BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Operational Risk Reporting (ORR)

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
11. Approved Operators of A Payment System
12. Registered Merchant Acquirers

Issued on: 30 January 2026 BNM/RH/PD 028 -128

LIST OF TABLES

PART A: OVERVIEW

1. Introduction

1.1 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 exposures.

1.3 This policy document aims to:

(a) promote more structured operational risk reporting across all REs for the relevant types of operational risk;

(b) streamline reporting with the enhanced ORR; and

(c) promote clarity of the reporting requirements through the insertion of examples and scenarios.

1.4 This policy document sets out the requirements for the reporting of Loss Event Data and Key Risk Indicators to the Bank through the ORR system.

2. Applicability and transitional arrangement

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

3. Legal provisions

3.1 This policy document is issued pursuant to:

(a) sections 18(2), 33(1), 47(1), 49 and 143(2) of the Financial Services Act 2013 (FSA);

(b) sections 29(2), 43(1), 57(1) and 155(2) of the Islamic Financial Services Act 2013 (IFSA); and

(c) sections 33E(2) and 41(1) of the Development Financial Institutions Act 2002 (DFIA) and constitutes a notice under section 116(1) of the 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 The policy document comes into effect on 30 January 2026.

5. Interpretation

5.1 The terms and expressions used in this policy document 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;

"BCM" refers to an enterprise-wide framework that encapsulates policies, processes and practices that ensure the continuous functioning of a Reporting Entity (RE) during an event of disruption. It also prepares the RE to resume and restore its operations and services in a timely manner during an event of disruption, thus minimising any material impact to the RE;

"banking institution" or "BI" means-

(a) a licensed bank under the FSA;

(b) a licensed investment bank under the FSA;

(c) a licensed Islamic bank which includes a licensed international Islamic bank under the IFSA; and

(d) a prescribed institution under the DFIA;

"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 it from time to time**;**

"CRO" means the Chief Risk Officer of a RE;

"e-money issuer" means a person, including a banking institution, approved under section 11 of the FSA or section 11 of the IFSA to issue electronic money;

"financial group" refers to a financial holding company approved by the Bank or a financial institution/ RE, and a group of related corporations under such financial holding company or financial institution/ RE 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 institution/ RE;

"financial institution" or **"FI"** means-

(a) a licensed bank under the FSA;

(b) a licensed investment bank under the FSA;

(c) a licensed insurer under the FSA;

(d) a licensed Islamic bank which includes a licensed international Islamic bank under the IFSA;

(e) a licensed takaful operator which includes a licensed international takaful operator under the IFSA; and

(f) a prescribed institution under the DFIA;

"GCRO" means the Group Chief Risk Officer of a RE;

"ITO" means licensed insurers and takaful operators;

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

"Loss Event Data" or **"LED"** refers to information required for assessing an RE'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;

"officer within the control function" or "OWCF" means an officer that meets the following criteria:

(a) is independent from the business lines and is not involved in revenue generation activities; and

(b) possesses sound understanding of relevant Shariah requirements applicable to Islamic financial business;

"Operational Risk[1]" or **"OR"** has the same meaning assigned to it under the Policy Document on Operational Risk issued by the Bank on 10 May 2016[2] and includes any amendments made to it from time to time.;

"**ORR**" system refers to the Operational Risk Reporting (formerly known as ORION – Operational Risk Integrated Online Network);

"payment instrument issuer" or **"PII"** means an approved issuer of a designated payment instrument or approved issuer of an Islamic designated payment instrument, consisting of a debit card, debit card-i, credit card, credit card-i, charge card, charge card-i and electronic money, under section 11 of the FSA or section 11 of the IFSA;

"payment system operator" or **"PSO"** means an approved operator of a payment system under section 11 of the FSA or section 11 of the IFSA;

---

[1] 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, cyber-attack, technology failures, transaction failures, legal and regulatory breaches as well as employee health and safety hazards. Operational risk may result in direct financial losses as well as indirect financial losses (*e.g.* loss of business and market share) due to reputational damage

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

"**registered merchant acquirer**" or **"MA"** refers to a person who is a registered person pursuant to sections 17(1) and 18(1) of the FSA to provide merchant acquiring services;

"Reporting Entity" or **"RE"** refers to –
(a) a financial institution;
(b) a payment instrument issuer;
(c) a registered merchant acquirer; and
(d) a payment systems operator;

"Reporting Entity's Administrator" or **"RE Admin"** refers to the staff in REs who are-

(a) the person in charge of the RE's user access management of the SOs; and

(b) the authorised 'checkers' whose responsibility is to verify and approve reportable OR events, KRIs created by Submission Officers and KRIs in ORR before the final submission to the Bank;

"Scenario Analysis" or **"SA"** refers to an assessment made by an RE 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;

"Shariah Non-Compliance risk" or **"SNC risk"** refers to the risk of legal or regulatory sanctions, financial loss or non-financial implications including reputational damage, which an IFI may suffer arising from failure to comply with the rulings of the Shariah Advisory Council of Bank Negara Malaysia (SAC), standards on Shariah matters issued by the Bank pursuant to section 29(1) of the IFSA and section 33E(1) of the DFIA, or decisions or advice of the Shariah committee;

"Submission Officer" or **"SO"** refers to the staff in REs authorised to submit reportable OR events and KRIs in the ORR system to the Bank, where such submissions have been verified and approved by the RE Admin.

6. Policy document superseded

6.1 This policy document supersedes the Operational Risk Reporting (ORR) policy document issued on 10 April 2025.

7. Related legal instruments and policy documents

7.1 This policy document must be read together with other relevant legal instruments and policy documents that have been issued by the Bank, as amended from time to time, 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 14 February 2024 for DFIA;

(d) Shariah Governance issued on 20 September 2019;

(e) Risk Management in Technology (RMiT) issued on 28 November 2025;

(f) Management of Customer Information and Permitted Disclosures issued on 31 October 2025;

(g) Business Continuity Management (BCM) Policy Document issued on 19 December 2022;

(h) Part C of Quality and Integrity Currency issued on 12 September 2023;

(i) Merchant Acquiring Services issued on 15 September 2021;

(j) Electronic Money (E-Money) issued on 31 January 2025;

(k) Debit Card/Debit Card-i issued on 19 December 2025;

(l) Credit Card/Credit Card-i issued on 19 December 2025;

(m) Charge Card/Charge Card-i issued on 19 December 2025;

(n) Guidelines on Dye-Stained Currency Notes issued on 26 August 2020;

(o) Reporting Requirements on Statistical Report of Complaints Statistics issued on 31 October 2019; and

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

(q) Payment System Operator issued on 22 December 2022

(r) Risk Governance issued on 1 March 2013

(s) BNM/RH/GL 004/17 Guidelines on Claims Settlement Practices - Consolidated issued on 1 April 2008

(t) BNM/RH/GL 003/09 Guideline on Claim Settlement Practices- Consolidated issued on 5 October 2006

(u) ORR Frequently Asked Questions (FAQ) document

8. Enquiries and correspondence

8.1 All enquiries and correspondences relating to this policy document must be addressed to:

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

PART B: POLICY REQUIREMENTS

9. Overview of the responsibilities of REs

S 9.1 REs must prepare and submit data and information on LED, KRIs and SA to the Bank through ORR system in accordance with the requirements specified under paragraph 13 of this policy document.

S 9.2 REs must ensure that the data and information are consolidated and centralised at the entity level prior to submitting the information to the Bank.

S 9.3 REs must establish appropriate internal governance and processes to ensure completeness, accuracy and timeliness of the data and information submitted 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.

10. Roles and responsibilities of ORR users

GCRO and CRO

S 10.1 The GCRO and CRO, or any other officer authorised by the RE to act in the capacity of the GCRO or CRO, are required to ensure the RE's compliance with the reporting requirements set out in this policy document.

S 10.2 The GCRO or CRO must-

(a) appoint up to 2 RE Admin(s) and up to 10 SOs to perform the functions set out in paragraphs 10.3 and 10.4; and

(b) ensure that the reporting requirements in paragraphs 10.3 and 10.4 are complied with at all times, in the absence of the RE Admin(s) and SOs.

RE Admin(s)

S 10.3 The RE Admins[3] must-

(a) ensure the reporting requirements in this policy document are complied with at all times and that the RE's submissions are in accordance with such reporting requirements;

(b) assign the SOs to perform the functions set out in paragraph 10.4;

(c) verify that the data and information to be submitted to the Bank is accurate, complete and has been consolidated at the entity level and reconciled with internal reports and databases, and approve such data and information to be submitted to the Bank;

(d) liaise with the Bank on matters pertaining to the data and information to be submitted or generally on the ORR system; and

---

[3] The approved RE Admin(s) will be responsible for two roles in the ORR system, as follows:
(a) to manage the SO's user access management; and
(b) specifically in respect of RE Submission Approvers, to verify and approve the submissions made by SOs before the official submission in the ORR system for REs under a single entity structure or a Financial group structure.

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

Submission Officer(s)

S 5.1 10.4 The SO must-

(a) prepare the data and information to the Bank through the ORR system; and

(b) perform corrections, amendments and provide updates on the submitted data and information via the ORR system, upon having knowledge of any inaccuracy in the submission.

11. Access to ORR

Financial group structure

G 11.1 In the case of REs operating as financial groups, access to the ORR system will be granted by the Bank to the GCRO, CRO, RE Admins and SOs via KijangNet once the REs have completed the self-registration process.

Single entity structure

G 11.2 In the case of REs operating on a stand-alone basis, access to the ORR system will be granted by the Bank to the CRO, RE Admins and SOs via KijangNet once the REs have completed the self-registration process.

12. Registration of ORR users

ORR user self-registration

S 12.1 REs must perform the self-registration process for their respective GCRO, CRO, RE Admins and SOs via KijangNet at https://kijangnet.bnm.gov.my/ .

Changes in GCRO, CRO, RE Admins and SOs

S 12.2 REs must register and update the changes to the GCRO, CRO, RE Admins or SOs in the ORR system within 1 working day from the official change in the role.

S 12.3 REs must ensure that any changes to the GCRO, CRO, RE Admins or SOs will not impact the timeliness of data and information submission to the Bank.

PART C: REPORTING REQUIREMENTS

13. ORR reporting requirements

S 13.1 REs must submit information to the Bank through the ORR system in accordance with **Table 1: ORR reporting requirements**.

Table 1: ORR reporting requirements

Appendices	Description	Applicability
Appendix 1	ORR user guide and technical specifications	REs
Appendix 2	Operational risk event reporting requirements	REs
Appendix 3	Cyber incident and cyber event reporting requirements	REs
Appendix 4	Critical BDSF event reporting requirements	REs
Appendix 5	Customer information breaches reporting requirements	REs
Appendix 6	SNC event reporting requirements	FIs and e-money issuers
Appendix 7	Payment-related fraud event reporting requirements	Banking institutions and PIIs
Appendix 8	Counterfeit notes and coins event reporting requirements	BIs
Appendix 9	Insurance-related event reporting requirements	ITOs
Appendix 10	Reporting requirements for all other reportable operational risk events	
	Aggregate reporting ≤ RM1,000 for: 1. Non-payment fraud 2. Non fraud	REs
	3. Physical cash shortage • Due to execution error	FIs

Appendices	Description	Applicability
	• Due to penalties on currency shortages / excess	BIs
	Individual reporting for: 1. Physical robbery > RM200k	FIs
	2. Self-Service Terminals (SST) robbery	BIs
	3. Non-payment fraud event > RM1,000 4. Fraud with new modus operandi (MO) excluding payment fraud, physical and SST robbery and cyber event 5. Non-fraud event > RM 1,000 6. Actual operational risk event with no financial loss	REs
Appendix 11	Boundary event reporting requirements	BIs
Appendix 12	Overseas loss event reporting requirements	FIs
Appendix 13	Business lines taxonomy	REs
Appendix 14	Event types taxonomy	REs
Appendix 15	Causal categories taxonomy	REs
Appendix 16	Key risk indicators taxonomy	REs
Appendix 17	Key risk indicators reporting details	REs

14. Scope of reporting

S 14.1 REs must report all operational risk events in accordance with the requirements and timelines set out in **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines**. 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 14.2 REs must 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.[4]

S 14.3 For reporting of the operational risk events of foreign and offshore subsidiaries or branches of the REs, REs must ensure compliance with the requirements of this policy document. Where there are challenges to comply with such requirements, REs must notify the Bank of such challenges in writing to seek a waiver from the Bank. For the avoidance of doubt, the Bank reserves its right in deciding whether the waiver is to be granted.

15. Reporting currency

S 15.1 All amounts must be reported by REs in Ringgit Malaysia (RM). 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.

16. Classification and quantification

Reportable operational risk event classification

S 16.1 REs must classify the reportable operational risk events in accordance with the following:

(a) **Actual Event** –refers to the operational risk event that impacted the REs with a financial and / or non-financial impact. This event may result in an actual loss or potential loss which will be concluded with an actual loss on a later date;

(b) **Potential Event –**refers to a possible operational risk event yet to be confirmed by the RE's internal governance. A Potential event has the tendency to be re-classified as Actual or Near Miss event upon completion of investigation; and

(c) **Near Miss Event** –refers to an event for which actual operational risk did not materialise due to the timely use of controls or mitigating actions implemented by the REs.

[4] For avoidance of doubt, REs that are onboarded at later dates are required to report LED and KRI modules for events that occurred from the date of onboarding onwards.

Reportable operational risk event reference dates

S 16.2 Apart from information on operational risk event types and loss classifications, REs must collect information about the reference dates of the operational risk event, in accordance with the following sequence:

(a) **Date of occurrence** – the date when the event happened or took place;

(b) **Date of detection –** the date on which the RE discovered the event;

(c) **Date of confirmation** – the date on which the RE has verified or confirmed the operational risk event;

(d) **Date of loss event captured in Profit & Loss (P&L) account** – the date when the operational risk loss is recognised based on the RE's accounting framework; and

(e) **Date of loss event captured in Provision account** – The earliest date when the operational risk loss has been accrued in suspense, reserve or provision of the RE's account.

Financial impact related operational risk event

S 16.3 REs must classify the financial impact in accordance with the following**:**

(a) **Actual Loss –**refers to a definitive loss amount in accordance with the RE's accounting framework.

