<br>Fraudsters may:<br>a) Copy legitimate logos or message formats with links to direct customers to fake internet banking websites that are convincing replicas of the banks' genuine internet banking websites; and/or<br>b) Direct customers to update or register mobile phone number via automated teller machine (ATM) to obtain transaction authorisation codes (TACs) for the completion of unauthorised internet banking transactions |
| **Others:** | REs must specify the fraud MO in the loss event description field: |
| • **Malware** | • Malicious software installed unknowingly in customers' computer / mobile phone / other devices to ultimately obtain internet banking credentials or TACs to conduct unauthorised internet banking transactions |
| • **SIM Card Hijack** | • Fraudster impersonating the customer at mobile service provider, to replace the SIM card of registered mobile number to receive TACs in order to conduct unauthorised internet banking transactions |

| MO | Description |
|---|---|
| • **Unauthorised Internet Banking Transaction** | • Fraudster used stolen customer credentials for the registration of new internet banking profile to conduct unauthorised internet banking transactions |
| • **Browser redirect** | • Fraudster used links on search engine results to direct customers to fake internet banking websites to conduct unauthorised internet banking transactions |
| • **Other new MO** | • Please provide details of the MO |

(e) Payment channel: Mobile banking fraud

Any fraudulent transactions performed by a third party through a mobile device via mobile banking applications (including but not limited to, SMS and Unstructured Supplementary Service Data, USSD[8] based banking platform) offered by the REs. Cases whereby beneficiary accounts or mule accounts are maintained at REs shall be excluded.

Any other scams involving customers transferring funds willingly via various social engineering methods, not classified as an unauthorised transaction (e.g. love scam and telephone scam) must not be captured in this report.

**Table 13: Mobile banking fraud MO**

| MO | Description |
|---|---|
| **Phishing**<br>• Email<br>• SMS<br>• Telephone | Customers are lured into divulging personal information such as username, PIN and passwords to conduct unauthorised mobile banking transactions |
| **Others:** | REs must specify the fraud modus operandi in the loss event description field: |
| • Malware | • Malicious software installed unknowingly in customers' computer / mobile phone / other devices to ultimately obtain mobile banking credentials or TACs to conduct unauthorised mobile banking transactions |
| • SIM Card Hijack | • Fraudster impersonating the customer at mobile service provider, to replace the SIM card of registered mobile number to receive TACs in order to conduct unauthorised mobile banking transactions |

[8] USSD is a technology used by a GSM network to send information, usually text menu between a mobile phone and a system on the network.

| MO | Description |
|---|---|
| • Unauthorised Mobile Banking Transaction<br>• Other new MO | • Fraudster used stolen customer credentials for the registration of new mobile banking profile to conduct unauthorised mobile banking transactions<br>• Please provide details of the modus operandi |

**Reporting payment-related fraud in ORION**

4. **Payment-related fraud**

**Category:** 1. Card related fraud with amount involved > RM 5,000
2. New MO
**Event Classification:** Actual loss, potential loss and near miss

| Data fields | Description |
|---|---|
| Reporting Entity Name | To select the respective reporting entity for operational loss events |
| Event Classification | Operational risk events must be classified as either one of the following:<br>• **Actual loss**<br>• **Potential loss**<br>• **Near miss** |
| Nature of Event | • **New** - New type of MO that impacted the REs for the first time.<br>• **Repeated** - MO that has occurred previously at REs<br>Refer to **FAQ No. 35.** |
| Islamic Business | (√) – If the operational risk event is relating to Islamic business or product |
| Loss Event Name | Clear and concise name that reflects an overall summary and nature of the loss event |
| Business Lines | Must be reported up to Level 3 (banking) in accordance with the taxonomy in Appendix 12 |
| Products / Services | Please choose where applicable |
| Delivery Channel | Please choose where applicable |
| Event Category | Must be reported up to Level 3 in accordance with the taxonomy in Appendix 13 |

| Data fields | Description |
|---|---|
| Causal Category | Must be reported up to Level 3 in accordance with the taxonomy in Appendix 14 |
| Date of Occurrence | The date that the event took place |
| Date of Detection | The date of event confirmation is obtained |
| Loss Event Description | An executive summary of the loss event and must include the following details:<br>(a) Chronology of the loss event<br>• Where the event took place<br>• How the event occurred<br>• The modus operandi involved<br>• Parties involved in the event (e.g. customer / staff / outsourced service provider / affiliates, etc.)<br>• The root cause of the event<br>(b) Remedial actions to resolve the event<br>(c) Mitigating action plans to prevent recurrence of similar incident in the future<br>(d) Indication of timeline when the event can be resolved<br>(e) Progressive update of the event post-reporting to ORION<br><br>The executive summary must not include customer / individual confidential information e.g. Name, I/C Number and other personal information |
| Event Impact | Please choose one event impact from the following:<br>• **Financial Impact** - There is an actual or potential financial loss<br>• **Non-Financial Impact** – No loss amount involved but has impact on reputation, non-compliance etc.<br>• **Both Financial and Non-Financial** – as defined above |
| Financial Impact >> Events For | RE must select whichever applicable:<br>• Event for ATM Acquirer<br>• Event for Payment Instrument<br>• Event for Payment Channel |
| Financial Impact >> Events For | **>> ATM Acquirer**<br><br>**>> Payment instrument**<br>REs must select whichever applicable:<br>• Credit Card |

| Data fields | Description |
|---|---|
| | • Debit Card<br>• Charge Card<br><br>**>> Card brands**<br>REs must select whichever applicable:<br><br>Credit card & Charge card:<br>• Visa<br>• MasterCard<br>• AMEX<br>• CUP<br>• Diners<br>• Other (please specify)<br><br>Debit card<br>• International debit card – Visa<br>• International debit card – MasterCard<br>• International debit card – Others (please specify)<br>• E-Debit (Domestic debit, MyDebit)<br>• Combo (Co-badge card[9]) |
| Financial Impact<br>>> Events For | **>>Payment instrument**<br><br>REs must select whichever applicable:<br>• Cheque<br>• Credit Card<br>• Debit Card<br>• Charge Card<br>• E-Money |
| >>Payment Instrument<br><br>>> Cheque | **>>Cheque**<br><br>**Modus operandi** - REs must select whichever applicable:<br>• Cloning<br>• Forgery<br>• Alteration<br>• Others (please specify)<br><br>**Source of detection** – REs must select whichever applicable:<br>• Detected by collecting bank<br>• Detected by issuing bank<br>• Detected by customers<br>• Others (please specify) |

[9] A co-badged card is a card with two payment brand applications (e.g. MyDebit and Visa) that can be used for purchases at point-of-sales (POS) terminals.

| Data fields | Description |
|---|---|
| | **Types of cheque issuers** - REs must select whichever applicable:<br>• Individual<br>• Corporate<br>• Government<br>• Others (please specify) |
| >>Payment Instrument<br><br>>> Credit card<br>>> Debit card<br>>> Charge card<br>>> E-money | **>> Credit card;**<br>**>> Debit card;**<br>**>> Charge card; and**<br>**>> E-money**<br><br>**Card brands** - REs must select whichever applicable:<br><br><u>Credit card & Charge card:</u><br>• Visa<br>• MasterCard<br>• AMEX<br>• CUP<br>• Diners<br>• Other (please specify)<br><br><u>Debit card</u><br>• International debit card – Visa<br>• International debit card – MasterCard<br>• International debit card – Others (please specify)<br>• E-Debit (Domestic debit, MyDebit)<br>• Combo (Co-badge card)<br><br><u>E-money</u><br>• Card-based – Proprietary prepaid card<br>• Card-based – International prepaid card – Visa<br>• Card-based – International prepaid card – MasterCard<br>• Card-based – International prepaid card – Others (please specify)<br><br>**Card types** - REs must select whichever applicable:<br>• Magnetic Stripe<br>• Chip<br>• Chip and PIN<br>• Contactless<br>• Others (please specify) |

| Data fields | Description |
|---|---|
| | **Business activity** - REs must select whichever applicable :<br>• Airlines or Air carriers<br>• Travel agencies and tour operators<br>• Telecommunication equipment including telephone sales<br>• Utilities (electric / gas / water / sanitation)<br>• Department stores<br>• Grocery stores and supermarkets<br>• Miscellaneous food stores<br>• Automotive parts stores<br>• Service stations<br>• Automated fuel dispensers<br>• Electronic sales<br>• Eating places / restaurants<br>• Bars / taverns / lounge / discos / night clubs<br>• Jewellery / watch / clock / silverware stores<br>• Direct marketing including insurance service / travel arrangement services / Telemarketing merchants / Subscription merchants<br>• Insurance sales or underwriting and premiums<br>• Lodging / hotels / motels / resorts<br>• Professional services<br>• Unauthorised cash withdrawals<br>• Others (please specify)<br>**Modus operandi** - REs must select whichever applicable:<br>Credit card, Debit card and Charge card<br>• Account takeover<br>• Counterfeit – credit master<br>• Counterfeit – skimming<br>• Counterfeit – white plastic<br>• Forged application<br>• Internet – authenticated internet transaction<br>• Internet - unauthenticated internet transaction<br>• Loss or stolen<br>• Mail and telephone order<br>• Wire tapping<br>• Non-receipt<br>• Other (please specify) |

| Data fields | Description |
|---|---|
| | E-money<br>• Card-based – Account takeover<br>• Card-based – Counterfeit – Credit Master<br>• Card-based – Counterfeit – skimming<br>• Card-based – Counterfeit – white plastic<br>• Card-based – Forged application<br>• Card-based – Internet – authenticated internet transaction<br>• Card-based – Internet - unauthenticated internet transaction<br>• Card-based – Loss or stolen<br>• Card-based – Mail and telephone order<br>• Card-based – Wire tapping<br>• Card-based – Non-receipt<br>• Card-based – Illegal E-money value<br>• Card-based – Other (please specify)<br>• Network-based – Loss or stolen mobile devices<br>• Network-based – stolen or compromised login credentials<br>• Network-based – Wire tapping<br>• Network-based – Illegal E-money value<br>• Network-based – Other (please specify) |
| Financial Impact<br>>> Event For | **>> Payment channel**<br>REs must select whichever applicable:<br>• Internet Banking<br>• Mobile Banking |
| >>Payment Channel<br>>> Internet Banking<br>>> Mobile Banking | **>>Internet Banking**<br>**>>Mobile Banking**<br>**Account type** - REs must select whichever applicable:<br>Internet Banking & Mobile Banking:<br>• Individual<br>• Corporate<br>• Others (please specify)<br>**Modus operandi** - REs must select whichever applicable:<br>Internet Banking & Mobile Banking:<br>• Phishing - Email<br>• Phishing – SMS<br>• Phishing – Telephone<br>• Others (please specify) |

| Data fields | Description |
|---|---|
| Amount Involved | This field must have a value to reflect the overall financial amount associated with the operational risk event reported |
| Financial Impact (for Banking, ATM Acquirer and Payment Channel)<br>>> Actual Loss / Potential Loss / Recoveries | REs must record the actual loss / potential loss / recovery amount incurred according to the following categories:<br>• Reporting Entity^<br>• Customer^^<br>• 3rd Party<br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field<br>*(Note:*<br>*^ Please input the date of write-off or provision recognised in P&L in the "Comments" column.*<br>*^^ Please input the loss amount borne or partially borne by the customer)* |
| Financial Impact (for Payment Instrument)<br>>> Loss Incurred by Malaysian Entities | REs must record the loss amount incurred according to the following categories:<br>• Actual Loss and / or;<br>• Recoveries and / or;<br>• Potential Loss<br>**Payment Instrument**<br>Payment card and e-money fraud:<br>• Card issuers;<br>• Cardholders;<br>• Acquirer / merchants; and<br>• Others<br>Cheque fraud:<br>• Collecting banks;<br>• Issuing banks;<br>• Customers; and<br>• Others<br>Please ensure the above selection is consistent with the "Event Classification" field above<br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field |

| **Data fields** | **Description** |
|---|---|
| Financial Impact (for Payment Instrument)<br>>> Loss Incurred by Foreign Entities | REs must record the loss amount incurred by foreign entities according to the following categories:<br>• Actual Loss and / or;<br>• Recoveries and / or;<br>• Potential Loss<br><br>Please ensure the above selection is consistent with the "Event Classification" field above<br><br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field |
| Actual Loss / Potential Loss / Recoveries | REs must record the actual loss / potential loss / recovery amount incurred according to the following categories:<br>• Reporting Entity^<br>• Customer^^<br>• 3rd Party<br><br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field<br><br>*(Note:*<br>*^ Please input the date of write-off or provision recognised in P&L in the "Comments" column.*<br>*^^ Please input the loss amount borne or partially borne by the customer)* |
| Non-Financial<br>>>Impact | Please choose either:<br>Low / Medium / High |
| Non-Financial<br>>> Comments | The detailed description of the non-financial impact must be provided to justify the selection of Low / Medium / High |

**">>"** represents sub-data fields

## APPENDIX 10 Aggregate reporting requirements

1. REs must submit aggregate reporting to ORION in accordance with the requirements and timeline set out in **Table 2: Reporting types and timelines**.

2. REs must report aggregate events in accordance with the categories and threshold specified in **Table 14: Aggregate reporting types and threshold**.

3. Events with new MO and / or with amount that are above the threshold specified in **Table 14,** must NOT be aggregated and must be reported as a single event in ORION according to **Appendix 2: Operational risk event reporting requirements.**

**Table 14: Aggregate reporting types and threshold**

| Category | Sub-category | Aggregate threshold | Aggregate submission to ORION |
|---|---|---|---|
| **Payment instrument** | Aggregate by card types*:<br>• Credit card<br>• Charge card<br>• Debit card<br>**Note: including card fraud committed overseas* | Amount involved ≤ RM5,000 | To submit:<br>• 1 event for ALL actual loss<br>• 1 event for ALL potential loss<br>• 1 event for ALL near miss |
| **Actual loss events ≤ RM 1,000** | Aggregate by event types:<br>• Internal fraud<br>• External fraud<br>• Employment practices and workspace safety<br>• Damage to physical assets<br>• Business disruption and system failure<br>• Clients, products and business practices<br>• Execution, delivery and process management | Actual loss ≤ RM1,000 | To submit:<br>• 1 event for actual loss per event type |

| Category | Sub-category | Aggregate threshold | Aggregate submission to ORION |
|---|---|---|---|
| **All physical cash shortages** | Aggregate by event types:<br>- Clients, products and business practices<br>- Execution, delivery and process management<br>- External fraud | All actual loss | To submit:<br>- 1 event for shortages at both branch and vendor per event type |

**Reporting aggregate events in ORION**

4. Payment instrument - Card related fraud with amount involved ≤ RM 5,000

**Category:** Card related fraud with amount involved ≤ RM 5,000
**Sub-Category:** Aggregate by credit card, debit card and charge card
**Event Classification:** Actual loss, potential loss or near miss

| Data fields | Description |
|---|---|
| Reporting Entity Name | To select the correct entity |
| Event Classification | Please select one (where applicable):<br>- **Actual Loss**<br>- **Potential Loss**<br>- **Near Miss** |
| Nature of Event | **Repeated** - MO that has occurred previously at REs |
| Islamic Business | If reporting on behalf of Islamic Entity, please '√' |
| Loss Event Name | Aggregate Credit Card***** fraud (MM/YY)<br>**interchangeable with Charge Card and Debit Card* |
| Business Lines | For credit card and charge card, please categorise the business line as follows:<br>- Level 1: Retail Banking<br>- Level 2: Card Services<br>- Level 3: Cards<br><br>For debit card, please categorise the business line as follows:<br>- Level 1: Retail Banking<br>- Level 2: Retail Banking |