- **Gross Actual Loss** – refers to actual loss that occurs before any form of recovery.
- **Net Actual Loss –** refers to actual loss after taking into account the impact of recoveries;

(b) **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 the RE's accounting framework; and

(c) **Recovery –**refers to a separate event from the original loss event, occurring at a different period, in which monies or inflows of economic advantages are received from a third party such as reimbursements received from insurers, repayments received from perpetrators of fraud, and recoveries of erroneous transfers. REs must distinguish the loss from the insurance and non-insurance recovery amount for the reportable operational risk event.

S 16.4 Indirect Financial Loss which resulted from an Operational Risk event must not be included by REs in the calculation of the actual and potential loss amount reported in ORR system.

S 16.5 Where a provision is made for the measurable loss of an on-going event, the amount must be classified by the REs as 'Actual Loss' or 'Potential Loss' in the ORR system based on the RE's accounting framework. The loss amount must be adjusted by the REs if the amount for the provision is subsequently changed.

Non-financial operational risk event

G 16.6 Non-financial operational risk events are events that are not defined in paragraph 16.2, and the non-financial impact ratings of "high", "medium" and "low" may be used to consider the following non-financial risks, which are non-exhaustive in nature:

(a) Reputational risks;

(b) Regulatory and legal risks;

(c) Compliance and conduct risk;

(d) Systemic risks;

(e) Cyber and IT risks; and

(f) Business continuity risks.

S 16.7 REs must determine the non-financial impact based on their internal policies (e.g. Reputational risk framework etc.) by considering the nature of the event, size of REs, nature of business and complexity of the respective entities.

G 16.8 REs may refer to Appendix 10, paragraph 16 for examples of Operational Risk events with no financial impact.

S 16.9 REs must report the following operational risk information as tabulated in **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines.** For an operational risk reporting that coincides with requirements in both **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines**, REs must adhere to the **earliest stipulated deadline**.

Table 2: Operational risk information reporting deadlines

Operational risk information	Event Classification	Deadline
Reputational Impact Event with 'High' impact as defined by REs internal policy	• Actual	By T+1 working day, T being the date of event confirmation
All reportable operational risk events ≥ RM 1mil losses	• Actual event with financial loss • Potential event with financial loss	By T+2 working days, T being the date of event confirmation
New modus operandi (MO) New fraud MO committed and impacted the REs for the first time must be reported **as an individual event**	• Actual • Potential • Near Miss	

S 16.10 **Table 3: ORR LED reporting types and deadlines** below is the key summary of the reportable operational risk events, event classifications and the respective reporting deadlines. REs must read **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines** together to determine the reporting deadline and the reportable operational risk details. REs must refer to the appendices of each respective reporting requirement stipulated in **Table 1: ORR reporting requirements** for further reporting information.

S 16.11 REs must report LEDs to the Bank according to the earliest deadline stipulated in **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines**, using LED forms that correspond to **Table 3: ORR LED reporting types and deadlines** reportable operational risk event upon selection of its respective Level 1, Level 2 and Level 3.

Table 3: ORR LED reporting types and deadlines

Reportable operational risk events			Event Classification	Deadline
Level 1	**Level 2**	**Level 3**		
Critical event	Robbery and Theft	SST[5] robbery	● Actual ● Near Miss	By T+1 working day, T being the date of event confirmation
		Physical Robbery ≥ RM 200k		
	Technology related	Cyber Incident / Event	● Actual ● Near Miss	By T+14 calendar days, T being the date of event confirmation
		Critical BDSF	● Actual	
		Critical BDSF - For counterfeit notes / coins accepted via SST		
	Customer information breaches		● Actual	By T+1 working day, T being the date of investigation is tabled to the Board
Shariah -related matter	Detection		● Potential	By T+1 working day, T being the date of event confirmation by an officer within the control function
	Confirmation		● Actual	By T+1 working day, T being the date of SNC confirmation by Shariah Committee (SC)
	Rectification		● Actual	By T+ 30 calendar days, T being the date of SNC confirmation by

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

Reportable operational risk events			Event Classification	Deadline
Level 1	**Level 2**	**Level 3**		
				Shariah Committee (SC)
Fraud Event	Payment related fraud	Payment Instrument	● Actual ● Near Miss	By the 15th calendar day of the following month from the date of detection of the event
		Payment Channel		
		Unauthorised cash withdrawal		
		Aggregate card fraud with amount ≤ RM5K	● Actual	
		Aggregate Mobile payment fraud ≤ RM5K		
	Non-payment related fraud event	Physical Robbery < RM200k	● Actual ● Near Miss	
		Individual event	● Actual ● Potential ● Near Miss	
		Aggregate Actual Loss Event ≤ RM1,000	● Actual event with actual loss	
Other loss event	Other than fraud events	Other Aggregate Actual Loss - Event ≤ RM1,000	● Actual event with actual loss	
	Aggregate physical cash shortages	Due to execution errors	● Actual	
		Due to penalties on currency shortages / excess	● Actual	

Reportable operational risk events			Event Classification	Deadline
Level 1	**Level 2**	**Level 3**		
		Due to counterfeit notes / coins discovered through over-the-counter and by outsourced service providers	● Actual	
	All other actual individual event	Event with financial losses > RM1,000	● Actual event with **actual** loss	
		Event with no financial losses	● Actual event with **medium** or **high** non-financial impact level	
Overse as loss events	Individual event ≥ RM1 million		● Actual event with **actual** loss	
	Aggregate by country < RM1 million			

17. Additional reporting requirements

S 17.1 All submissions to the ORR system by REs must not contain any customer information or employee data in line with the relevant data secrecy and privacy requirements, unless the submissions are for the purpose of reporting breaches involving customer information, as stipulated in **Appendix 5**.

S 17.2 All on-going Operational Risk events must be re-assessed and updated by REs to reflect any changes to event classifications and latest information.

S 17.3 Notwithstanding the timeline for reporting critical events as stated in **Table 3: ORR LED reporting types and deadlines**, the REs must notify the Bank of the occurrence of critical events through other communication channels at the earliest opportunity, upon the detection of the event.

S 17.4 REs must notify the Bank via oprisku@bnm.gov.my of any late submission and reason(s) for the delay, and such notification would not constitute a waiver of the reporting requirements or an extension to the reporting timelines, by the Bank.

S 17.5 For an event which causes or involves multiple different reportable operational risk events in the ORR system, REs must report each event as separate reportable operational risk events according to **Table 3: ORR LED reporting types and deadlines**. The OR events must be reported separately as follows:

Scenario A: Hacking on internet banking database system that causes customers' data leakage.

(i) Event 1 (for hacking) –
Event Types: External Fraud > Systems Security > Hacking Damage.

(ii) Event 2 (for customers' data leakage) –
Event Types: Clients, products, and business practices (CPBP) > Fiduciary > Breach of Privacy.

Event 1 must be linked using the **'Submission ID Link'** function available in the ORR system to link the event with Event 2.

G 17.6 Additional examples of separate reporting of different event types related to the same loss event are provided below:

Scenario A: Attempted robbery with no cash loss (no cash stolen from the Self-Service Terminals as the robbery was unsuccessful but there was some loss due to damage).

(i) Event 1 (for robbery event)

- **Loss Event Name:** Attempted Self-Service Terminals robbery.
- **Event Types:** External fraud > Theft and fraud > Theft/robbery.
- **Loss Event Classification:** Near Miss.

(ii) Event 2 (for repair work if the loss has been charged to P&L)

- **Loss Event Name:** Attempted Self-Service Terminals robbery repair cost.
- **Event Types:** Damage to physical assets > Natural disaster & other losses > Vandalism.
- **Loss Event Classification:** Actual Event with actual loss

Scenario B: Successful robbery with cash loss (stolen cash from the Self-Service Terminal with loss due to damage)

(i) Event 1 (for robbery event)

- **Loss Event Name:** Self-Service Terminal (SST) robbery.
- **Event Types:** External fraud > Theft and fraud > Theft/robbery.
- **Loss Event Classification:** Potential Loss (if the loss has yet to be charged to P&L) or Actual Loss (if the loss has been charged to P&L).

(ii) Event 2 (for repair work if the loss has been charged to P&L)

- **Loss Event Name:** Attempted ATM/CDM robbery repair cost.
- **Event Types:** Damage to physical assets > Natural disaster & other losses > Vandalism.
- **Loss Event Classification:** Actual Event.

REs must use the **'Submission ID Link'** to link the events involved or impacted due to the operational risk in ORR system.

S 17.7 The event types, business lines and causal categories must be mapped to the closest ORR taxonomies. This includes the following circumstances:

(a) The existing taxonomies in the REs are not as granular;

(b) The event that occurred impacted several business lines / branches. In this case REs must establish a principle of allocating the loss, e.g. to the highest impacted business activity such as "deposit" hence the loss would be allocated to commercial banking; and

(c) The use of "Others" must be done after REs have tried to exhaust all possible options in the taxonomies. If it is genuinely new e.g. new MO for fraud, the Bank must be **immediately notified**.

G 17.8 REs may provide a concise description of the MO to clarify the cause of the reported OR event.

Table 4: Examples of Modus Operandi

Examples of Modus Operandi in ORR PD	
Fat finger error	Intentional disclosure of confidential information
Rogue trading	Documents containing customer information compromised but not "read" by a 3rd party
Lack of transparency or conflict of interest	Documents containing customer information compromised and read by a 3rd party
Market manipulation	Insider trading
Ghost employee scheme	Third-party/customer collusion
Management incompetence	Accounting error
Creative accounting	Spoofing
Mis-selling of products	Documentation forgery
Phishing	Vandalism
Model bias	Distributed Denial of Service (DdoS)
Zero-day exploit	Supply chain attack

S 17.9 For Nature of Event and Sub Nature of Event, the timeframe to be classified as 'New' event or 'New' MO must be compared to the last three years of historical operational risk events reported in ORR. Where there is re-occurrence of similar events or MO beyond the last three years, the event or MO shall be classified as 'New'. All operational risk events or MO that is classified as 'New' shall be reported in ORR based on suitable Reportable Operational Risk event in **Table 3: ORR LED reporting types and deadlines**.

18. Key risk indicators (KRIs)

S 18.1 REs must submit information on the KRIs according to the applicability, description and frequency set out in **Appendix 16 – Key risk indicators Taxonomy.**

G 18.2 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 18.3 REs must report the KRIs to the Bank within the timeline specified in **Table 5** below.

Table 5: Timeline for KRI reporting to ORR

KRI frequency	Reporting deadline
Monthly	By the 15th calendar day of the following month
Quarterly	By the 15th of April, July, October and January
Semi-annually	• By the 28th of July and January for Complaint KRIs • By the 15th of July and January, for other KRIs
Annually	By the 15th of January of the following year

APPENDICES

APPENDIX 1 ORR user guide and technical specifications

1. Please refer to the attached appendices for the ORR technical specification and ORR User Guide document, as follows:

   (a) Appendix A – ORR User Guide Document;

   (b) Appendix B – ORR Technical Specifications Document; and

   (c) Appendix C – ORR Bulk Submission Technical Specifications Document.

APPENDIX 2 Operational risk event reporting requirements

ORR data fields requirements

1. REs must report the following information for each operational risk event as guided in Table 6. Additional data fields for the reportable operational risk events are provided in Appendix 3 to Appendix 12 respectively.

Table 6: Data fields for operational risk event reporting

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as one of the following: • New • Work In Progress (WIP) • Completed • Reclassified • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values.

Data fields	Mandatory field	Description
		3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Reclassified**' for potential SNC event that are reclassified to non-SNC during the confirmation stage to become '**WIP**' until all mandatory fields are filled. 8. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	Reportable operational risk events must be reported based on the "Level 1" to "Level 3" in **Table 3: ORR LED reporting types and deadlines.**
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event must be stated.
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function.

Data fields	Mandatory field	Description
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • Actual Event; • Potential Event; or • Near Miss Event *Please refer to paragraph 16.1 for the definitions of the above-mentioned categories.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes a **high** reputational impact based on the RE's internal framework.
Boundary Event	No	REs must categorise the reportable operational risk event as being related to either Credit risk, Market risk or Not Applicable with reference to **Appendix 11**. Note: This is applicable to BIs only.
Islamic Business?	Yes	REs must select '**Yes**' for an event that involves Islamic products or services, which may or may not be related to shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC.
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss; • **Non-financial impact** – No loss amount involved but there is an impact on reputation, non-compliance etc; or

Data fields	Mandatory field	Description
		• **Both financial and non-financial** – There is actual / potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	Res must select one of the following for reportable operational risk event with Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for reportable operational risk event with Non-Financial Impact: • Low; • Medium; or • High *Note: the non-financial impact is not confined to reputation risk, but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7.*
Non-Financial Impact Justification	Yes	REs must justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks.
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13.** *Please refer to the specific appendix that is related to the reportable OR for the specific selection, if any.*
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Delivery Channel	Yes	Channels used to deliver the product / services of the operational risk events. **For REs <u>except</u> ITOs:** • Internet • Mobile

Data fields	Mandatory field	Description
		• Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A **For ITOs only:** • Direct Clients – Walk In • Direct Clients – Internet • Direct Clients – Direct Mailing • Direct Clients – Marketing Staff • Direct Clients – Others • Telemarketing • Franchise Holders / Dealers (for GITOs only) • Registered Individual Agents • Registered Corporate Agents • E-Commerce Marketplace • Partners in Digital Platforms • Financial Advisers • Bancassurance / Bancatakaful • Co-Insurer / Co-Takaful • Insurance / Takaful Brokers • Reinsurance / Retakaful Accepted • Others (please specify)
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event. *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any.*
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15**.
Date of Event Occurrence	Yes	The date on which the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*

Data fields	Mandatory field	Description
Date of Event Detection	Yes	The date on which the REs became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Loss Event Captured in Provision Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date on which the operational risk loss is recognised based on the accounting framework of the REs. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction values associated with the reportable operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss Incurred By	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields.

Data fields	Mandatory field	Description
		Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'.
Loss Event Description		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • On-pemise – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre. • Off-premise – occurs outside premise(s) of REs: To describe the speific places i.e. outsourced service provider, legal firm, customer premise, remote working. **b) <u>For ITOs only</u>** • On premise: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service ➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance

Data fields	Mandatory field	Description
		➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • Off-premise: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster.
Number of Business Lines Affected	Yes	To provide the number of affected business lines: • **For banking**: by Business Line Level 1 • **For ITOs**: by Business Line Level 2 • **For PIIs and PSOs**: by Business Line Level 3 • **For Payments Network Malaysia Sdn. Bhd.**: by Business Line Level 2
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia.