<table>
<tr><th>Data fields</th><th>Description</th></tr>
<tr><td></td><td>• Level 3: Deposit</td></tr>
<tr><td>Products / Services</td><td>Please select one (where applicable):<br>• Credit Card<br>• Debit Card<br>• Charge Card</td></tr>
<tr><td>Delivery Channel</td><td>Please select: N/A</td></tr>
<tr><td>Event Category</td><td>Please categorise the event as follows:<br>• Level 1: External Fraud<br>• Level 2: Theft &amp; Fraud<br>• Level 3: Card Related Fraud</td></tr>
<tr><td>Causal Category</td><td>Please categorise the causal as follows:<br>• Level 1: External Event<br>• Level 2: Others<br>• Level 3: Others<br><br>Please type ‘N/A’ in the comment box</td></tr>
<tr><td>Countries of Event</td><td>Please select ‘Malaysia’</td></tr>
<tr><td>State of Events</td><td>Please select any state</td></tr>
<tr><td>Districts of Events</td><td>Please select any district</td></tr>
<tr><td>Date of Event Occurrence &amp; Date of Detection</td><td>Choose one date to represent the overall events recorded in a particular month</td></tr>
<tr><td>Loss Event Description</td><td>Please use this standard format for:<br><b>Card-related fraud amount involved ≤ RM 5,000</b><br><br>1. <b>Modus Operandi (MO)</b><br>
<table>
<tr><th>MO</th><th>Amount</th><th>No. of cases</th></tr>
<tr><td>Account take over</td><td>x</td><td>x</td></tr>
<tr><td>Counterfeit</td><td>…</td><td>…</td></tr>
<tr><td>Forged application</td><td>…</td><td>…</td></tr>
<tr><td>Internet – Authenticated</td><td>…</td><td>…</td></tr>
<tr><td>Internet – Unauthenticated</td><td>…</td><td>…</td></tr>
<tr><td>Mail &amp; Telephone Order</td><td>…</td><td>…</td></tr>
<tr><td>Loss or Stolen</td><td>…</td><td>…</td></tr>
<tr><td>Wire Tapping</td><td>…</td><td>…</td></tr>
<tr><td>Non-Receipt</td><td>…</td><td>…</td></tr>
<tr><td>TOTAL AMOUNT / CASE</td><td>x</td><td>x</td></tr>
</table>
<br>2. <b>Card Brand</b><br>
<table>
<tr><th>Credit / Charge Card</th><th>Amount</th><th>No. of cases</th></tr>
<tr><td>• Visa</td><td>x</td><td>x</td></tr>
<tr><td>• MasterCard</td><td>x</td><td>x</td></tr>
</table>
</td></tr>
</table>

| Data fields | Description |
|---|---|
| | • AMEX … …<br>• CUP … …<br>• Diners … …<br>• Others … …<br><br>**Debit Card** **Amount** **No. of cases**<br>• International debit card - Visa x x<br>• International debit card - MasterCard x x<br>• International debit card - Others x x<br>• E-Debit (Domestic debit, MyDebit) x x<br>• Combo (Co-badge card) x x<br><br>**3. Card Type**<br><br>**Credit / Charge Card / Debit card** **Amount** **No. of cases**<br>• Magnetic stripe x x<br>• Chip x x<br>• Chip and PIN … …<br>• Contactless … …<br>• Others … … |
| Event Impact | Select one from the list:<br>• Financial<br>• Non-financial<br>• Financial & Non-financial |
| Events For | Select 'Payment Instrument' |
| >> Payment Instruments | Select one from the list (where applicable):<br>• Credit Card<br>• Debit Card<br>• Charge Card |
| >> Card Brands | Select 'N/A' – to represent the overall incidents recorded in a particular month |
| >> Card Types | Select 'N/A' – to represent the overall incidents recorded in a particular month |
| >> Business Activity | Select 'Others' – to represent the overall incidents recorded in a particular month<br><br>Please type 'N/A' in the comment box |
| >> Modus Operandi | Select 'Others' – to represent the overall incidents during the reporting month<br><br>Please type 'N/A' in the comment box |

| **Data fields** | **Description** |
|---|---|
| Amount Involved | This field must have a value to reflect the overall financial amount associated with the operational risk event reported |
| Loss By Malaysian Entities | Input the total aggregated loss incurred according to the specific categories provided:<br>• Reporting Entity / Issuer<br>• Cardholder / Customer<br>• Acquirer / Merchant<br>• Others<br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field |
| Loss By Foreign Entities | Input the total aggregated loss incurred according to the specific categories provided.<br>• Foreign Entity<br>The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field.<br>Instead, recovered amount must be recorded in the 'Recovery Amount' field |

**“>>”** represents sub-data fields

## 5. Actual loss events ≤ RM 1,000

**Category:** Actual loss events ≤ RM 1,000<br>
**Sub Category:** Aggregate by Event Types<br>
**Event Classification:** Actual loss

| Data fields | Description |
|---|---|
| Reporting Entity Name | To select the correct entity |
| Event Classification | only **Actual Loss** |
| Nature of Event | **Repeated -** MO that has occurred previously at REs |
| Islamic Business | If reporting on behalf of Islamic Entity, please '√' |
| Loss Event Name | Aggregate loss below RM 1,000 (MM/YY) |
| Business Lines | Since this is an aggregate report, please select the business lines that are mostly affected.<br>Must be reported up to Level 3 (banking) and Level 2 (insurance) in accordance with the taxonomy in Appendix 12 |
| Products / Services | Please select: N/A |
| Delivery Channel | Please select: N/A |
| Event Category | **Level 1**: Please select according to your submission:<br>• Internal Fraud<br>• External Fraud<br>• Employment Practices and Workspace Safety<br>• Damage to Physical Assets<br>• Business Disruption and System Failure<br>• Clients, Products and Business Practices<br>• Execution, Delivery and Process Management<br>**Level 2**: Since this is an aggregate report, please select the Event Types that are mostly relevant<br>**Level 3**: Since this is an aggregate report, please select the Event Types that are mostly relevant |
| Causal Category | Since this is an aggregate report, please select the Causal Category that are mostly relevant. |

<table>
<tr><th>Data fields</th><th>Description</th></tr>
<tr><td></td><td>Must be reported up to Level 3 in accordance with the taxonomy in Appendix 14</td></tr>
<tr><td>Countries of Event</td><td>Please select ‘Malaysia’</td></tr>
<tr><td>State of Events</td><td>Please select any state</td></tr>
<tr><td>Districts of Events</td><td>Please select any district</td></tr>
<tr><td>Date of Event Occurrence &amp; Date of Detection</td><td>Select one date to represent the overall incidents recorded in a particular month</td></tr>
<tr><td>Loss Event Description</td><td>Please use this standard format for:<br><b>Actual loss events ≤ RM 1,000</b>
<table>
<tr><th>Event Type</th><th>Amount</th><th>No. of cases</th><th>No. of customers impacted</th></tr>
<tr><td>Ext. Fraud</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>Damage to Physical Assets</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>TOTAL</td><td>X</td><td>X</td><td>X</td></tr>
</table>
<i>*Note: this aggregate table formal is applicable to all seven operational risk event types</i></td></tr>
<tr><td>Event Impact</td><td>Please select: Financial</td></tr>
<tr><td>Events For</td><td>Please select one (where applicable):<br>• Banking<br>• Insurance &amp; Takaful Operators</td></tr>
<tr><td>&gt;&gt; Banking</td><td>&gt;&gt;&gt; Boundary Event: No</td></tr>
<tr><td>&gt;&gt; Insurance &amp; Takaful Operators</td><td>&gt;&gt;&gt; Insurance category:<br>Please select: N/A</td></tr>
<tr><td>Amount Involved</td><td>This field must have a value to reflect the overall financial amount associated with the operational risk event reported</td></tr>
<tr><td>Loss By Banks<br>OR<br>Loss By Insurance &amp; Takaful Operators</td><td>The REs must input the total aggregated loss incurred according to the specific categories provided:<br>• Reporting Entity<br>• Customer<br>• 3rd Party<br><br>The REs must not use losses net of insurance recoveries as an input to the ‘Actual Loss’ field. Instead, recovered amount must be recorded in the ‘Recovery Amount’ field.</td></tr>
</table>

**“>>”** represents sub-data fields

6. Physical cash shortages

**Category:** Banking OR Insurance & Takaful Operators
**Scope:** Physical cash shortages at branch, over-the-counter and / or Vendor for offsite Self-Service Terminals (SST).
Refer to **FAQ No. 40.**
**Event Classification:** Actual loss

| **Data fields** | **Description** |
|---|---|
| Reporting Entity Name | To select the correct entity |
| Event Classification | only **Actual Loss** |
| Nature of Event | **Repeated** - MO that has occurred previously at REs |
| Islamic Business | If reporting on behalf of Islamic Entity, please '√' |
| Loss Event Name | Physical Cash Shortage (MM/YY) |
| Business Lines | **Banks**; please select:<br>Level 1: Retail Banking<br>Level 2: Retail Banking<br>Level 3: Deposits<br><br>**Insurance & Takaful Operators**; please select up to Level 2 (where applicable) |
| Products / Services | Please select: N/A |
| Delivery Channel | Please select: N/A |
| Event Category | Please categorise the event as follows:<br>For execution errors<br>Level 1: EDPM<br>Level 2: Transaction capture, execution & maintenance<br>Level 3: Other Task miss-performance<br><br>For counterfeit notes accepted by Self-Service Terminals<br>Level 1: BDSF<br>Level 2: System<br>Level 3: Software - Application system bug / unpatched<br><br>For counterfeit notes discovered through over-the-counter and during internal processing and/or by the outsourced service provider<br>Level 1: External Fraud<br>Level 2: Theft and fraud<br>Level 3: Forgery/ Counterfeit<br><br>For penalties on cash shortages / cash excess |

<table>
<tr><th>Data fields</th><th>Description</th></tr>
<tr><td></td><td>Level 1: CPBP<br>Level 2: Suitability, disclosure and fiduciary<br>Level 3: Fiduciary breaches/guideline violations</td></tr>
<tr><td>Causal Category</td><td>Please select the Causal Category that are mostly relevant. Must be reported up to Level 3 in accordance with the taxonomy in Appendix 14</td></tr>
<tr><td>Date of Event Occurrence &amp; Date of Detection</td><td>Select one date to represent the overall incidents recorded in a particular month</td></tr>
<tr><td>Loss Event Description</td><td>Please use this standard format for:<br><b>All physical cash shortages* at branch or offsite Self-Service Terminals (SSTs)</b>
<table>
<tr><th>Cash shortage</th><th>Amount</th><th>No. of cases</th><th>No. of customers impacted</th><th>PDRM Report Number</th><th>Serial Number</th><th>No of pieces</th></tr>
<tr><td>Branch SSTs</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>Over-the-counter</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>Offsite SSTs</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>TOTAL</td><td>X</td><td>X</td><td>X</td><td></td><td></td><td>X</td></tr>
</table>
<i>*Note: including events where losses were absorbed by outsourced vendor</i></td></tr>
<tr><td>Event Impact</td><td>Please select: Financial</td></tr>
<tr><td>Events For</td><td>Select either:<br>• Banking<br>• Insurance &amp; Takaful Operators</td></tr>
<tr><td>&gt;&gt; Banking</td><td>&gt;&gt;&gt; Boundary Event: No</td></tr>
<tr><td>&gt;&gt; Insurance &amp; Takaful Operators</td><td>&gt;&gt;&gt; Insurance category:<br>Please select: N/A</td></tr>
<tr><td>Amount Involved</td><td>This field <u>must</u> have a value to reflect the overall financial amount associated with the operational risk event reported</td></tr>
<tr><td>Loss By Banks<br>OR<br>Loss By Insurance &amp; Takaful Operators</td><td>The REs must input the total aggregated loss incurred according to the specific categories provided:<br>• Reporting Entity<br>• Customer<br>• 3<sup>rd</sup> Party<br><br>The REs must not use losses net of insurance recoveries as an input to the ‘Actual Loss’ field. Instead, recovered amount must be recorded in the ‘Recovery Amount’ field</td></tr>
</table>

**“>>”** represents sub-data fields

## APPENDIX 11 Overseas loss event reporting requirements

1. The REs must report all operational risk events occurred at foreign and offshore subsidiaries or branches of the REs which resulted in financial-related losses in accordance with the requirements and timelines set out in **Table 2: Reporting types and timelines**.

2. REs must report these losses in aggregate according to **Table 15: Overseas loss event reporting requirements**.

3. Events with amount that are above the threshold specified in **Table 15,** must NOT be aggregated and must be reported as a single event in ORION. Refer to **FAQs No. 46 and 47.**

**Table 15: Overseas loss event reporting requirements**

| Category | Sub-category | Amount | Submission to ORION |
|---|---|---|---|
| **Overseas losses** | Event ≥ RM 1mil | All actual financial loss | To submit loss event individually |
| | Aggregate by country for event < RM 1mil | All actual financial loss | To submit the loss event aggregated by country (1 event for ALL actual loss) |

**Reporting overseas operational risk events in ORION**

4. Overseas operational risk events

**Category:** Overseas operational risk events
**Event Classification:** Actual loss

| Data fields | Individual ≥ RM 1mil | Aggregate < RM 1mil |
|---|---|---|
| Reporting Entity Name | To select the correct entity | To select the correct entity |
| Event Classification | Only **Actual Loss** | Only **Actual loss** |
| Loss Event Name | [Country name] Overseas Losses (MM/YY) | [Country name] Overseas Losses (MM/YY) |
| Countries of Event | Please select the 'country' involved | Please select the 'country' involved |
| Loss Event Description | (a) Chronology of the loss event<br>• Where the event took place | Please input 'N/A' |

| Data fields | Individual ≥ RM 1mil | Aggregate < RM 1mil |
|---|---|---|
| | • How the event occurred<br>• The modus operandi involved<br>• Parties involved in the event (e.g. customer / staff / outsourced service provider / affiliates, etc.)<br>• Number of customers affected by the event<br>• Number of business lines affected<br>• The root cause of the event<br>(b) Remedial actions to resolve the event<br>(c) Mitigating action plans to prevent recurrence of similar incident in the future | |
| Level 1 Business Line | Please select the relevant Business Line | N/A – this is a mandatory field, please select any from the list |
| Level 1 Event Category | Please select the relevant Event Type | N/A - this is a mandatory field, please select any from the list |
| No of Events | Please input '1' | Count of loss events reported |
| Amount Involved | This field must have a value to reflect the overall financial amount associated with the operational risk event reported | This field must have a value to reflect the overall financial amount associated with the operational risk event reported |
| Net Actual Loss | The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. | The REs must not use losses net of insurance recoveries as an input to the 'Actual Loss' field. |

| Data fields | Individual ≥ RM 1mil | Aggregate < RM 1mil |
|---|---|---|
| | Instead, recovered amount must be recorded in the ‘Recovery Amount’ field | Instead, recovered amount must be recorded in the ‘Recovery Amount’ field |
| Net Potential Loss | Please input ‘0’ (zero) | Please input ‘0’ (zero) |
| Add Row Link | | N/A |
| Delete Row Link | | N/A |
| Check box | | N/A |

## APPENDIX 12 Business lines taxonomy

1. The event must be assigned by REs to the business line category that most accurately describe the business that bears the loss.

2. Events impacting more than one business line must be mapped by REs to the most dominant, or the most suitable business line category.

**Banking**

| Business line level 1 | Business line level 2 | Business line level 3 | Product / Services |
|---|---|---|---|
| 1. Commercial Banking | Corporate Banking | Trade Finance | Export Finance |
| | | | Bills of Exchange |
| | | | LC or BA or TR |
| | | Lending / Financing | Project Finance |
| | | | Non-Individual Mortgage |
| | | | Non-Individual Hire Purchase |
| | | | TL or OD etc. |
| | | | Lending / Financing |
| | | Factoring | |
| | | Leasing | |
| | | Deposits / Funding | Current Account |
| | | | Fixed Deposit |
| | | | Savings |
| | | | NID |
| | | | CP / MTN |
| | | Guarantees | Bank Guarantee |
| | | | Performance Guarantee |
| | Commercial Banking | Trade Finance | Export Finance |
| | | | Bills of Exchange |
| | | | LC or BA or TR |
| | | Lending / Financing | Project Finance |
| | | | Non-Individual Mortgage |
| | | | Non-Individual Hire Purchase |
| | | | TL or OD etc. |
| | | | Lending / Financing |
| | | Factoring | |
| | | Leasing | |
| | | Deposits / Funding | Current Account |
| | | | Fixed Deposit |
| | | | Savings |
| | | | NID |
| | | | CP / MTN |