Data fields	Mandatory field	Description
		• **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.
How the Event Occurred?	Yes	1. General operational risk event: An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g., Name, I/C number and other personal information. 2. Aggregate operational risk event: For further description and reporting format on aggregate reporting, please refer to the relevant appendices.
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years.
Sub Nature of Event	No	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years. *Note: **All** **External** and **Internal Fraud** **LED** events must be classified as either new or repeated MO.*

Data fields	Mandatory field	Description
Modus Operandi Involved	Yes	REs must concisely define the method or manner of the reportable operational risk event occurrence. The MO involved in the LED is not limited to fraud MO. *Please refer to paragraph 17.8 for examples.*
Parties Involved In / Affected By The Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved /affected • Staff • Third party service provider • Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number Of Individual(s) Involved In / Affected by the Event	Yes	Based on the '**Parties involved in / affected by the event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided and at minimum, must include the underlying cause of the event.
Number of Transactions	Yes	To specify total number of transactions impacted due to the reportable operational risk events. Examples of reportable total number of transactions impacted: • Internet banking transactions, mobile banking transactions, SST transactions etc. • Number of impacted insurance policies.

Data fields	Mandatory field	Description
		• E-money transactions, card transactions, etc. REs must also specify the number of transactions impacted for each critical system category and must avoid duplication for overall total of transactions for an event that encounters more than one critical system. REs may report "0" for events which do not involve any transactions.
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event. REs may select 'TBC' [To Be Confirmed] for remedial action plans that are not finalised during the initial reporting.
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs must select 'TBC'. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided.
Remedial Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

Data fields	Mandatory field	Description
Mitigation Action Plan(s)	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.
Mitigation Action Plan(s) Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

APPENDIX 3 Cyber incident and event reporting requirements

1. Cyber is defined as anything 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 cybersecurity. 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. Cybersecurity 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 7: Types of cyber incident and cyber event

Types	Description	Example
Data breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed.	• Customer Personally Identifiable Information (PII) data advertised on leak site. • Sample template, test manual, or files containing genuine customer PII data wrongly uploaded on production server. • Cloud misconfiguration unknowingly disclosing customer PII data.
Distributed Denial of Service (DDoS)	Distributed Denial of Service is an attack that results in 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 • Application attack
Hacking	Hacking is an unauthorised intrusion into a computer or a network.	• N/A

Types	Description	Example
Insider threat	A trusted entity with potential to use their access or knowledge to adversely affect an organisation's assets.	• Disgruntled staff
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 • Bots • Bugs • Rootkits • Spyware
Phishing	A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication	• Spear-phishing • Whale-phishing
Ransomware	Malware that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied.	• CryptoLocker
Supply chain attack	Attackers infiltrate the systems or networks through a compromised third-party software, service provider or partner that is trusted and legitimate.	• Open-source supply chain attack
Web defacement	Website defacement is an attack on a website that changes the visual appearance of the website or a webpage.	N/A
Zero-day exploit	An exploit targeting a system, network or software by leveraging a previously unknown vulnerability or undisclosed vulnerability.	• Software vulnerabilities

Cyber incident and event reporting types

4. REs must report **all** cyber incidents and events that occurred as stipulated below to the ORR system in accordance with the requirements set out in **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines** within **14 calendar days** upon the event confirmation:

   (a) Cyber incident

   Defined as a cyber event that adversely affects the cybersecurity of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not.

   (b) Cyber event

   Defined as any observable occurrence in an information system. Cyber 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. The reportable cyber incident and event includes:

   (a) any cyber incident occurred within REs' network, infrastructure or environment;

   (b) any 'High' or 'Critical' severity cyber event occurred within REs' network, infrastructure or environment; and

   (c) any cyber incident occurred within third-party service providers' network, infrastructure or environment that has impact to REs' operations.

6. Non-high or non-critical severity cyber event such as external probing, scanning, phishing emails and isolated malware detected and blocked within REs' internal and external environment are only reportable under the KRI reporting i.e. number of hacking attempts on IT infrastructure.

7. Examples of reportable cyber incidents

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

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

   (b) DDoS attack on RE's network that caused network downtime

   - **Loss Event Classification:** Actual Event
   - **Event type**: BDSF **>>** System **>>** Security breach – Distributed Denial of Service; or

   (c) Ransomware that has affected RE's third-party service provider that caused system or operational disruption to the RE.

   - **Loss Event classification:** Actual Event

- **Event type:** BDSF >> System >> Security breach – virus / malware infection.

8. Examples of reportable cyber events

(a) Malware infection and Command & Control (C&C) communication attempts detected and blocked on critical systems, where there was no impact to RE's systems and operations.

- **Loss Event classification:** Near Miss
- **Event type:** BDSF >> System >> Security breach – virus / malware infection

(b) Senior officer received a highly targeted spear phishing email that managed to bypass and avoid detection from email protection system on their corporate email account, however the malicious phishing link was not clicked and had no impact to RE's data and operations.

- **Loss Event classification**: Near Miss
- **Event type**: External Fraud >> System Security >> Social engineering targeting institution

(c) Malware or malicious files attributed to high profile threat actor successfully detected and quarantined in one of the production servers with no further compromise detected and no system downtime.

- **Loss Event classification:** Near Miss
- **Event type:** BDSF >> System >> Security breach – virus / malware infection

9. In addition to the reporting requirements for cyber incidents and cyber events outlined in paragraphs 5 to 7 above, REs that are subject to the Business Continuity Management Policy Document (BCM PD) are required to notify the Bank on the occurrence of a cyber incident within 2 hours upon the confirmation of such cyber incident. The notification must be submitted using the Cyber Incident Scoring System (CISS) form, via the designated centralised email, mylod@bnm.gov.my.

10. Cyber incident and cyber event

Category: Cyber incident and cyber event

Loss Event Classification: Actual Event or Near Miss

Applicability: All REs

Table 8: Data fields for reporting cyber incidents

Data fields	Mandatory field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as one of the following: • New • Work In Progress (WIP) • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the

Data fields	Mandatory field	Description
		event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	Reportable operational risk events must be reported based on the "Level 1" to "Level 3" in **Table 3: ORR LED reporting types and deadlines** REs must report the cyber event ONLY under the following selection: • **Level 1:** Critical Event • **Level 2:** Technology Related • **Level 3:** Cyber Incident / Event
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event must be stated
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • **Actual Event** – Any cyber incident that has been detected and had impact to services, systems, or data; or • **Near Miss Event** – Any 'High' or 'Critical' severity cyber event that has been detected and blocked by the existing controls resulted in no impact to services, systems or data. *Please refer to paragraph 16.1 for the definitions of the above-mentioned categories.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes a **high** reputational impact based on the

Data fields	Mandatory field	Description
		RE's internal framework
Islamic Business?	Yes	REs must select 'Yes' for an event that involves Islamic products or services, which may or may not be related to shariah related matters Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss; • **Non-financial impact** – No loss amount involved but there is an impact on reputation, non-compliance etc; or • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	Res must select one of the following for reportable operational risk event with Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for reportable operational risk event with Non-Financial Impact: • Low; • Medium; or • High *Note: the non-financial impact is not confined to reputation risk, but includes*

Data fields	Mandatory field	Description
		legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7
Non-Financial Impact Justification	Yes	REs must justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13**
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Delivery Channel	Yes	Channels used to deliver the product / services of the operational risk events. **For REs <u>except</u> ITOs:** • Internet • Mobile • Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A **For ITOs only:** • Direct Clients – Walk In • Direct Clients – Internet • Direct Clients – Direct Mailing • Direct Clients – Marketing Staff • Direct Clients – Others • Telemarketing • Franchise Holders / Dealers (for GITOs only) • Registered Individual Agents • Registered Corporate Agents • E-Commerce Marketplace • Partners in Digital Platforms • Financial Advisers • Bancassurance / Bancatakaful • Co-Insurer / Co-Takaful • Insurance / Takaful Brokers • Reinsurance / Retakaful Accepted • Others (please specify)

Data fields	Mandatory field	Description
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event. For cyber incident and cyber event reporting, REs must categorise the event using ONLY the following selection of event types: **OPTION 1** Level 1: Internal Fraud Level 2: Unauthorised Activity Level 3: Select one: • unauthorised changes to programmes, data, or transactions; • hacking / cracking; • misuse of system access (e.g., Power system ID); or • computer virus / malware injection **OPTION 2** Level 1: External Fraud Level 2: System Security Level 3: Select one: • hacking / cracking damage; • theft of information; • unauthorised changes to programs or data by external parties; • misuse of system access by external parties; • sabotage by external parties; or • social engineering targeting institution **OPTION 3** Level 1: Business Disruption and System Failures (BDSF) Level 2: Systems Level 3: Select one: • security breach – virus / malware

Data fields	Mandatory field	Description
		infection; • security breach – denial of service / distributed denial of service; or • security breach – web defacement
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15** REs must categorise the causes using the following definition of causal categories for technology-related incident / event: • People – Lapses in staff resources and competencies • Process – Lapses in IT operations management • System (IT) – IT products/ solutions' defect, limitation and/ or unknown vulnerabilities • External Event – Causal beyond REs' control e.g., service provider
Date and Time of Event Occurrence	Yes	The date and time on which the event happened or took place *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Event Detection	Yes	The date on which the REs became aware of the event *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Event Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Loss Event Captured in Provision Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of loss event captured	No	The date on which the operational risk loss is recognised based on the

Data fields	Mandatory field	Description
in P&L account		accounting framework of the REs *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction values associated with the reportable operational risk event reported Note: This field is mandatory if Financial Impact is selected.
Loss incurred by	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'.
Loss Event Description		
Where the event happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • On-premise – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • Off-premise – occurs outside premise(s) of REs: To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working **b) <u>For ITOs only</u>**

Data fields	Mandatory field	Description
		• On premise: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service ➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance ➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • Off-premise: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster
Number of Business Lines	Yes	To provide the number of affected business lines.

Data fields	Mandatory field	Description
affected		• **For banking**: by Business Line Level 1 • **For ITOs**: by Business Line Level 2 • **For PIIs and PSOs**: by Business Line Level 3 • **For Payments Network Malaysia Sdn. Bhd.**: by Business Line Level 2
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only
How the event occurred?	Yes	1. General operational risk event: An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g., Name, I/C number and other personal information.
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – for new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – for OR that REs have experienced previously within the last three years
Sub Nature of Event	No	Reportable operational risk events must be classified as either one of the following:

Data fields	Mandatory field	Description
		• **New MO –** for new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** for MO that REs have experienced previously within the last three years Examples: • **New** – Threat actor managed to gain unauthorised access to the RE's network for the first time by exploiting vulnerability in the VPN solution. • **Repeated** – Threat actor applied the same MO where the same vulnerability was exploited to gain unauthorised access to the RE's network in a separate cyber incident.
Modus Operandi Involved	Yes	REs must concisely define the method or manner of the cyber incidents or cyber events occurrence by referring to the types of cyber threats in 'Table 7: Types of cyber incident and cyber event'. An incident or event reporting may contain one or more types of cyber threats.
Root cause of the event	Yes	A detailed explanation on factors leading to the event must be provided and at minimum, must include the underlying cause of the event. If the root cause is yet to be determined, please specify the preliminary findings and update it as and when the root cause is identified.
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event. REs may select 'TBC' [To Be Confirmed]

Data fields	Mandatory field	Description
		for remedial action plans that are not finalised during the initial reporting.
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs may input expected remediation date. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided.
Remedial Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP
Reason (If Unresolved)	No	Justification(s) for delay(s) in resolving the operational risk event. E.g., The event root cause has been identified, however, the system / application impacted is yet to be resolved due to pending components from the vendor. Only applicable for events that are yet to recover.
Target Completion Date (If Unresolved)	No	REs must specify the target completion dateline to resolve the remedial action plans.
Mitigation action plan(s)	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may select 'TBC' [To Be Confirmed] for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation action completion date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs may input expected mitigation date. REs are required to update the LED with the latest date in the ORR system once the

Data fields	Mandatory field	Description
		mitigation action plan is completed.
Mitigation action plan(s) attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP
Technology Related Details		
IT-related categories	Yes	REs must select one or multiple relevant categories of IT-related event of the following: • **Cloud** – Application / service(s) hosted in cloud service provider (CSP) infrastructure • **IoT** –Internet of Things (IoT) device • **AI** – Artificial Intelligence (AI) based application • **Data Centre** – Management of RE's data centre, facilities and operations • **3rd Party** – Management of application / service(s) is procured / outsourced from / to external parties • **Hardware** – Physical server and / or devices • **Software** – System and / or application • **Utilities** – Electric, water, *etc*.
Consequence to Technology Operation	Yes	REs must select one or multiple impact to their IT infrastructure / technology operations of the following: • System / Service Unavailability • System Performance Degradation • Network Disruptions • Data Corruption • Data Leakage • Others (please specify) For each consequence selected, REs must provide respective information of the following:

		• Description of Consequence to Technology Operation • Parties involved in the event • Number of Individuals Involved / Affected by the Event • Description of Consequence to Users • System Involved/ Impacted table (if applicable) • Application Involved/ Impacted table details (if applicable)
Description of Consequence to Technology Operation	Yes	REs must describe the event impact to their IT infrastructure, technology and/ or business operations
Parties involved in the event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. Conditionally populated; please select the relevant parties involved and the number of users involved / affected • Customer(s) involved /affected • Staff • Third party service provider • Others (please specify)
Number of Individual(s) Involved in / Affected by the Event	Yes	Based on the 'Parties involved in the event' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Description of Consequence to Users	Yes	Description of the event impact to the parties involved respectively
System Involved / Impacted ?	Yes	Only applicable for an event that has affected IT system

		REs must select one of the following for operational risk event with / without system involvement or impact • Yes • No
System Involved/ Impacted (Name)	Yes	REs to provide the respective system name of the selected 'System Involved / Impacted (Type). Applicable when 'Yes' is selected under 'System Impacted'
System Involved/ Impacted (Type)	Yes	REs must select one or multiple affected critical business functions or systems as outlined in Appendix 4, **Table 9** Applicable when 'Yes' is selected under 'System Impacted'
Number of Transactions	Yes	To specify the total number of transactions impacted due to the OR event. Examples of reportable total number of transactions impacted: • Internet banking transactions, mobile banking transactions, SST transactions etc. • Number of impacted insurance policies. • E-money transactions, card transactions, etc. REs must also specify the number of transactions impacted for each critical system category and must avoid duplication in the overall total transactions for an event that encounters more than one critical system. In the event REs are unable to determine the actual number of transactions affected, REs shall strive to provide an estimate based on a sound basis.
System Cumulative Event Duration (in minutes)	Yes	REs must indicate the duration of event in minutes for each disrupted system services. If this event does not result in system / network outage or performance degradation, please indicate '0'. If the event has yet to resolve, state the duration (from event occurrence until reporting date) and update it as and when the system has been restored. Applicable when 'Yes' is selected under 'System Involved / Impacted'.