| Business line level 1 | Business line level 2 | Business line level 3 | Product / Services |
|---|---|---|---|
| | | Guarantees | Bank Guarantee |
| | | | Performance Guarantee |
| | SME | Trade Finance | Export Finance |
| | | | Bills of Exchange |
| | | | LC or BA or TR |
| | | Lending / Financing | Project Finance |
| | | | Non-Individual Mortgage |
| | | | Non-Individual Hire Purchase |
| | | | TL or OD etc. |
| | | | Lending / Financing |
| | | Factoring | |
| | | Leasing | |
| | | Deposits / Funding | Current Account |
| | | | Fixed Deposit |
| | | | Savings |
| | | | NID |
| | | | CP / MTN |
| | | Guarantees | Bank Guarantee |
| | | | Performance Guarantee |
| 2. Retail Banking | Retail Banking | Mortgage | Residential |
| | | | Non-Residential |
| | | Personal Loan / Financing | |
| | | Hire Purchase | |
| | | Wealth Management | |
| | | Deposits | Current Account |
| | | | Fixed Deposits |
| | | | Savings |
| | | | NID |
| | | | Structured Deposits |
| | Private Banking | Mortgage | Residential |
| | | | Non-Residential |
| | | Personal Loan / Financing | |
| | | Hire Purchase | |
| | | Wealth Management | |
| | | Deposits | Current Account |
| | | | Fixed Deposits |
| | | | Savings |
| | | | NID |

| Business line level 1 | Business line level 2 | Business line level 3 | Product / Services |
|---|---|---|---|
| | | | Structured Deposits |
| | Card Services | Cards | Credit Card |
| | | | Debit Card |
| | | | Charge Card |
| | E Money | Card Based | |
| | | Network Based | |
| 3. Trading and Sales | Treasury | Fixed income | |
| | | Equity | |
| | | Foreign exchanges | |
| | | Commodities | |
| | | Credit | |
| | | Funding | |
| | | Own position securities | |
| | | Lending and repos | |
| | | Brokerage | |
| | | Debt | |
| | | Prime brokerage | |
| | Sales | Fixed income | |
| | | Equity | |
| | | Foreign exchanges | |
| | | Commodities | |
| | | Credit | |
| | | Funding | |
| | | Own position securities | |
| | | Lending and repos | |
| | | Brokerage | |
| | | Debt | |
| | Market Making | Fixed income | |
| | | Equity | |
| | | Foreign exchanges | |
| | | Commodities | |
| | | Credit | |
| | | Funding | |
| | | Own position securities | |
| | | Lending and repos | |
| | | Brokerage | |
| | | Debt | |
| | | Prime brokerage | |
| | Proprietary Positions | Fixed income | |
| | | Equity | |
| | | Foreign exchanges | |
| | | Commodities | |
| | | Credit | |

| Business line level 1 | Business line level 2 | Business line level 3 | Product / Services |
|---|---|---|---|
| | | Funding | |
| | | Own position securities | |
| | | Lending and repos | |
| | | Brokerage | |
| | | Debt | |
| | | Prime brokerage | |
| 4. Agency Services | Custody | Escrow | |
| | | Depository receipts | |
| | | Securities lending (customers) corporate actions | |
| | Corporate Agency | Issuer and paying agents | |
| | Corporate Trust | | |
| 5. Asset Management | Discretionary Fund Management | Retail | |
| | | Whole Sale | |
| | Non-Discretionary Fund Management | Retail | |
| | | Whole Sale | |
| 6. Payment and Settlement<br>**Note:** Payment and Settlement losses related to a bank's own activities would be incorporated in the loss experience of the respective affected eight Business Line | Fund Transfer | Interbank | |
| | | Intrabank | |
| | | Local Remittances | |
| | | Overseas Remittances | |
| | Payment & Collection | | |
| | Clearing and Settlements | | |
| 7. Corporate Finance | Advisory Services | Equity | Equity Capital Market |
| | | | Flotation |
| | | | Bonus Issue |
| | | | M&A |
| | | | IPO |
| | | | Private Placement |
| | | | Corporate Restructuring |
| | | Debt | Fund Raising |
| | | | Structured financing |
| | Underwriting | Equity | Equity Capital Market |
| | | | Flotation |
| | | | Bonus Issue |

| Business line level 1 | Business line level 2 | Business line level 3 | Product / Services |
|---|---|---|---|
| | | | M&A |
| | | | IPO |
| | | | Private Placement |
| | | | Corporate Restructuring |
| | | Debt | Fund Raising |
| | | | Structured financing |
| 8. Retail Brokerage | Broking | Equity Broking – Margin | |
| | | Equity Broking– Non Margin | |
| | Futures Broking | Futures Broking – Margin | |
| | | Futures Broking – Non Margin | |

**Insurance**

| Business line level 1 | Business line level 2 |
|---|---|
| 1. General | Fire |
| | Motor |
| | Medical & Health |
| | Marine Hull |
| | Marine Cargo |
| | Aviation |
| | On-shore and Off-shore oil related |
| | Personal accident |
| | Workmen’s compensation & Employee's Liability |
| | Contractor's all risk and engineering |
| | Bonds |
| | Liabilities |
| | Others (Golfers/ D&O/ Plate glass/ Credit Insurance) |
| 2. Takaful General | Fire |
| | Motor |
| | Medical & Health |
| | Marine Hull |
| | Marine Cargo |
| | Aviation |
| | On-shore and Off-shore oil related |
| | Personal accident |
| | Workmen’s compensation & Employee's Liability |
| | Contractor's all risk and engineering |
| | Bonds |
| | Liabilities |
| | Others (Golfers/ D&O/ Plate glass/ Credit Insurance) |
| 3. Life | Ordinary Life Protection |
| | Ordinary Life Investment |
| | Investment Linked |
| | Medical & Health |
| | Annuities |
| | Others (Please Specify) |
| 4. Takaful Family | Ordinary Life Protection |
| | Ordinary Life Investment |
| | Investment Linked |
| | Medical & Health |
| | Annuities |
| | Others (Please Specify) |
| 5. Reinsurers | Facultative |
| | Non Proportional Treaty |
| | Proportional Treaty |
| | Others (Please Specify) |
| 6. Retakaful Operators | Facultative |
| | Non Proportional Treaty |
| | Proportional Treaty |
| | Others (Please Specify) |

## APPENDIX 13 Event types taxonomy

### Banking

| Event type level 1 | Event type level 2 | Event type level 3 |
|---|---|---|
| 1. Internal fraud | Unauthorised activity | Transactions not reported (intentional) |
| | | Transaction type unauthorised |
| | | Mismarking of position (intentional) |
| | | Misuse of privilege information |
| | | Falsifying personal details |
| | | Activity with unauthorised counterparty |
| | | Activity leading to incorrect pricing |
| | | Transactions over-reported |
| | | Unauthorised changes to programs or data or transactions |
| | | Hacking / Cracking |
| | | Misuse of system access (e.g. powerful system ID) |
| | | Computer Virus / Malware Injection |
| | | Programming fraud |
| | Theft and fraud | Fraud / credit fraud / worthless deposits |
| | | Theft or extortion or embezzlement or robbery |
| | | Misappropriation of assets |
| | | Malicious destruction of assets |
| | | Forgery |
| | | Disclosure of confidential information |
| | | Cheque kiting |
| | | Smuggling |
| | | Account take-over / impersonation / etc. |
| | | Tax non-compliance / evasion (wilful) |
| | | Bribes / kickbacks |
| | | Insider trading (not on firm's account) |
| | | Accounting irregularities |
| 2. External fraud | Theft and fraud | Theft / Robbery |
| | | Forgery / Counterfeit (Cover Notes, Policy Certificates, Currency, Cheque, Security Documents / Identification documents) |
| | | Fraudulent billing by suppliers |
| | | Cheque kiting |
| | | Card Related Fraud |
| | | Internet Banking fraud |
| | | Mobile Banking fraud |
| | | E-money / Prepaid card fraud |
| | | Fraudulent account opening |
| | | Fraudulent application for banking products / facilities |
| | Systems security | Hacking damage |
| | | Theft of information |

| **Event type level 1** | **Event type level 2** | **Event type level 3** |
|---|---|---|
| | | Unauthorised changes to programs by external parties |
| | | Misuse of system access by external parties |
| | | Sabotage by external parties |
| 3. Employment practices and workspace safety | Employee relations | Compensation, benefit, termination issues |
| | | Organised labour activity |
| | Safe environment | General liability (slips and falls, etc.) |
| | | Employee health & safety rules events |
| | | Workmen's compensation |
| | Diversity and discrimination | All discrimination types |
| 4. Damage to physical assets | Natural disaster & other losses | Natural disaster – Flood |
| | | Natural disaster – Earthquake |
| | | Natural disaster – Tsunami |
| | | Natural disaster – Others |
| | | Human Losses – Vandalism |
| | | Human Losses – Terrorism |
| | | Damage to Islamic Inventory |
| 5. Business disruption and system failures | Systems | Hardware – Server |
| | | Hardware - Storage Disk |
| | | Hardware - Local Area Network (LAN)/ Wide Area Network (WAN) equipment |
| | | Software - Application system bug / unpatched |
| | | Software - Operating system bug / unpatched |
| | | Software - Database error |
| | | Software - Local Area Network(LAN) / Wide Area Network (WAN) application |
| | | Software - Inadequate system capacity |
| | | Software - System interfaces / linkages issues |
| | | Software - Delay or failure in batch processing |
| | | Telecommunication - Telecommunication network |
| | | Telecommunication - Internet Service providers |
| | | Telecommunication - International and Local Switches (VISA, MasterCard, MEPS & My Clear) |
| | | Security Breach – Virus / Malware |
| | | Security Breach - Distributed Denial of Service |
| | | Security Breach – Hacking / Cracking |
| | | Security Breach - Web defacement |

| Event type level 1 | Event type level 2 | Event type level 3 |
|---|---|---|
| | Non systems | Business Disruption – Fire |
| | | Business Disruption – Earthquake |
| | | Business Disruption – Flood |
| | | Business Disruption – Pandemic |
| | | Business Disruption – Civil Unrest |
| | | Utility Disruption – Electrical Supply |
| | | Utility Disruption – Water Supply |
| 6. Clients, products and business practices | Suitability, disclosure and fiduciary | Fiduciary breaches / guideline violations |
| | | Suitability / disclosure issues (KYC, etc.) |
| | | Retail customer disclosure violations |
| | | Breach of privacy |
| | | Aggressive sales |
| | | Account churning |
| | | Misuse of confidential information |
| | | Lender liability |
| | | Insider trading (on firm's account) |
| | | Unlicensed activity |
| | | Misrepresentation of facts |
| | Improper business or market practices | Antitrust |
| | | Improper trade / market practices |
| | | Market manipulation |
| | | Insider trading (on firm’s account) |
| | | Unlicensed activity |
| | | Money laundering |
| | | Mis-selling |
| | | Mis-informing of Underlying Shariah contract |
| | | Poor servicing by agents |
| | Product flaws | Product defects |
| | | Model errors |
| | | Product defects from Shariah perspective |
| | Selection, sponsorship and exposure | Failure to investigate client per guidelines |
| | | Exceeding client exposure limits |
| | Advisory activities | Disputes over performance of advisory activities |
| 7. Execution, delivery and process management | Transaction capture, execution and maintenance | Miscommunication |
| | | Data entry or maintenance or loading |
| | | Missed deadline or responsibility |
| | | Model / system mis-operation |
| | | Accounting error / entity attribution |
| | | Other task miss-performance |
| | | Service delivery failure |
| | | Collateral management failure |
| | | Reference data maintenance |
| | | Incomplete / failed batch processing |
| | | Ambiguous and unclear policy terms |

| Event type level 1 | Event type level 2 | Event type level 3 |
|---|---|---|
| | Monitoring and reporting | Failed mandatory reporting |
| | | Inaccurate external reporting |
| | | Inaccurate internal report (including not updating recent trends / ratios into claims / premium reserves / inaccurate aging report) |
| | Customer intake and documentation | Client permissions / disclaimers missing |
| | | Legal documents missing / incomplete |
| | | Improper documentation (improper receipting or failure to lodge documents, etc.) |
| | Customer or client account management | Unapproved access given to accounts |
| | | Incorrect client records |
| | | Negligent loss or damage of client assets |
| | Trade counterparties | Non-client counterparty mis-performance |
| | | Miscellaneous non-client counterparty disputes |
| | Vendors & suppliers | Outsourcing |
| | | Breach of SLA |
| | | Technology failure in supplier systems |
| | | Service Delivery failure / capacity |
| | | Vendor disputes |

**Insurance**

| Event type level 1 | Event type level 2 | Event type level 3 |
|---|---|---|
| 1. Internal fraud | Unauthorised activity | Transactions not reported (intentional) |
| | | Transaction type unauthorised |
| | | Mismarking of position (intentional) |
| | | Misuse of privilege information |
| | | Falsifying personal details |
| | | Activity with unauthorised counterparty |
| | | Transactions over-reported |
| | | Unauthorised changes to programs or data or transactions |
| | | Hacking / Cracking |
| | | Misuse of system access (e.g. powerful system ID) |
| | | Computer Virus / Malware Injection |
| | | Programming fraud |
| | Theft and fraud | Theft or extortion or embezzlement or robbery |
| | | Misappropriation of assets |
| | | Malicious destruction of assets |
| | | Forgery |
| | | Disclosure of confidential information |
| | | Smuggling |
| | | Account take-over / impersonation / etc. |
| | | Tax non-compliance / evasion (wilful) |
| | | Bribes / kickbacks |
| | | Insider trading (not on firm's account) |
| | | False insurance claims / premiums |
| | | Inflated insurance claims / payment |
| | | Misappropriation of insurance premium |
| | | Accounting irregularities |
| 2. External fraud | Theft and fraud | Theft / Robbery |
| | | Forgery / Counterfeit (Cover Notes or Policy Certificates or Currency or Cheque or Security Documents) |
| | | Fraudulent billing by suppliers |
| | | False insurance claims / premiums |
| | | Inflated insurance claims |
| | | Misappropriation of insurance premium |
| | | Fraudulent application for products / facilities |
| | Systems security | Hacking damage |
| | | Theft of information |
| | | Unauthorised changes to programs by external parties |
| | | Misuse of system access by external parties |
| | | Sabotage by external parties |

| Event type level 1 | Event type level 2 | Event type level 3 |
|---|---|---|
| 3. Employment practices and workspace safety | Employee relations | Compensation, benefit, termination issues |
| | | Organised labour activity |
| | Safe environment | General liability (slips and falls, etc.) |
| | | Employee health & safety rules events |
| | | Workmen's compensation |
| | Diversity and discrimination | All discrimination types |
| 4. Damage to physical assets | Natural disaster & Other Losses | Natural disaster - Flood |
| | | Natural disaster - Earthquake |
| | | Natural disaster - Tsunami |
| | | Natural disaster - Others |
| | | Human Losses - Vandalism |
| | | Human Losses - Terrorism |
| | | Damage to Islamic Inventory |
| 5. Business disruption and system failures | Systems | Hardware - Server |
| | | Hardware - Storage Disk |
| | | Hardware - Local Area Network (LAN) / Wide Area Network (WAN) equipment |
| | | Software - Application system bug / unpatched |
| | | Software - Operating system bug / unpatched |
| | | Software - Database error |
| | | Software - Local Area Network(LAN) / Wide Area Network (WAN) application |
| | | Software -Inadequate system capacity |
| | | Software - System interfaces / linkages issues |
| | | Telecommunication - Telecommunication network |
| | | Telecommunication - Internet Service providers |
| | | Security Breach – Virus / Malware |
| | | Security Breach – Hacking / Cracking |
| | | Security Breach - Web defacement |
| | Non Systems | Business Disruption - Fire |
| | | Business Disruption - Earthquake |
| | | Business Disruption - Flood |
| | | Business Disruption - Pandemic |
| | | Business Disruption – Civil Unrest |
| | | Utility Disruption –Electrical Supply |
| | | Utility Disruption – Water Supply |
| 6. Clients, products and business practices | Suitability, disclosure and fiduciary | Fiduciary breaches / guideline violations |
| | | Suitability / disclosure issues (KYC, etc.) |
| | | Regulatory compliance of appointed representatives |