MTD of services	Yes	REs must state the defined Maximum Tolerable Downtime (MTD) of the selected system(s) Applicable when 'Yes' is selected under 'System Involved / Impacted'
RTO of services	Yes	REs must state the defined RTO of the selected system(s) Applicable when 'Yes' is selected under 'System Involved / Impacted'
Application Involved / Impacted?	Yes	Only applicable for an event that has affected IT applications REs must select one of the following for operational risk event with / without application involvement or impact • Yes • No
Application Involved/ Impacted (Name)	Yes	REs must specify the name of the selected application(s) Applicable when 'Yes' is selected under 'Application Impacted'
Application Involved/ Impacted (Type)	Yes	REs must select one or multiple affected critical applications of the following: • Network application • Security application • Database • Operating System • Middleware • Hypervisor • Storage • Others (please specify) Applicable when 'Yes' is selected under 'Application Impacted'
Application Cumulative Event Duration (in minutes)	Yes	REs must indicate the duration of event in minutes for each disrupted system and/ or application services. If this event does not result in system / network outage or performance degradation, please indicate '0'. If the event has yet to be resolved, state the duration (from event occurrence until the

		reporting date) and update it as and when the system has been restored.
RE Loss Event Severity	Yes	REs must provide its own internal event severity for each technology-related event reported in ORR system e.g., 1 - Critical
Number of Transactions Affected	Auto-generated / Yes	If REs selected 'Yes' for System Involved / Impacted, data field will be auto-generated based on the input for 'Number of Transactions'. If REs selected 'No' for System Involved / Impacted, data field will be mandatory. REs must specify the total number of transactions impacted due to the OR event. Examples of reportable total number of transactions impacted: • Internet banking transactions, mobile banking transactions, SST transactions etc. • Number of impacted insurance policies. • E-money transactions, card transactions, etc. REs must also specify the number of transactions impacted for each critical system category and must avoid duplication for overall total of transactions for an event that encounters more than one critical system. In the event REs are unable to determine the actual number of transactions affected, REs shall strive to provide an estimate based on a sound basis.
Breach SLA?	Yes	Only applicable for an event that has breached any internal / external SVS or System Level Agreement(SLA)
Justify the breach	Yes	Description of the SLA breached e.g.: • Vendor ABC breached outsourcing SLA with 90% uptime • Breached system SLA with 95% uptime Applicable when 'Yes' is selected under 'Breach SLA'
(Applicable upon selecting 'cloud' in 'IT-related categories')		

Cloud Service Provider Name	Yes	REs must select one of the following Cloud Service Provider names: • Amazon Web Services (AWS) • Alibaba • Microsoft Azure • Google Cloud Platform • VMware • Oracle Cloud • IBM Cloud • Red Hat • Verizon Cloud • Salesforce • SAP • Adobe • Cisco • Hewlett Packard Enterprise • Workday • Others (please specify) Applicable upon selecting 'cloud' in 'IT-related categories'
Type of cloud service model subscribed	Yes	REs must select one of the following cloud service models subscribed to: • **IaaS –** Infrastructure-as-a-service is a model providing infrastructure capabilities such as compute, network, or storage. • **PaaS –** Platform-as-a-service is a model providing platform capabilities i.e. execution environments for applications. • **SaaS –** Software-as-a-service is a model providing software capabilities which is managed and hosted by the provider.
Type of cloud deployment model	Yes	REs must select one of the following cloud deployment models subscribed to: • **Public** – The cloud infrastructure is made available to the general public and resources are controlled by the cloud service provider. • **Private** – The cloud infrastructure is operated exclusively for a single

		organization. It may be owned and managed by the organization or a third party and may exist on-premises or off premises. • **Community** – The cloud infrastructure is shared by a specific community of consumers from organizations who have shared specific concerns and requirements, and where resources are controlled by at least one member of this collection. • **Hybrid** – The cloud infrastructure is a composition of two or more clouds (public, private, or community) that remain as unique entities but are bound together by standardized or proprietary technology that enables data and application portability.
Affected CSP data centre location (Country)	Yes	REs must select the country of affected CSP data centre.
Affected CSP data centre location (State)	Yes	REs must select the state of affected CSP data centre.
Affected CSP data centre location (District)	No	REs must select the district of affected CSP data centre. *Only applicable to CSP data centres located in Malaysia
Backup CSP data centre location (Country)	Yes	REs must select the country of affected backup CSP data centre.
Backup CSP data centre location (State)	Yes	REs must select the state of affected backup CSP data centre.
Backup CSP data centre location (District)	No	If applicable, REs must select the district of affected backup CSP data centre. *Only applicable to CSP data centres located in Malaysia
(End of 'cloud' reporting for 'IT-related categories')		
Functional Impact	Yes	REs must measure the actual ongoing impact to the business functionality or the ability of the institution to provide services. REs must select one of the following Functional Impacts: • No impact • No impact to services • Minimal impact to non-critical services

		• Minimal impact to critical services • Significant impact to non-critical services • Denial of non-critical services or loss of control • Significant impact to critical services • Denial of critical services or loss of control Please refer to **Table 9** for the detailed description of each selection.
Observed Activity	Yes	REs must describe observed or detected threat actor activity on the REs' network or systems. REs must select one of the following Observed Activity: • Prepare • Engage • Presence • Effect Please refer to **Table 9** for the detailed description of each selection.
Location of Observed Activity	Yes	REs must describe and identify where the Observed Activity was detected in the institution's network. The location of Observed Activity is likely to change during the evolution of the incident and must be updated accordingly as and when information becomes available. REs must select one of the following Locations of the Observed Activity: • Level 0: Unsuccessful • Level 1: Business DMZ • Level 2: Business Network • Unknown • Level 3: Business Network Management • Level 4: Critical System DMZ • Level 5: Critical System Management • Level 6: Critical Systems • Level 7: Safety Systems Please refer to **Table 9** for the detailed description of each selection.
Information Impact	Yes	REs must identify the impact on the confidentiality and integrity of information stored or processed by various systems. REs must

		describe the type of information lost, compromised or corrupted. REs must select one of the following Information Impact: • No impact • Suspected but not identified • Privacy data loss • Proprietary information loss • Destruction of non-critical systems • Critical system data breach • Core credential compromised • Destruction of critical systems *Please refer to **Table 9** for the detailed description of each selection.*
Actor Characterization	Yes	REs must provide the attribution of the cyber incident to a particular actor set based on REs' understanding of the skill level, intentions and capabilities of that actor. REs must select one of the following Actor Characterizations: • Hacktivist • Unwitting insider • Criminal • Unknown • Witting insider • APT • APT (targeted) *Please refer to **Table 9** for the detailed description of each selection.*
Recoverability	Yes	REs must identify the scope of resources required to recover from the cyber incident. REs must select one of the following Recoverability: • Regular • Supplemented • Extended • Not recoverable

		*Please refer to **Table 9** for the detailed description of each selection.*
Damage (loss of integrity)	Yes	REs must select one or more of the following to indicate any impact on the loss of integrity: • Database of FI – Loss of FI's data integrity. For example, unauthorized modification of consumer and interbank counterparty related data or unauthorized modification of system files. • Database of major data provider – Loss of major data provider's data integrity. For example, financial data vendor (e.g., Bloomberg) provides erroneous data due to a compromised system. • None – No impact.
Disruption (loss of availability)	Yes	REs must select one or more of the following to indicate any impact on the loss of availability: • Payment systems – Loss of access to payment systems by REs. For example, RENTAS cannot be accessed. • Trading systems – Loss of access to trading systems by REs. • Client-facing systems – Unavailability of client-facing systems such as ATMs, online banking services, customer database servers and insurer claim systems. • Internal systems – Unavailability of RE's internal systems such as HR system, Customer Relationship Manager (CRM), email, desktops and laptops. • None – No impact.
Theft (loss of confidentiality)	Yes	REs must select one or more of the following to indicate any impact on the loss of confidentiality: • Data – Exfiltration of confidential data. For example, banking customer data breach. • Funds – Unauthorized transactions leading to direct monetary loss. For example, monetary transactions via compromised SWIFT systems at a FI. • None – No impact.
Threat Indicator	No	If applicable, REs must include any artefact or forensic evidence found on a network, system,

		database or file during incident investigation that indicates a cyber intrusion or attack. For example, hash values of malware, malicious IP addresses, malicious URLs, malware signature, etc. REs may update the submission as the investigation progresses and more information becomes available.

Table 9: Cyber Incident Scoring System Data Field drop down selections and definitions.

Data Field	Selection	Description
Functional Impact	No impact	The event has no impact. For instance, a dormant malware detected on an isolated PC.
	No impact to services	The incident has no impact to the business or external facing services. For example, scans and probes or a successfully defended attack, or DdoS attack which was mitigated by subscribed clean pipe services.
	Minimal impact to non-critical services	Insignificant disruption to non-critical systems and services (up to 120 minutes per incident). For example, minor disruption to internal Human Resources (HR) system.
	Minimal impact to critical services	Less significant disruption (up to 120 minutes per incident) to critical systems such as core banking services, active directory, ATM network, etc.
	Significant impact to non-critical services	Prolonged downtime (more than 120 minutes per incident) or disruption to internal systems such as internal HR system.
	Denial of non-critical services	Non-critical system rendered unavailable or destroyed. For example, internal HR system affected by ransomware or wiper malware.
	Significant impact to critical services	Prolonged disruption (more than 120 minutes per incident) or downtime of critical systems such as core banking, encryption / authentication systems, ATM network and active directory.

Data Field	Selection	Description
	Denial of critical services or loss of control	Critical system rendered unavailable or destroyed. For example, ransomware or wiper malware on core banking systems / active directory.
Observed Activity	Prepare	• Actions taken to establish the intent, capability and objectives. • Indicators of identifying potential targets and attack vectors, identifying resource requirements and developing capabilities, phishing or targeted phishing. • Cyber-attack lifecycle: reconnaissance / weaponisation.
	Engage	• Actions taken against targets prior to gaining access, with intent to gain access to victims' physical or virtual computer or information systems, network and data storage. • Stealing of sensitive information. • Installation of malware. • Contacting command & control (C&C). • Cyber-attack lifecycle: delivery.
	Presence	• Set of actions taken once access to the target physical or virtual computer or information system has been achieved. • Establish and maintain conditions for the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network or data storage. • Hijack server admin accounts, moving laterally in the network, hijack database admin accounts and C&C taking control of a system. • Cyber-attack lifecycle: exploitation / installation / command & control.

Data Field	Selection	Description
	Effect	• Outcomes of actions on a victim's physical or virtual computer or information system, network or data storage. • Corrupt, destroy or wipe data. • Deny availability to a key system or service. • Damage computer and networking hardware. • Cyber-attack lifecycle: exfiltration / actions on objectives.
Location of Observed Activity	Level 0: Unsuccessful	Existing network defences repelled all observed activity.
	Level 1: Business demilitarized zone (DMZ)	Activity was observed in the business network's DMZ. The systems are generally untrusted and are designed to be exposed to the Internet. For example, external web server or email server (Outlook Web Access).
	Level 2: Business Network	Activity was observed in the business or corporate network. For example, corporate user workstations, application servers and other non-core management systems.
	Unknown	Activity is observed, but the network segment, location source or extent of spread could not be identified.
	Level 3: Business Network Management	Activity was observed in business network management systems such as active directory servers or administrative workstations.
	Level 4: Critical System DMZ	Activity was observed in the DMZ that exists between the business network and a critical system network. For example, internally facing servers and services, SharePoint sites, jump servers and email systems.

Data Field	Selection	Description
	Level 5: Critical System Management	Activity was observed in critical internal management systems. For example, endpoint used to operate RENTAS / SWIFT, administrative workstations for core banking system and internal critical servers such as databases.
	Level 6: Critical Systems	Activity was observed in the critical systems. For example, core banking, treasury system, SWIFT or RENTAS.
	Level 7: Safety Systems	Activity was observed in critical safety systems that ensure the safe operation of an environment. For example, fire suppression systems in a data centre.
Actor Characterization	Hacktivist	Hacktivists use hacking to increase awareness of their social or political agendas. They are usually involved in activities such as website disabling and defacing. Common targets include government agencies and multinational corporations.
	Unwitting Insider	A person who has legitimate access to the internal network but has made a bad judgement call. For example, such person has plugged in a USB drive found unattended, clicked on a malicious link, accidentally opened a malicious attachment or made an accidental error during a change management process.
	Criminal	Organized hackers that aim to attack systems for monetary gain, such as ransom. Often hack systems, network and data storages to obtain confidential data or financial information such as credit card data.
	Unknown	The threat actor or type of threat origin is unknown or is yet to be determined.
	Witting Insider	A person who has legitimate access to systems and networks but makes a conscious decision to cause harm to the systems, networks or data. For example, disgruntled employees / vendors.

Data Field	Selection	Description
	APT	A threat actor that possesses sophisticated levels of expertise and significant resources which allows it to create opportunities to achieve its objectives by using multiple threat vectors. The advanced persistent threat (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to execute its objectives. APT attacks are stealthy in nature, hence the effect on computer and network performance is usually unnoticeable. The threat can remain undetected for a long period of time.
	APT (Targeted)	A targeted Advanced Persistent Threat (APT) is specifically crafted to pick the victim carefully driven by a certain motive. Actor would usually leverage spear-phishing techniques. A targeted attack can potentially cause a catastrophic impact.
Recoverability	Regular	Time to recover is predictable with existing resources. For example, institution's internal security team is able to handle the incident with existing controls and measures in place.
	Supplemented	Time to recover is predictable with additional resources. For example, institution requires additional resources such as existing vendor or support from group security team.
	Extended	Time to recover is unpredictable and additional resources or outside assistance may be required. For example, institution requires assistance from new vendors or state cybersecurity agencies.
	Not recoverable	Recovery from the incident is not possible. For example, sensitive data exfiltrated, critical systems including backups encrypted or wiped.

Data Field	Selection	Description
Information Impact	No impact	No known impact to data or information.
	Suspected but not identified	Suspected data theft or unauthorised modification to confidential data with no visible impact.
	Privacy data loss	Customer or employee personal data exfiltrated such as contact details, addresses, etc.
	Proprietary information loss	Theft of confidential business information. For example, business plan, network designs, etc.
	Destruction of non-critical systems	Data of non-critical system is modified. For example, email system configuration or data in employee internal portal.
	Critical systems data breach	Data of critical system is exfiltrated. For example, credit card information or online banking user credentials.
	Core credential compromise	Critical system credentials hijacked or exfiltrated. For example, administrative credentials for critical system management.
	Destruction of critical systems	Data of critical system is altered to cause systemic impact to the business in the long run. For example, unauthorised modification of codes in a treasury system resulted in wrong business decisions.

APPENDIX 4 Critical BDSF event reporting requirements

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

2. REs must report all actual critical BDSF events to ORR in accordance with the requirements set out in **Table 10: Critical BDSF event reporting types** within **14 calendar days** upon event confirmation regardless of whether the events are translated into a financial / non-financial impact.

3. REs that are subject to the BCM Policy Document must notify the relevant stakeholders in the Bank (Relationship Managers and/or Supervisors) within 2 hours of any major disruptions (i.e., Level of Disruption (LoD) 3 and above). In addition, REs must report the BDSF events to ORR in accordance with **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR reporting types and deadlines.**

4. For the avoidance of doubt, REs that are not subject to BCM Policy Document must report critical BDSF events to ORR in accordance with **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR reporting types and deadlines.**

5. For critical BDSF events that are non-technology related, please refer to Appendix 10, paragraph 15 for the reporting requirements.

Table 10: Critical BDSF event reporting types

Category	Definition
Critical BDSF event	• Any business disruption of LoD 1 event involving failure at the main branch or processing hub, irrespective of breaching or not breaching Maximum Tolerable Downtime (MTD) timeline including network. • Any business disruption of LoD 2[6] and above irrespective of breaching or not breaching MTD timeline including network. • Any system failure or system execution failure occurred at REs or outsourced service providers affecting the critical business functions or systems of REs irrespective of the disruption severity, impact, or MTD timeline breach. Critical business functions or systems may include but are not limited to: 1. Core Banking System 2. Core Insurance System

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

Category	Definition
	3. Payment System: • e-SPICK • RENTAS • Interbank Fund Transfer 4. Treasury System 5. Self-Service Terminals: • CRM • CDM • ATM 6. Internet Banking 7. Mobile Banking 8. Call Centre 9. Insurance e-Covernote 10. Internet Insurance 11. Mobile Insurance 12. Accounting / General Ledger (GL) System 13. Card System 14. SWIFT 15. Core Payment System 16. Others (please specify) ***Note:*** *The list of critical systems above is not exhaustive and REs should assess whether other systems should be considered as critical, with consideration that the application system supports the provision of critical banking, insurance or payment services, where failure of the system has the potential to significantly impair the FI's provision of financial services to customers or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements* • Any acceptance of counterfeit Malaysian currency notes by deposit-accepting SST. **Please refer to appendix 8.**

6. A critical BDSF event may affect several lines of business. REs 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 a descending priority):

   (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).

7. Examples of reportable critical BDSF events:

   a. Card system was down due to the inability to connect with middleware application (enterprise service bus) after system patch i.e. changes / fixes was performed on the card system

      - **Loss Event Name**: Card system was down
      - **Loss Event Classification**: Actual Event
      - **Event Type Level 1**: Business disruption and system failures
      - **Event Type Level 2**: System
      - **Event Type Level 3**: Software – Application issue
      - **Causal categories**: Process >> Inadequate process change / implementation >> Inadequate testing

   b. Internet Banking experienced slow performance due to a database hung as there is limited database capacity

      - **Loss Event Name:** Online banking experienced performance degradation
      - **Loss Event Classification:** Actual Event
      - **Event Type Level 1:** Business disruption and system failures
      - **Event Type Level 2:** System
      - **Event Type Level 3:** Software – Database issues
      - **Causal categories:** System (IT) >> Software (IT application/ OS/ DB) >> Application Defect

c. Firewall engineer accidentally configured external-facing firewall wrongly and caused multiple system inaccessibility by the customer (online banking, mobile banking and ATM):

- **Loss Event Name:** Internet banking (web and mobile) and ATM was down
- **Loss Event Classification:** Actual Event
- **Event Type Level 1:** Business disruption and system failures
- **Event Type Level 2:** System
- **Event Type Level 3:** Network / Security devices or tools/appliances issues
- **Causal categories:** People >> Competence >> Unintentional error

Reporting critical business disruption and/ or system failure (BDSF) event in ORR

Category: Technology-related event for critical BDSF

Loss Event Classification: Actual Event

Applicability: All REs

Table 11: Data fields for reporting critical BDSF events

Data fields	Mandatory field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as one of the following: • New • Work In Progress (WIP) • Completed • Withdrawn

Data fields	Mandatory field	Description
		Note: 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	Reportable operational risk events must be reported based on the "Level 1" to "Level 3" in **Table 3: ORR LED reporting types and deadlines.** REs must report critical BDSF event using ONLY the following selections: • **Level 1:** Critical Event • **Level 2:** Technology Related • **Level 3:** Critical BDSF
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event.

Data fields	Mandatory field	Description
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Auto-generated	The reportable operational risk event will be classified as: • **Actual Event** – Any technology-related event that has been confirmed. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes a high reputational impact based on REs' internal framework
Islamic Business?	Yes	RE must select '**Yes**' for event that involves Islamic products or services, which may or may not be related to shariah related matters Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin
Impact, Business Line & Event Type		
Loss Event impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss • **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc.

Data fields	Mandatory field	Description
		• **Both financial and non-financial impacts** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	REs must select one of the following for operational risk event with Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk, but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraph 16.6 and 16.7*
Non-Financial Impact Justification	Yes	REs must justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Business lines	Yes	Must be reported up to Level 3 based on **Appendix 13** *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any*
Product / Service	Yes	Must be reported based on Level 3 Business Line selection in accordance with the taxonomy in **Appendix 13.**
Delivery Channel	Yes	Channel used to deliver the product/services of the operational risk events. **For REs except ITOs:** • Internet • Mobile

Data fields	Mandatory field	Description
		• Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A **For ITOs only:** • Direct Clients – Walk In • Direct Clients – Internet • Direct Clients – Direct Mailing • Direct Clients – Marketing Staff • Direct Clients – Others • Telemarketing • Franchise Holders / Dealers (for GITOs only) • Registered Individual Agents • Registered Corporate Agents • E-Commerce Marketplace • Partners in Digital Platforms • Financial Advisers • Bancassurance / Bancatakaful • Co-Insurer / Co-Takaful • Insurance / Takaful Brokers • Reinsurance / Retakaful Accepted • Others (please specify)
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event.

Data fields	Mandatory field	Description
		REs must categorise the event using ONLY the following selection of event types: **Level 1:** BDSF **Level 2:** Systems **Level 3:** Select one: • Hardware – Server issues • Hardware – Storage platform issues • Network / Security devices or tools/appliances issues • Hardware – Others • Software – Application issues • Software – Operating System issue • Software – Database issues • Software – System interfaces / linkages issues • Software – Others • Telecommunication – Telecommunication network issue • Telecommunication – Internet Service providers' issue • Telecommunication – International and Local Switches issues (VISA, MasterCard, MEPS & My Clear) Please refer to the examples provided in paragraph 8 of **Appendix 4**.
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in Appendix 15 REs must categorise the causal using the following definition of causal categories for technology-related event: • People – Lapses in staff resources and competencies • Process – Lapses in IT operations management

Data fields	Mandatory field	Description
		• System (IT) – IT products/ solutions' defect, limitation and/ or unknown vulnerabilities • External Event – Causal beyond REs' control e.g., service provider *Please refer to the examples provided in paragraph 8 of **Appendix 4**.*
Date and Time of Event Occurrence	Yes	The date and time when the technology-related event occurred. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date when the technology-related event is detected. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Confirmation	Yes	The date the technology-related event confirmation is obtained. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Loss Event Captured in Provision Account	No	The earliest date when the operational risk loss has been accrued in suspense, reserve or provision of REs' accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date when the operational risk loss is recognised based on REs' accounting framework. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transactions value associated with the operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss incurred by	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance

Data fields	Mandatory field	Description
		Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'.
Loss Event Description		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • On-premise – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • Off-premise – occurs outside premise(s) of REs: To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working **b) <u>For ITOs only</u>** • On premise: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims

Data fields	Mandatory field	Description
		➢ Corporate communication / marketing ➢ Customer service ➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance ➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • Off-premise: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster
Number of Business Lines Affected	Yes	Only applicable for event that affects multiple business lines. Please refer to Appendix 2.
Location(s) of Events	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred

Data fields	Mandatory field	Description
		• **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only
How the Event Occurred?	Yes	REs must provide an executive summary of the chronology of the event. The executive summary must not include customer / individual confidential information e.g., name, IC number and other personal information.
Nature of Event	Yes	Technology-related events must be classified as either one of the following: • **New** - For new types of technology events impacting the REs for the first time in the last three years or same types of technology events which re-occur after three years. Please refer to paragraph 17.9; or • **Repeated** - For technology event that REs have experienced previously within the last three years
Sub Nature of Event	Yes	Technology-related events must be classified as either one of the following: • **New** – For new types of MO which may include tactics, techniques and procedures impacting the REs for the first time in the last three years or for MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For MO that REs have experienced previously within the last three years.

Data fields	Mandatory field	Description
Modus operandi involved	Yes	REs must concisely define the method or manner of the occurrence of technology-related events. The modus operandi involved in the LED must be stated and it is not limited to fraud modus operandi. For examples, please refer to paragraph 17.8.
Root cause of the event	Yes	REs must provide a detailed explanation on factors leading to the operational risk which at minimum must include the underlying cause of the event and the detection medium. If the root cause is yet to be determined, please specify the preliminary findings and update it as and when the root cause is identified.
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event REs may select 'TBC' [To Be Confirmed] for remedial action plans that are not finalised during the initial reporting .
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs may input expected remediation date. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided.
Remedial Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF

Data fields	Mandatory field	Description
Reason (If Unresolved)	No	Justification(s) for delay(s) in resolving the operational risk event. E.g., The event root cause has been identified, however, the system / application impacted is yet to be resolved due to pending components from the vendor. Only applicable for events that are yet to recover.
Target Completion Date (If Unresolved)	No	REs must specify the target completion dateline to resolve the remedial action plans.
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying operational risk event and to ensure prevention of recurrence of similar incidents in the future. REs may select 'TBC' [To Be Confirmed] for mitigation action plan(s) that are not finalised during the initial reporting
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs may input expected mitigation date. REs are required to update the LED with the latest date in the ORR system once the mitigation action plan is completed.
Mitigation Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP
Technology Related Details		
IT-related categories	Yes	REs must select one or more relevant categories of IT-related events of the following: • **Cloud** – Application / service(s) hosted in CSP infrastructure • **IoT** –Internet of Things (IoT) device

Data fields	Mandatory field	Description
		• **AI** – Artificial Intelligence (AI) based application • **Data Centre** – Management of RE's data centre, facilities and operations • **3rd Party** – Management of application / service(s) is procured / outsourced from / to external parties • **Hardware** – Physical server and / or devices • **Software** – System and / or application • **Utilities** – Electric, water, etc.
Consequence to Technology Operation	Yes	REs must select one or more of the following impacts to their IT infrastructure / technology operations: • System / Service Unavailability • System Performance Degradation • Network Disruptions • Data Corruption • Data Leakage • Others (please specify) For each consequence selected, REs must provide the respective information of the following: • Description of Consequence to Technology Operation • Parties Involved in the Event • Number of Individuals Involved / Affected by the Event • Description of Consequence to Users • System Involved / Impacted table details (if applicable) • Application Involved / Impacted table details (if applicable)

Data fields	Mandatory field	Description
Description of Consequence to Technology Operation	Yes	REs must describe the event impact to their IT infrastructure, technology and / or business operations
Parties Involved in the Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. Conditionally populated; please select the relevant parties involved and the number of users involved / affected • Customer(s) involved / affected • Staff • Third party service provider • Others (please specify)
Number of Individual(s) Involved In / Affected By the Event	Yes	Based on the 'Parties involved in the event' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Description of Consequence to Users	Yes	Description of the event impact to the respective parties involved
System Involved / Impacted	Yes	Only applicable for an event that has affected IT system REs must select one of the following for operational risk event with / without system involvement or impact • Yes • No
System Involved / Impacted (Name)	Yes	REs must provide respective system name of the selected 'System Involved / Impacted Type' Applicable when 'Yes' is selected under 'System Involved / Impacted'

Data fields	Mandatory field	Description
System Involved / Impacted (Type)	Yes	REs must select one or multiple affected critical business functions or systems as outlined in Appendix 4 **Table 9** Applicable when 'Yes' is selected under 'System Involved / Impacted'
Number of Transactions	Yes	To specify total number of transactions impacted due to the OR event. Examples of reportable total number of transactions impacted: • Internet banking transactions, mobile banking transactions, SST transactions etc. • Number of impacted insurance policies. • E-money transactions, card transactions, etc. REs must also specify the number of transactions impacted for each critical system category and must avoid duplication for overall total of transactions for an event that encounters more than one critical system. In the event REs are unable to determine the actual number of transactions affected, REs may strive to provide an estimate based on sound basis.
System Cumulative Event Duration (in minutes)	Yes	REs must indicate the duration of event in minutes for each disrupted system services. If this event does not result in system / network outage or performance degradation, please indicate '0'. If the event has yet to resolve, state the duration (from event occurrence until reporting date) and update it as and when the system has been restored. Applicable when 'Yes' is selected under 'System Involved / Impacted'

Data fields	Mandatory field	Description
MTD of services	Yes	REs must state the defined MTD of the selected system(s) Applicable when 'Yes' is selected under 'System Involved/ Impacted'
RTO of services	Yes	REs must state the defined Recovery Time Objective (RTO) of the selected system(s) Applicable when 'Yes' is selected under 'System Involved / Impacted'
Application Involved / Impacted	Yes	Only applicable for an event that has affected IT application REs must select one of the following for operational risk event with / without application involvement or impact • Yes • No
Application Involved / Impacted (Name)	Yes	REs must specify the name of the selected application(s) Applicable when 'Yes' is selected under 'Application Involved / Impacted'
Application Involved / Impacted (Type)	Yes	REs must select one or more of the following affected critical applications: • Network application • Security application • Database • Operating System • Middleware • Hypervisor • Storage • Others (please specify) Applicable when 'Yes' is selected under 'Application Involved / Impacted'
Application Cumulative Event Duration (in minutes)	Yes	REs must indicate the duration of event in minutes for each disrupted application services.