| Event type level 1 | Event type level 2 | Event type level 3 |
|---|---|---|
| | | Breach of privacy |
| | | Unlicensed activity |
| | | Misrepresentation of facts |
| | | Misuse of confidential information |
| | | Insider trading (on firm's account) |
| | | Aggressive sales |
| | Improper business or market practices | Antitrust |
| | | Improper trade / market practices |
| | | Market manipulation |
| | | Insider trading (on firm's account) |
| | | Unlicensed activity |
| | | Money laundering |
| | | Mis-selling |
| | | Mis-informing of underlying Shariah contract |
| | | Poor servicing by agents |
| | Product Flaws | Product defects |
| | | Product defects from Shariah perspective |
| | | Unintentional guarantees |
| | Selection, sponsorship and exposure | Failure to investigate client per guidelines |
| | | Exceeding client exposure limits |
| | Advisory activities | Mis-selling due to mortgage endowment |
| 7. Execution, delivery and process management | Transaction capture, execution and maintenance | Miscommunication |
| | | Data entry, maintenance or loading |
| | | Missed deadline or responsibility |
| | | Model / system mis-operation |
| | | Accounting error / entity attribution |
| | | Other task miss-performance |
| | | Service delivery failure |
| | | Incorrect unit pricing / allocation |
| | | Reference data maintenance |
| | | Incomplete / failed batch processing |
| | | Improper maintenance of claim files (claims not updated or not closed in a timely and an appropriate manner) |
| | | Ineffective and inefficient recruitment / termination of agents |
| | Monitoring and reporting | Failed mandatory reporting |
| | | Inaccurate external reporting |
| | | Inaccurate internal report (including not updating recent trends / ratios into claims / premium reserves / inaccurate aging report) |
| | | Client permissions / disclaimers missing |
| | | Legal documents missing / incomplete |

| Event type level 1 | Event type level 2 | Event type level 3 |
|---|---|---|
| | Customer intake and documentation | Inappropriate underwriting |
| | | Inappropriate reinsurance |
| | Customer or client account management | Payment to incorrect client |
| | | Incorrect client records |
| | | Incorrect payment to client |
| | Trade counterparties | Non-client counterparty mis-performance |
| | | Miscellaneous non-client counterparty disputes |
| | Vendors and suppliers | Outsourcing |
| | | Breach of SLA |
| | | Technology failure in supplier systems |
| | | Service delivery failure / capacity |
| | | Vendor disputes |

## APPENDIX 14 Causal categories taxonomy

| Causal categories level 1 | Causal categories level 2 | Causal categories level 3 |
|---|---|---|
| 1. People | Training | Calibre of recruits |
| | | Human error |
| | | Misinterpretation |
| | | Poor relationship management |
| | Competence | Lack of communication |
| | | Not meeting customers reasonable expectations |
| | | Senior management awareness |
| | Knowledge | Key person / knowledge dependency |
| | Culture / Behaviour | Unaware of change |
| | | Senior management knowledge |
| | Inadequate resources | Product too complex |
| | Inappropriate customer / product fit | |
| | Regional / international differences | |
| | Succession planning | |
| | Others | Others (Please specify) |
| 2. Process | Inadequate operational procedures | Dealing with change |
| | Product design | Spreadsheet workarounds |
| | | Lack of documentation |
| | Inadequate monitoring / reporting | Lack of due diligence |
| | | Poor contract / service level agreement |
| | Process change / implementation | Management decision / change not implemented |
| | | Management information inadequate |
| | Inadequate policies | Inadequate checks/balances on senior individuals |
| | Inadequate allocation of accountabilities | |
| | Others | Others (Please specify) |
| 3. System (IT) | Coding | Software design |
| | Testing | Virus |
| | IT strategy | Hardware failure |
| | Complexity of interfaces | Security |
| | Maintenance | Poor user acceptance testing / regression testing |
| | Investment | Legacy systems |

| Causal categories level 1 | Causal categories level 2 | Causal categories level 3 |
|---|---|---|
| | Data integrity | |
| | Resilience | |
| | Others | Others (Please specify) |
| 4. External Event | Trade counterparty | Lack of understanding of third-party data |
| | Customer | Third-party situation beyond firm control (power / telephony / water / services) |
| | Regulatory / political | Reliance on third-party data |
| | Infrastructure failure | Lack of understanding of implications of change to third-party systems |
| | Service Provider | Increase in transaction volume |
| | Environmental factors | Natural disasters |
| | Unrealistic customer expectation | |
| | Disgruntled employee | |
| | Others | Others (Please specify) |

## APPENDIX 15 Key risk indicators taxonomy

### 1. Generic indicators

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 1. Number of application fraud near miss | • Banking<br>• Insurance &Takaful Operators | Number of fraudulent application detected and thwarted for secured / unsecured facility, account opening, insurance proposal submission etc.<br>*Note: Remittance/cheque book/trading bill applications should not be included in the KRI.* | Monthly* |
| 2. Number of new litigation cases initiated against the FI with SNC implications | • Banking<br>• Takaful Operators | Number of new cases that have SNC implications, where the FI was served with Letter of Demand / letter from lawyer within that month | Monthly* |
| 3. Number of reprimands received from other regulators/ enforcement agencies/ operator of designated payment systems | • Banking<br>• Insurance &Takaful Operators | Number of reprimands received from **other** regulators / enforcement agencies / operator of designated payment systems (e.g. Bursa Malaysia, Securities Commission of Malaysia, Inland Revenue Board Of Malaysia (LHDN), Ministry of Human Resource, Companies Commission of Malaysia, Royal Malaysia Police, Fire and Rescue Department of Malaysia, Municipal Council (DBKL), Labuan Financial Services Authority, Paynet etc.) Refer to **FAQ No. 82.** | Monthly* |
| 4. Number of new litigation cases initiated against the FI | • Banking<br>• Insurance &Takaful Operators | Number of new cases initiated against the FI, where the FI was served with Letter of Demand / letter from lawyer within that quarter. The number includes orders received from Industrial Court. | Quarterly* |

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 5. Staff attrition rate | • Banking<br>• Insurance &Takaful Operators | **Attrition rate for permanent staff**<br>$\left[\frac{\text{No of turnover in current quarter}}{\text{No of staff beginning of current quarter}}\right] X100$ | Quarterly* |
| 6. Number of customers’ names in the freeze orders received from enforcement agency without prior STR raised | • Banking<br>• Insurance &Takaful Operators | Number of customers’ names in the freeze orders received from enforcement agency that does not match against internal list of STR raised | Quarterly* |
| 7. Number of new audit findings | • Banking<br>• Insurance &Takaful Operators | Number of new audit findings from internal and / or external auditor engaged for non-financial audits to the entity which have never been raised before. Any recurring issues across different business lines must be excluded | Quarterly* |

** ALL Reinsurers and Retakaful companies are to report these KRIs on a yearly basis.*

## 2. Technology

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 1. Number of instances of critical systems downtime exceeding Recovery Time Objective (RTO) | • Banking<br>• Insurance &Takaful Operators | Tracks specific critical system availability as outlined in **FAQ No. 61.** | Monthly |
| 2. Number of instances of critical services downtime exceeding Recovery Time Objective (RTO) | • Banking<br>• Insurance &Takaful Operators | Tracks specific critical system availability as outlined in **FAQ No. 61.** | Monthly |
| 3. Number of instances of network utilisation exceed threshold of 60% | • Banking<br>• Insurance &Takaful Operators | Tracks network bandwidth utilisation to identify potential threats to Denial of Service attack (DDoS) | Monthly |
| 4. Number of instances response time for critical services exceeded predetermined threshold / SLA | • Banking<br>• Insurance &Takaful Operators | Tracks specific critical system availability as outlined in **FAQ No. 61.**<br>More details in **FAQ No. 88.** | Monthly |
| 5. Number of hacking attempts on IT infrastructure | • Banking<br>• Insurance &Takaful Operators | The number of hacking attempt on internet facing application by external parties. | Monthly |
| 6. Number of instances storage or memory utilisation exceed maximum threshold of 70% | • Banking<br>• Insurance &Takaful Operators | Tracks specific critical system availability as outlined in **FAQ No. 61.** | Quarterly |
| 7. Numbers of batch overrun incidents | • Banking<br>• Insurance &Takaful Operators | Tracks specific critical system availability as outlined in **FAQ No. 61.** | Quarterly |
| 8. Number of instances of failed Disaster Recovery Plan (DRP) tests for critical systems | • Banking<br>• Insurance &Takaful Operators | To ascertain the reliability of the DRP and readiness of the FI in the event of a system failure | Yearly |

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 9. Number of DRP tests planned but not conducted for the year | • Banking<br>• Insurance &Takaful Operators | To ascertain the reliability of the DRP and FI readiness in the event of a system failure | Yearly |
| 10. Number of scheduled core system maintenance not conducted | • Banking<br>• Insurance &Takaful Operators | To ascertain system integrity | Yearly |
| 11. Number of incidents relating to loss of confidential data | • Banking<br>• Insurance &Takaful Operators | To ascertain any breaches of preservation of data confidentiality in accordance to the FSA, IFSA and Personal Data Protection Act | Yearly |
| 12. Number of incident relating to transactional reporting or updating errors of critical system | • Banking<br>• Insurance &Takaful Operators | The transactional reporting error refers to a material error in the financial figure or other information in public reports / documents or reports / documents released to the customers or BNM<br>The transactional updating error refers to the error in the financial or customer information database. Refer to **FAQ No. 86.** | Yearly |

## 3. Complaints

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 1. Number of new complaints on Sales and Marketing | • Banking<br>• Insurance &Takaful Operators** | Complaints on sales representatives' unethical behaviour such as harassing or coercing; or acting in a manner with the intention to misrepresent or mislead customers (e.g. force selling of products, mis-selling of financial products, misleading advertisement / brochure, misrepresentation by staff / agent, lack of / wrongful advice / info, bundled or sold with another product) | Monthly |
| 2. Number of new complaints on Services | • Banking<br>• Insurance &Takaful Operators** | Complaints on staff or third party engaged by FIs who are involved in providing services to customers (e.g. delay / no response to customers' queries / requests / complaints, harassment of customers by staff / debt collector, delay in processing, delay in disbursement, unprofessional conduct / behaviour, wrongful advice / info) | Monthly |
| 3. Number of new complaints on Operations | • Banking<br>• Insurance &Takaful Operators** | Complaints on inefficiency of the internal process, system, control and procedure to ensure fair and equitable business practices (e.g. delay in clearing of cheques, wrongly cleared / debited of cheques, card retained by ATM, incorrect recording of dispensed amount in e-channel, system offline, freezing / opening / closing of accounts / credit facilities, revised credit limit, dispute in agreement / document, discharge of guarantor, loss of documents, going after guarantor) | Monthly |

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 4. Number of new complaints on Products | • Banking<br>• Insurance &Takaful Operators** | Complaints on products offered not meeting the needs and financial affordability of customers (e.g. different term offered than applied for, unfair term and condition) | Monthly |
| 5. Number of new complaints on Fees & Charges | • Banking<br>• Insurance &Takaful Operators** | Complaints on terms and conditions relating to fees and charges, unreasonable and unfair imposition of fees and charges to prevent customer from terminating or switching products / services to another financial service provider (e.g. request to waive / reduce penalty interest, excessive fees / charges / penalty / interest, refund of compensation, non-disclosure of fees / charges / penalty / interest, fees charged by merchant without consent) | Monthly |
| 6. Number of new complaints on Benefits & Claims | • Insurance &Takaful Operators** | Complaints on demand for payment of an amount due under a policy / refund / claim / surrender etc. (e.g. repudiation of claim, delay in claim settlement, dispute / dissatisfaction of claim settlement / surrender / maturity value, unsatisfactory repair work) | Monthly |
| 7. Number of new complaints on Underwriting | • Insurance &Takaful Operators** | Complaints on the process that an insurer uses to assess the eligibility of a customer to receive their products (e.g. refuse to insure / renew / unfair policy condition, dispute on underwriting) | Monthly |
| 8. Number of new Shariah-related complaints | • Banking<br>• Takaful Operators** | Complaints lodged by customers on potential non-compliance with Shariah requirements in product implementation, legal documentation, product brochures, transparency, etc. | Monthly |

*** ALL Reinsurers and Retakaful companies are excluded from reporting the KRIs*

## 4. Insurance and Takaful

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 1. Instances of delay in issuance of policies | • Insurance &Takaful Operators* | Number of policy issuance exceeding 30 days for Motor and 60 days for Non-motor from the acceptance of risk until issuance of policies. Refer to **FAQ No. 89.** | Monthly |
| 2. Instances of delay in registering claims | • Insurance &Takaful Operators* | Number of claim registration > 7 working days from receipt of claims notification | Monthly |
| 3. Instances of delay in payment of claims | • Insurance &Takaful Operators* | Number of delay in payment of claims > 35 working days from receipt of the last supporting document for assessment for example medical report and / or final adjuster's report until issuance of payment voucher. Refer to **FAQ No. 90.** | Monthly |
| 4. Number of replacement of life policy / certificate | • Insurance & Takaful Operators with life / family business* | Number of life policy / certificate replaced in a particular month. Refer to **FAQs No. 91 and 92.** | Monthly |
| 5. Number of occurrences of holding cover prior to facultative placement | • Insurance &Takaful Operators* | Number of risks that are not included in the treaty coverage but were accepted prior to facultative placement | Monthly |
| 6. Number of disputed and repudiated claims recovery from reinsurers and subrogation | • Insurance &Takaful Operators* | Number of:<br>• claims recovery disputed and repudiated from reinsurers<br>• claims recovery disputed and repudiated from subrogation<br>**Note: This applies to all Reinsurance arrangement which include Treaty and Facultative.* | Monthly |
| 7. Number of delay in death claims | • Insurance &Takaful Operators* | Number of death claims paid > 60 days after the notification date. Refer to **FAQ No. 93.** | Monthly |

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 8. Instances of delay in appointing licensed / in-house adjuster | • General Insurance & General Takaful Operators* | Appointment of licensed / in-house adjuster was done >7 working days from receipt of completed claims documents. Refer **FAQ to No. 94.** | Monthly |

** ALL Reinsurers and Retakaful companies are excluded from reporting the KRIs*

## 5. Treasury

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 1. Number of treasury room limit breaches (including trading positions) | • Banking | Number of treasury limit breaches on dealing / trading activities as per the approved internal policy | Monthly |
| 2. Total number of confirmation mismatches | • Banking | Number of confirmation mismatches between the bank and its counterparties | Monthly |
| 3. Number of instances off-market price transactions | • Banking | Number of deals / trades concluded not within the observable market rates and daily quoted price inclusive of private placements | Monthly |
| 4. Number of instances off-premise trading | • Banking | Number of deals / trades executed outside the treasury dealing room | Monthly |
| 5. Number of instances - failed trade reconciliation between Front Office and Back Office | • Banking | Number of unreconciled deals / trades (variance) between Front Office and Back Office, whereby the trades which were concluded by the front office but there were no corresponding confirmations obtained by the back office | Monthly |
| 6. Number of payment and settlement disputes by customers and counterparties | • Banking | Number of payment and settlement transactions disputed by customers and counterparties | Monthly |

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 7. Instances of buying and selling of the same stock / securities at the same price within the same trading day | • Banking | Number of trades which are executed on an immediate buy / sell basis, at the same price in the same stock / securities within the same day | Monthly |
| 8. Number of instances – ad hoc request to increase trading limit | • Banking | Number of specific request by dealers to increase approved trading limit, including instances when dealers share limits with other dealers | Monthly |
| 9. Number of trade / deal cancellations and amendments | • Banking | Number of trades / deals amended or cancelled by trader / dealer<br>Refer to **FAQ No. 95.** | Monthly |
| 10. Number of unconfirmed corporate trade / deals | • Banking | Number of corporate trades / deals not confirmed (not signed and returned by corporate clients) | Monthly |

## 6. Corporate Finance

| KRI | Sector | Description | Cycle |
|---|---|---|---|
| 1. Number of Qualified Senior Personnel (QSP) resignation | • Banking | To monitor minimum number of QSPs specified as a “registered persons” in third column of Part 1 of Schedule 4 in the Capital Markets and Services Act 2007 | Monthly |
| 2. Number of submissions rejected / returned by SC | • Banking | Number of submissions not meeting SC's standards | Monthly |
| 3. Breaches of the Chinese Wall policy | • Banking | Number of Chinese Wall Policy breaches occurred in the month | Monthly |