Data fields	Mandatory field	Description
		If this event does not result in application outage or performance degradation, please indicate '0'. If the event has yet to resolve, state the duration (from event occurrence until reporting date) and update it as and when the application has been restored. Applicable when 'Yes' is selected under 'Application Involved / Impacted'
RE Loss Event Severity	Yes	REs must provide its own internal event severity for each technology-related event reported in ORR e.g., 1 – Critical
Number of Transactions Affected	Auto-generated	If REs select 'Yes' under 'System Involved / Impacted', data field will be auto-generated based on the input for 'Number of Transactions'. REs must specify the total number of transactions impacted due to the OR event. Examples of reportable total number of transactions impacted: • Internet banking transactions, mobile banking transactions, SST transactions etc. • Number of impacted insurance policies. • E-money transactions, card transactions, etc. REs must also specify the number of transactions impacted for each critical system category and must avoid duplication for overall total of transactions for an event that encounters more than one critical system. In the event REs are unable to determine the actual number of transactions affected, REs may strive to provide an estimate based on sound basis.
Breach Service or System Level Agreement (SLA)	Yes	Only applicable for an event that has breached any internal / external SLA

Data fields	Mandatory field	Description
Justify the breach	Yes	Description of the SLA breached e.g.: • Vendor ABC breached outsourcing SLA with 90% uptime • Breached system SLA with 95% uptime Applicable when 'Yes' is selected under 'Breach SLA'
(Applicable upon selected 'cloud' in 'IT-related categories')		
Cloud Service Provider Name	Yes	REs must select one of the following Cloud Service Provider name: • Amazon Web Services (AWS) • Alibaba • Microsoft Azure • Google Cloud Platform • VMware • Oracle Cloud • IBM Cloud • Red Hat • Verizon Cloud • Salesforce • SAP • Adobe • Cisco • Hewlett Packard Enterprise • Workday • Others (please specify) Applicable once 'cloud' in 'IT-related categories' is selected
Type of cloud service model subscribed	Yes	REs must select one of the following cloud service models subscribed: **IaaS** - Infrastructure-as-a-service is a model providing infrastructure capabilities such as compute, network, or storage.

Data fields	Mandatory field	Description
		• **PaaS** - Platform-as-a-service is a model providing platform capabilities i.e., execution environments for applications. • **SaaS** - Software-as-a-service is a model providing software capabilities, managed and hosted by the provider.
Type of cloud deployment model	Yes	REs must select one of the following cloud deployment models subscribed: • **Public** - The cloud infrastructure is made available to the general public and resources are controlled by the cloud service provider. • **Private** - The cloud infrastructure is operated exclusively for a single organization. It may be owned and managed by the organization or third party and may be exist on-premises or off premises. • **Community** - The cloud infrastructure is shared by a specific community of consumers from organizations who have shared specific concerns and requirements, and where resources are controlled at least one member of this collection. • **Hybrid** - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.
Affected CSP data centre location (Country)	Yes	REs must select the country of affected CSP data centre.
Affected CSP data centre location (State)	Yes	REs must select the state of affected CSP data centre.

Data fields	Mandatory field	Description
Affected CSP data centre location (District)	No	REs must select the district of affected CSP data centre. *Only applicable to CSP data centres located in Malaysia
Backup CSP data centre location (Country)	Yes	REs must select the country of affected backup CSP data centre.
Backup CSP data centre location (State)	Yes	REs must select the state of affected backup CSP data centre.
Backup CSP data centre location (District)	No	REs must select the district of affected backup CSP data centre. *Only applicable to CSP data centres located in Malaysia

APPENDIX 5 Customer information breaches reporting requirements

1. Reporting of customer information breaches must be done in line with the requirements stipulated in the Management of Customer Information and Permitted Disclosures policy document issued by the Bank (MCIPD).

2. The Reporting As 'Actual Event' to ORR system must be done **within 1 working day** upon the **tabling of the investigation report on the customer information breach to the Board.**

3. RE must report the occurrence of any customer information breach that:

   (a) causes or is likely to cause significant harm to the affected customer(s);
   (b) is of significant scale (i.e., affected customers exceeds or is likely to exceed 1,000); or
   (c) involves a deliberate attempt on unauthorised disclosure of customer information.

4. Examples of customer information breaches:

   - **Loss Event Classification:** Actual Event
   - **Event Type Level 1:** Clients, products and business practices
   - **Event Type Level 2:** Fiduciary
   - **Event Type Level 3:** Breach of privacy or select the event types that are most relevant

   Scenario 1: RE detected staff A in the IT department has accessed information on a few customers without proper authorisation and used the information to contact the customers for unsolicited sales in meeting his KPI. There is no evidence that staff A has disclosed the customers' information to any third party.

   - **Type of Breach:** RE must select 'breach of the MCIPD'.

   Scenario 2: An anonymous person hacked a merchant's system and gained access to the information of credit card customers of the RE stored in the system. The hacker consequently dumped the credit card information (including the credit card numbers and expiry dates) in the dark web.

   - **Type of Breach:** RE must select 'breach of FSA /IFSA /DFIA'.

   Scenario 3: RE detected that staff A in IT department had accessed information of more than 1,000 customers without proper authorisation, and noted that staff A had disclosed the information to a third party.

   - **Type of Breach:** RE must select 'Both'.

Reporting customer information breaches in ORR

Category: Customer information breaches
Loss Event Classification: Actual Event
Applicability: All REs

Table 12: Data fields for reporting customer information breaches

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure • REs must select the respective reporting entity for REs under "Financial Group structure"
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised.

Data fields	Mandatory field	Description
		6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	For customer information breaches, REs must report under the following: • **Level 1**: Critical Event • **Level 2**: Customer information breaches
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event must be stated
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Auto-generated	Customer information breaches should be reported as **'Actual Event**'. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes high reputational impact based on REs internal framework. This may include, but not be limited to events that: • attract/is likely to attract significant media attention; or • pose a threat to public confidence and trust in the financial system
Boundary Event	No	REs must categorise the operational risk event as being either related to Credit, Market risk or Not Applicable with reference to **Appendix 11.** Note: This is applicable to BIs only.

Data fields	Mandatory field	Description
Islamic Business?	Yes	REs must select 'Yes' for an event that involves Islamic products or services, which may or may not be related to shariah related matters Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss • **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc • **Both financial and non-financial –** There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	REs must select one of the following for an operational risk event with a Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for an operational risk event with a Non-Financial Impact:

Data fields	Mandatory field	Description
		• Low • Medium • High *Note: the non-financial impact is not confined to reputation risk, but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7*
Non-Financial Impact Justification	Yes	REs must justify the reason behind the selection of High / Medium / Low for the non-financial impact with an explanation of the related non-financial risks
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13** *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any*
Product / Service	Yes	Must be reported based on Level 3 Business Line selection in accordance with the taxonomy in **Appendix 13**.
Event Type	Auto-generated	REs must categorise the customer information breach event as follows: • **Level 1:** Client, products and business practices • **Level 2:** Fiduciary • **Level 3:** Breach of Privacy
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15**
Date of Event Occurrence	Yes	REs must report the date when the customer information breach took place *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Event Detection	Yes	REs must report the date on which the REs became aware of the event *Please refer to paragraph 16.2 for the definition of the mentioned date*

Data fields	Mandatory field	Description
Date of Event Confirmation	Yes	REs must report the date on which the REs verified or confirmed the customer information breach *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Loss Event Captured in Provision Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction value associated with the operational risk event reported Note: This field is mandatory if Financial Impact is selected.
Loss Incurred By	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'
Loss Event Description		

Data fields	Mandatory field	Description
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • **On-premise** – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre. • **Off-premise** – occurs outside premise(s) of REs: To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working. **b) <u>For ITOs only</u>** • **On premise**: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service ➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance ➢ Human resource ➢ Information technology ➢ Investment ➢ Legal

Data fields	Mandatory field	Description
		➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • **Off-premise**: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster.
Number of Business Lines Affected	Yes	Only applicable for an event that affects multiple business lines. Please refer to Appendix 2.
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.
How the Event Occurred	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential

Data fields	Mandatory field	Description
		information e.g., Name, I/C number and other personal information.
Nature of Event	Yes	Operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or for OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years.
Modus Operandi Involved	Yes	REs must concisely define the method or manner of the reportable operational risk event occurrence. The MO involved in the LED is not limited to fraud MO. *Please refer to paragraph 17.8 for examples*
Parties Involved in / Affected by the Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer involved / affected • Staff • Third party service provider • Others (please specify) Conditionally populated, please select the relevant parties involved and the number of users involved / affected
Parties Involved in / Affected by the Event - Other	No	If applicable, REs must specify and explain the selection of "Others" under "Parties Involved in / Affected by the Event"
Name of Parties Who / Which Have Committed the Breach	Yes	RE must provide the name of the individual(s) who committed the breach
Name of Employer	No	If applicable, REs must provide the name of the employer if the person who committed

Data fields	Mandatory field	Description
		the breach is not directly employed by the RE
Name of Customer(s)	Yes	REs must provide the name(s) of customer(s) that is / are affected by the customer information breach. RE must either list down each customer under this data field or attach the list of customers under 'Attachment of evidence and supporting information'. If RE chooses the latter, the RE must specify 'Refer to Attachment' in the data field for this item.
Type of Customer	No	Select the type of customer affected by the customer information breach from the following options: • Public figure • Celebrity • Political figure • Others likely to attract media attention • Others (please specify)
Type of customer - Others	No	If applicable, REs must explain and specify the selection of "Others" for the type of customer
Staff ID	No	Provide the Staff ID(s) of the staff who committed the breach
Frequency of offence by staff	Yes	REs must select between the 1st / 2nd / 3rd / more than 3 to specify whether the customer information breach reported is the staff's 1st breach / 2nd / 3rd / more than 3 times. Where more than one staff is involved, RE must select the frequency of offence for each staff
Degree of personal culpability	Yes	This item is relevant only where the RE's staff is involved in the customer information breach REs must select the degree of personal culpability (Level 1 to 4) Where more than one staff is involved in the breach, RE must select the Degree of Personal Culpability for each staff

Data fields	Mandatory field	Description
		Level 1 • Performed duties accordingly but customer information breach occurred due to factors that are beyond control; and/or • unaware that the action will lead to unauthorized disclosure of customer information **Level 2** • Performed duties but failed to take reasonable steps that a person in his position ought to and would have taken to avoid the customer information breach **Level 3** • Failed to perform duties to avoid the occurrence of the customer information breach **Level 4** • Actively committed a misconduct to circumvent rules and procedures that led to the customer information breach with the intention of receiving any personal gain/interest/benefit
Type of 3rd Party Service Provider	Yes	If '3rd Party Service Provider' is selected under 'Parties Involved In / Affected By Event', REs must select one of the options below: o External debt collectors o Courier company o Law firm o Accounting firm o Others (please specify)
Information on Other Entity Involved (If Applicable)	No	REs must explain the selection of 'Others' under 'Type of 3rd Party Service Provider' such as the nature and name of the 3rd party service provider, as well as the extent of involvement by the 3rd party service provider in the customer information breach.

Data fields	Mandatory field	Description
Remedial Action Plans	Yes	Immediate actions taken by the staff/RE to minimize adverse effects from the customer information breach. REs must select all applicable remedial actions from the given options: • Require unintended recipient to delete the email with customer information and obtain confirmation of the said deletion • Recall the email using the RE's email system • Require the return of the Letter/Document/Parcel to the RE • Alert the account holder of the breach • Obtain an undertaking from the unintended recipient, that the recipient would not disclose the customer information • Others
Remedial Action Plans - Others	No	If applicable, REs must explain and specify the selection of "Others" under remedial actions
Remedial Action Completion Date	Yes	The date the remedial action is implemented. If the remedial action has not been implemented, REs may input 'TBC'. REs are to update the reported case with the date in the ORR, once the remedial action plan is implemented.
Remedial Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF
Mitigation Action Plans	Yes	Actions taken by the RE to prevent future occurrences of customer information breaches of a similar nature. REs must select all applicable mitigation action plans from the given options: • Legal Action

Data fields	Mandatory field	Description
		• Retraining • Introducing new Policy & Procedures • Others (please specify)
Mitigation Action Plan(s) - Others	No	If applicable, REs must explain and specify the selection of “Others” under mitigation action plans
Mitigation Action Completion Date	Yes	The date the mitigation action plan is implemented. If the mitigation action has not been implemented, REs may input ‘TBC’. REs are to update the reported case with the date in the ORR system, once the mitigation action plan is implemented
Mitigation Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF
Disciplinary action(s) taken	Yes	REs must select all applicable disciplinary actions to be taken against the staff that have committed the breach, from the following options: • Termination • Demotion • Monetary penalty (e.g., bonus/commission reduction) • Blacklisted/barred from certain functions • Warning letter • Verbal warning • Counselling • Others (please specify) • No actions taken Where "No actions taken" is selected, REs should explain the reason why no actions were taken on the customer information breach

Data fields	Mandatory field	Description
Disciplinary Action(s) Taken – Others	Yes	If applicable, REs must explain and specify the selection of "Others" disciplinary action(s)
Disciplinary Action(s) – No Actions Taken	No	If applicable, REs must explain why no disciplinary actions have been taken (e.g., staff resigned)
Disciplinary Action(s) Completion Date	Yes	The date on which the disciplinary action(s) is taken/implemented
Customer Info Breach Details		
Type of breach	Yes	State whether the incident is a breach or contravention of: • the provisions within the FSA / IFSA / DFIA (the Acts); • the standards within the MCIPD; or • both of the above A contravention of the secrecy provisions within the Acts occurs when an RE discloses any customer information to another party, where such disclosure is prohibited[7] by the Acts and is not within the scope of permitted disclosures as provided for in the Acts[8]. A breach of the standards within the MCIPD, on the other hand, covers a wider scope that includes theft, loss, misuse or unauthorised access and modification of customer information. Thus, in practice, there may be instances where: • breaches of the standards within the MCIPD do not result in a contravention of the secrecy provisions under the Acts mentioned above; or

[7] Section 133 FSA and the corresponding section 145 IFSA and section 119 DFIA.
[8] Section 134 FSA and the corresponding section 146 IFSA and section 120 DFIA.

Data fields	Mandatory field	Description
		• the incident is both a contravention of the secrecy provisions under the Acts, as well as a breach of the standards within the MCIPD.
Details of the breach of the MCIPD standards	Yes	REs must state the relevant regulatory provision / policy document that is breached and include the specific paragraph / requirement breached
Channel of disclosure	Yes	REs must select the channel through which the breach involving customer information had occurred from the following options: • Email • Letter • Face-to-face • Phone • Internet banking • Others (please specify)
Channel of disclosure - Others	No	If applicable, REs must explain and specify the selection of “Others” type of channel
Detection Mechanism	Yes	REs must select all applicable means through which the incident was detected from the following options: • Internal Data Loss Prevention • Customer complaint • Identified by other staff • Whistle-blower • Others (please specify)
Detection Mechanism - Others	No	If applicable, REs must explain and specify the selection of “Others” detection mechanism
Type of information disclosed	Yes	REs must select all applicable types of customer information that was disclosed in the customer information breach from the following options: • Customer name

Data fields	Mandatory field	Description
		• IC number • H/P number • Address • Email • Account/policy/certificate number • Account/policy/certificate details • Transaction details • Others (please specify)
Type of information disclosed - Others	No	If applicable, REs must explain and specify the selection of "Others" type of information
Recipient of customer information	Yes	REs must select all applicable recipients of the customer information in the customer information breach from the following options: • Family member • Internal staff of RE • Staff of other domestic entities in the Group • Staff of other entities in the Group in other countries • Vendor/3rd party panel • Other REs • Other 3rd party • Unable to be determined
Number of Recipient	Yes	REs must specify the total number of recipients of the customer information
Harm to Customer	Yes	REs must select the type of harm to the customer(s) from the breach from the 2 options: • Financial • Others (please specify)

Data fields	Mandatory field	Description
		Financial Harm: Customer has suffered monetary loss due to the breach of information Other: Customer has suffered other tangible or intangible harm due to the breach of information, including but not limited to litigation, reputational harm, and personal hardship.
Harm to Customer - Others	No	If applicable, REs must explain and specify the selection of “Others” harm to customer
Monetary Benefit Gained by Offender	Yes	REs must state if there was monetary benefit gained by the staff and if so, specify the amount involved
Escalation of Breach Incident to Board of Directors	Yes	REs must state if the breach has been tabled to the Board of Directors. RE must attach the supporting minutes of the Board meeting under ‘Attachment of evidence and supporting info’. If the minutes of the Board meeting is not ready at the point of reporting via the ORR, RE can submit the minutes at a later date as soon as it is finalised, via ORR.
Reason	No	If the breach was not escalated to the Board of Directors, REs must provide the justification as to why the customer information breach has not been escalated to the Board of Directors.
Availability of evidence	Yes	REs must state whether evidences of the breach are available. Where REs select 'Yes', evidences should be provided under 'Attachment of evidence and supporting info'
Attachment of evidence and supporting info	Yes	REs must attach evidence and supporting information/documents relevant to the customer information breach. Examples include (but are not limited to) minutes of Board meeting where customer information breaches were tabled, investigation reports, internal audit reports, bank statements, letters sent to customers, email correspondences, conversation screenshots, signed SLAs, etc.

APPENDIX 6 SNC event reporting requirements

1. REs must ensure all operational risk events that relate to Islamic financial businesses are assessed and reported appropriately.

2. REs must report both potential and actual SNC events via the ORR system in accordance with the requirements and timelines set out in **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines**.

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

4. In order to promote vigilance and responsiveness in addressing SNC risks, REs are expected to ensure the overall management of SNC events (i.e., detection, confirmation and rectification) is expedited, without any undue delay.

5. The reporting of SNC events are applicable to all entities which offer Islamic financial business. The SNC events must be reported by the product or business owner regardless of where the event occurred. For example, Investment Bank A encounters a SNC event of which the loss impacts the general ledger (GL) of Islamic Bank A. In this case, Islamic Bank A is required to report the SNC event via the ORR system.

Shariah Committee (SC) / Shariah Advisor (SA)[9]

6. The RE's SC/SA must deliberate on and decide whether Potential SNC event is SNC or non-SNC. This decision must be clearly reflected in the SC's SC/SA's meeting minutes.

7. The loss event classification of "Actual" or "Potential" is not under the purview of the SC/SA.

Shariah contracts

8. In relation to the definition of specific Shariah contracts, please refer to the relevant policy documents on Shariah contracts and Shariah rulings issued by the Bank.

Potential SNC event

9. A potential SNC event is defined as any Shariah related event detected and confirmed by an officer within the control function where the SC/SA's decision is pending.

---

[9] Shariah Advisor (SA) refers to paragraphs 12.4 and 12.5 in the policy document on Electronic Money (E-Money) issued by the Bank and includes any amendments made to it from time to time.

10. The REs must report any potential SNC event via the ORR system within **1 working day** upon confirmation of the event by an officer within the control function. Please refer to **Table 3: ORR reporting types and deadlines**.

11. The event must be tabled at the SC/SA meeting within **14 working days** from the event confirmation by an officer within the control function.

12. In the event where no SC/SA meeting will be held within the 14 working day period, REs are required to conduct an ad-hoc SC/SA meeting (may consist of the minimum required quorum) specifically to deliberate on the matter.

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

Actual SNC event

14. Actual SNC event is defined as any SNC event that has been confirmed by the RE's SC/SA.

15. The REs must report any actual SNC event via the ORR system within **1 working day** from the SC/SA's confirmation date. Please refer to **Table 3: ORR reporting types and deadlines**.

16. The REs must submit to the ORR system, a rectification plan as endorsed by SC/SA and subsequently approved by the Board within **30 calendar days** from the reporting date of the actual SNC.

17. In the event there is no Board meeting that will be held within the 30-day period, REs 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.

18. REs must take appropriate remedial rectification measures or follow up measures to resolve the actual SNC and control mechanisms must be put in place to avoid recurrences. Latest facts and actions taken on the case must be updated in the ORR.

Determining loss from SNC event

19. 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 fines as stipulated in section 28(5) of IFSA and section 33D(5) of DFIA;

    (c) Restitution – Payments to third parties on account of operational losses for which the RE is legally responsible;

    (d) Loss of recourse – Losses experienced when a third party does not meet its obligations to the REs;

(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/SA.

Reporting SNC event in ORR

20. 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 10, 11 and 12** by the following stages:

(a) Detection stage

(b) Confirmation stage

(c) Rectification stage

Detection Stage

REs must report the Potential SNC in the Detection Stage at the point the Potential SNC is confirmed by an officer within the control function.

Category: Detection of Potential SNC event
Loss Event Classification: Potential SNC
Applicability: REs which are FIs and e-money issuers

Table 13: Data fields for reporting Potential SNC Detection

Data fields	Mandatory field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure • REs must select the respective reporting entity for REs under "Financial Group structure"
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as one of the following: • New • WIP • Completed

Data fields	Mandatory field	Description
		• Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report the event using ONLY the following selections: • **Level 1**: Shariah Related Matters • **Level 2**: Detection REs must report Shariah related matters in sequence based on the following: 1. Detection Stage: at the point when the potential SNC event is confirmed by an officer within the control function 2. Confirmation stage: at the point when the actual SNC event is confirmed by the SC/SA

Data fields	Mandatory field	Description
		3. Rectification stage: at the point when the rectification plan is approved by the Board and endorsed by SC/SA
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event must be stated.
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked using this function.
Loss Event Classification	Auto-generated	The reportable operational risk events will be automatically tagged as the following stage: • **Detection Stage**: **Potential event** to capture potential SNC *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes a high reputational impact based on REs' internal frameworks
Boundary Event	No	REs must categorise the operational risk event as either 'Credit', 'Market risk' or 'Not Applicable' with reference to **Appendix 11** Note: This is applicable to BIs only.
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin

Data fields	Mandatory field	Description
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss • **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc. • **Both financial and non-financial** impacts– as defined above
Financial Impact Classification	Yes	REs must select one of the following for an operational risk event with a Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for an operational risk event with a Non-Financial Impact: • Low; • Medium; or • High *Note: the non-financial impact is not confined to reputation risk, but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7*
Non-Financial Impact Justification	Yes	REs must justify the reason behind the selection of High / Medium / Low for the non-financial impact with an explanation of the related non-financial risks
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13** *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any*

Data fields	Mandatory field	Description
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Delivery Channel	Yes	Channels used to deliver the product / services of the operational risk events. **For REs <u>except</u> ITOs:** • Internet • Mobile • Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A **For ITOs only:** • Direct Clients – Walk In • Direct Clients – Internet • Direct Clients – Direct Mailing • Direct Clients – Marketing Staff • Direct Clients – Others • Telemarketing • Franchise Holders / Dealers (for GITOs only) • Registered Individual Agents • Registered Corporate Agents • E-Commerce Marketplace • Partners in Digital Platforms • Financial Advisers • Bancassurance / Bancatakaful • Co-Insurer / Co-Takaful • Insurance / Takaful Brokers • Reinsurance / Retakaful Accepted • Others (please specify)
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event.

Data fields	Mandatory field	Description
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15**
Date of Event Occurrence	Yes	The date when the event happened or took place *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Event Detection	Yes	The date the event was confirmed as a potential SNC by an officer within the control function *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Loss Event Captured in Provision Account	No	The earliest date when the operational risk loss has been accrued in suspense, reserve or provision of REs' accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date when the operational risk loss is recognised based on REs accounting framework *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved (RM)	Yes	This field must have a value to reflect the overall financial amount and/or transaction value associated with the operational risk event reported Note: This field is mandatory if Financial Impact is selected.
Loss Incurred By	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party

Data fields	Mandatory field	Description
		REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'
Loss Event Description		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • On-premise – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre. • Off-premise – occurs outside premise(s) of REs: To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working. **b) <u>For ITOs only</u>** • On premise: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service

Data fields	Mandatory field	Description
		➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance ➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • Off-premise: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster.
Number of Business Lines Affected	Yes	Only applicable for an event that affects multiple business lines. Please refer to **Appendix 2**.
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia

Data fields	Mandatory field	Description
		• **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only
How the Event Occurred?	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g. name, I/C number and other personal information
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years *Note: **All** **External** and **Internal Fraud** **LED** events must be classified as either new or repeated MO*
Modus Operandi Involved	Yes	REs must concisely define the method or manner of the reportable operational risk event occurrence. The MO involved in the LED is not limited to fraud MO. *Please refer to paragraph 17.8 for examples*

Data fields	Mandatory field	Description
Parties Involved In / Affected By The Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved/affected • Staff • Third party service provider • Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected
Number of Individual(s) Involved In / Affected by the Event	Yes	Based on the '**Parties Involved In / Affected By The Event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided, and at minimum, must include the underlying cause of the event
Shariah Related Details		
Shariah Primary Contract	Yes	REs must select only ONE primary Shariah contract applied to the product. If there are several products involved in an event, REs must select more than one main Shariah contract according to the number of products involved. The option "Others (please specify)" is meant for a transaction that does not involve any Shariah primary contract e.g. where an advertisement does not comply with Shariah requirements or transactions that involve questionable sponsorship etc.

Data fields	Mandatory field	Description
		(Note: In relation to the definition of specific Shariah contracts, please refer to the respective policy documents on Shariah contracts and Shariah ruling issued by the Bank)
Shariah Supporting Contract	Yes	REs must provide the type of secondary Shariah contract used under a particular Shariah primary contract (where applicable). If the option "Others (please specify)" is selected, REs must specify the specific contract used in the 'Shariah Supporting Contract Comments' field. *(Note: In relation to the definition of specific Shariah contracts, please refer to the respective policy documents on Shariah contracts issued by the Bank).*
Shariah Source of Detection	Yes	REs must report the source of detection of the Shariah related matters (potential SNC) e.g. Shariah Compliance Unit, Business Unit, etc.
No of Accounts / Certificates Involved	Yes	The number of accounts / certificates involved in a particular SNC event
Name of Product	Yes	REs must report the name of product impacted for Shariah related matters
Justification By The Officer Within The Control Function	Yes	Reasons for classifying the Shariah related matters as Potential SNC

Confirmation Stage

REs must update the Potential SNC to Actual SNC or non-Shariah related matter in the Confirmation Stage without any undue delay. No new LED is to be reported at the Confirmation Stage.

Category: 1. Confirmation of Actual SNC event from Potential SNC; or

2. Confirmation of non-Shariah related matter by re-classification of the reported Potential SNC to other reportable operational risk event based on **Table 3: ORR LED reporting types and deadlines**

Loss Event Classification: Actual SNC

Applicability: REs which are FIs or e-money issuers

Table 14: Data fields for reporting Actual SNC Confirmation

Data fields	Mandatory field	Description
		General
Is This LED Still A Shariah Related Event?	Yes	REs must select one of the dropdown selections below, before proceeding with the other data fields: • **Yes:** Event reported as 'actual' SNC • **No:** Event classified as non-SNC REs must select 'No' when a potential SNC reported at the detection stage is later confirmed by SC/SA to not be an actual SNC. This data field allows REs to re-classify the event from Shariah related matters to other reportable OR events. This field must be answered at the 'Confirmation Stage' reporting.
Loss Event Classification	Yes	The reportable operational risk events will be automatically tagged as the following stage: • **Confirmation Stage**: **Actual event** to capture actual SNC. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*

Data fields	Mandatory field	Description
Non-Shariah related event justification	Yes	Upon selecting 'No' for the above data field for "Is this LED still a shariah related event?", REs must provide the justification/ reason for the event to be deemed as not being a Shariah related event.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as one of the following: • New • WIP • Completed • Withdrawn • Reclassified **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Reclassified**' for potential SNC event that are reclassified to non-SNC during the confirmation stage to become '**WIP**' until all mandatory fields are filled.

Data fields	Mandatory field	Description
		8. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Yes	REs must report the event using ONLY the following selection: • **Level 1:** Shariah Related Matters • **Level 2**: Confirmation REs must report shariah related matters in sequence based on the following: 1. Detection stage: at the point when the potential SNC event is confirmed by an officer within the control function. 2. Confirmation stage: at the point when the actual SNC event is confirmed by the SC/SA. 3. Rectification stage: at the point when the rectification plan is approved by the Board and endorsed by the SC/SA.
Submission ID link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked using this function.
Impact, Business Line & Event Type		
Date of Event Confirmation	Yes	The date the event was confirmed by SC/SA as SNC or non SNC.
Date of Loss Event Captured in Provision Account	No	The earliest date when the operational risk loss has been accrued in suspense, reserve or provision of REs' accounts. (applicable if Financial Impact is selected)
Date of Loss Event Captured in P&L Account	No	The date when the operational risk loss is recognised based on REs' accounting framework. (applicable if Financial Impact is selected)
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction value associated with the operational risk event reported.

Data fields	Mandatory field	Description
Loss Incurred By	Yes	REs must identify party(ies) that incur(s) the (Actual loss or Potential loss or Insurance / Takaful Recoveries / Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party The REs must not use losses net of insurance / takaful recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field).
Shariah Related Details		
Date of Shariah Committee / Shariah Advisor Reporting	Yes	The date of the event is tabled to SC/SA for decision. Note: • The date should be before or same with data field "date of event confirmation". • The date should not be more than 14 working days from the Detection date.
Shariah Decisions	Yes	Entailing Shariah resolutions including the basis of the decision on the SNC event. The decision made by SC/SA must be distinctly documented in the minutes of the meeting.

Rectification Stage

REs are required to update the rectification plan endorsed by SC/SA and approved by the Board at the rectification stage. REs are also required to update the rectification date once the actual SNC is rectified.

Category: Actual SNC tabled to Board

Loss Event Classification: Actual SNC

Applicability: REs which are FIs or e-money issuers

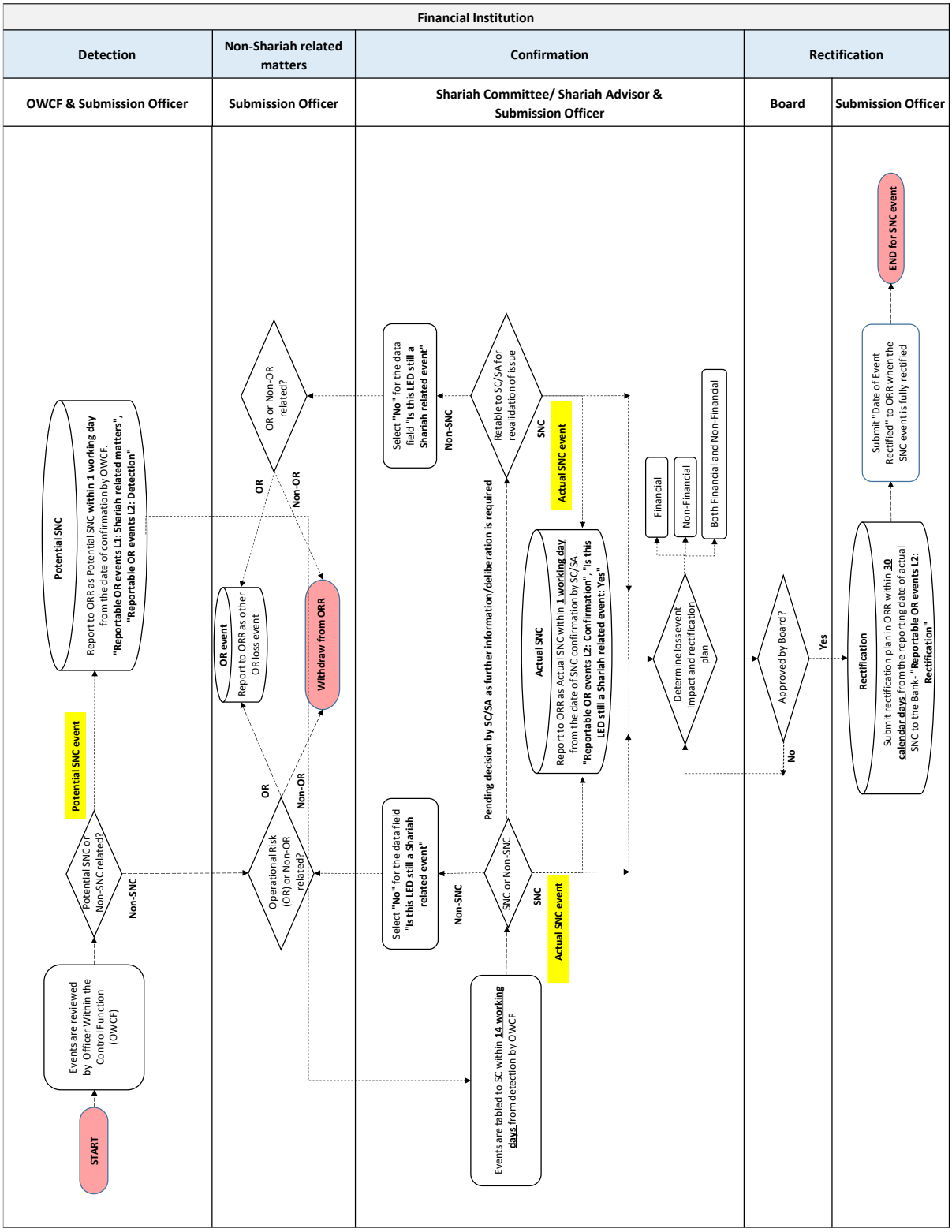
Table 15: Data fields for reporting Actual SNC Rectification

Data fields	Mandatory field	Description
		General
Loss Event Classification	Yes	The reportable operational risk events will automatically be tagged as the following stage: • **Rectification Stage**: '**Actual**' SNC event to capture rectification plan. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as one of the following: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact.

Data fields	Mandatory field	Description
		5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Yes	REs must report the event using ONLY the following selections: • **Level 1:** Shariah Related Matters • **Level 2**: Rectification REs must report Shariah related matters in sequence, based on the following stages: 1. Detection stage: at the point when the potential SNC event is confirmed by an officer within the control function. 2. Confirmation stage: at the point when the actual SNC is confirmed by the SC/SA. 3. Rectification stage: at the point when the rectification plan is approved by the Board and endorsed by the SC/SA.
Impact, Business Line & Event Type		
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction value associated with the operational risk event reported
Loss Incurred By	Yes	REs must identify party(ies) that incur(s) the (Actual loss or Potential loss or Insurance / Takaful Recoveries / Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party

Data fields	Mandatory field	Description
		The REs must not use losses net of insurance / takaful recoveries as an input to the 'Net Actual Loss' field. Instead, the recovered amount must be recorded in the 'Recovery Amount' field.
Shariah Related Details		
Rectification Action Plan	Yes	Entailing the rectification plan following SC/SA'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. Concurrently, REs must update the ORR system on the detailed rectification actions taken by REs
Attachment: Rectification Plan	Yes	To attach Board minutes on the rectification plan. The formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP
Date of Event Rectified	Yes	The date of the actual SNC is rectified based on the rectification plan approved by the Board.
Date of Board Approval	Yes	Date where the Board approved the rectification plan endorsed by SC/SA

Figure 1: Process flow for reporting SNC events



Examples of SNC event

21. Appropriate assessment has to be carried out in determining SNC events attributed to operational risk loss event types. These types of events may have potential SNC implications. The following examples are provided to illustrate the 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 must 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 facilities have been disbursed to corporate clients who are involved in entertainment and tobacco-related industries. Further review revealed that there was no due diligence conducted on the business activities during the credit approval process".
>
> **Conclusion:** The failure to investigate the clients per the guidelines led to non-compliance with the ruling issued by the 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 REs. Hence, the affected REs need to recognise this actual loss".
>
> **Conclusion:** This incident may have Shariah concerns as the subject matter i.e., the trade invoices, are not genuine, leading to non-existence of the 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 REs maintain commodity warehouses to facilitate financing transaction with customers. Nevertheless, when Shariah review team performed an on-site review, it was found that the commodity used in the financing transaction was of inferior quality due to improper maintenance of the warehouse. Further, it was found that the warehouse was affected by the recent flash flood caused by poor drainage systems. The customer has been purchasing and selling the commodity which was of lower quality and not the quality specified in the Aqad process, for financing transactions."
>
> **Conclusion:** This incident has led to a potential SNC occurrence as the customers have been transacting using commodity of inferior quality, and not what was 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 the Participant Risk Fund (PRF) which can be utilised in the event of mishap and claims made by the participants.

APPENDIX 7 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[10] must report all payment-related fraud events based on the **Table 16: Payment-related fraud types**.

2. For the payment-related fraud reporting, REs must comply with the **Table 17: Payment related fraud reporting types & thresholds.**

3. For any payment-related fraud with a new modus operandi (MO) committed and impacting REs for the first time, REs must report the said event individually, on a per transaction basis, based on the **Table 2: Operational risk information reporting deadlines.**

Table 16: Payment-related fraud types

Fraud	Type of instruments and channels	Applicability
Payment Instruments	• Credit card • Charge card • Debit card • E-money[11] • Cheque	• Issuers of credit cards, charge cards or debit cards (“card issuers”) • E-money issuers • BIs which issue cheques (“cheque issuing banks”)
Payment channels	• Internet banking • Mobile banking • Mobile payment services[12]	• BIs which offer internet banking (“Internet banking offering banks”) • BIs which offer mobile banking (“Mobile banking offering banks”)

[10] Applicable REs refer to the REs set out in Table 16.

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

[12] Mobile payment services refer to mobile payment transactions that are linked directly to a payment card account, current account or savings account (CASA) issued by banking institutions and are made via payment modes such as Near Field Communication (NFC), Magnetic Secure Transmission (MST), Quick Response Code (QR Code), proxy identifiers and other modes other than bank account numbers.

Fraud	Type of instruments and channels	Applicability
		• BIs which offer mobile payment ("Mobile payment offering banks")
Unauthorised cash withdrawal	• ATM	• REs that acquire ATM (s) to offer ATM services ("ATM acquirers")

Table 17: Payment related fraud reporting types & thresholds

Category	Sub-category	Threshold	Submission to ORR
Payment Instrument	• Credit card • Charge card • Debit card	Loss amount > RM5,000	To report the event individually on a per transaction basis
		Loss amount ≤ RM5,000	Aggregate reporting by card types (i.e. credit card, charge card and debit card) To report: • 1 event for ALL actual events with actual loss ≤ RM5,000 • 1 event for ALL actual events with potential loss ≤ RM5,000
	E-money	N/A	To report the event individually on a per transaction basis
	Cheque	N/A	To report the event individually on a per transaction basis
Payment Channels	• Internet banking • Mobile banking	N/A	To report the event individually on a per transaction basis

Category	Sub-category	Threshold	Submission to ORR
	• Mobile payment services	Loss amount > RM5,000	To report the event individually on a per transaction basis
		Loss amount ≤ RM5,000	Aggregate reporting. To report: • 1 event for ALL actual event with actual loss ≤ RM5,000 • 1 event for ALL actual event with potential loss ≤ RM5,000

Description of MO for payment-related fraud

4. REs must refer to the detailed description of MO in **Table 18** to **Table 24** when reporting loss events arising from specific payment instruments or payment channels.

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

Table 18: Card-related fraud MO

MO Level 1	MO Level 2	Description
Account Take Over		Fraudster gains access to the existing card account and uses it to make fraudulent transactions. This could happen by making a fraudulent card replacement request or a false change of address request
Counterfeit (Cloned)		Fraudster copies data from the card (typically a magnetic strip) and illegally reproduces or duplicates the card and subsequently makes fraudulent transactions
Forged Application		Fraudster applies for a card under the identity of another person and subsequently uses the card to make fraudulent transactions

MO Level 1	MO Level 2	Description
Internet	Authenticated Internet Transactions	Internet transaction that was authenticated by verifying the cardholder's password
	Unauthenticated Internet Transactions	Internet transaction where authentication was not performed or could not be performed
Mail and Telephone Order (CNP)		Card information obtained illegally and subsequently used to order goods or services through telephone or mail *CNP – Card not present
Loss or Stolen	Misplaced / Lost	Card is misplaced or lost (by accident or other means) and is subsequently used fraudulently
	Stolen	Card is stolen as a result of theft, burglary, robbery or other criminal means and is subsequently used fraudulently
Wire Tapping		Card information is 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 is subsequently used to make fraudulent transactions
Others (please specify)		Please provide details of the MO

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

Table 19: Network based e-money scheme MO

MO Level 1	MO Level 2	Description
Lost or stolen mobile devices	Lost	Mobile device is either misplaced or lost (by accident or by other means) and is subsequently used fraudulently
	Stolen	Mobile device is stolen as a result of theft, burglary, robbery or other criminal means and is used fraudulently
Stolen or compromised login credentials	Stolen	Login credentials are stolen via social engineering techniques (e.g., shoulder surfing, dumpster diving, phishing via SMS / email, customer leaks information to family and friends, etc.) and are subsequently used to access the e-money account of the customer to make payment for goods or services or to transfer funds
	Compromised	Login credentials are compromised via compromised devices or applications (e.g., malware infection, malicious software, keylogging, etc.) and are subsequently used to access the e-money account of the customer to make payment for goods or services or to transfer funds
Wire Tapping		Account information obtained illegally by tapping the telephone lines, where such information is subsequently used to make fraudulent transactions
Illegal e-money value (*also applicable to card-based e-money scheme)*	Manipulation balance	Manipulation of e-money balance such as via hacking or compromised applications/ accounts, so that the account appears to have a greater monetary value than the actual amount.
	Illegal reload/ top-up	Illegal reload or top-up by a fraudster so that the account appears to have a greater monetary value than the amount actually paid by the user
Others (please specify)		Please provide details of the MO

(c) Payment instrument: Proprietary Prepaid Card based e-money scheme MO

Table 20: Proprietary Prepaid Card based e-money scheme MO

MO	Description
Card Hacking	Unauthorised intrusion into the card's wallet balance by manipulating the balance amount (illegal reload) using publicly available software and hardware for personal use or to sell it to the public with a discounted price.
Card Cloning	Cloning is a process of using a special software and hardware where a fraudster can make a copy of one card (with Value[13] as a "template") and re-write the template onto multiple new "white cards".
Other missing reload (missing transaction sequence no.)	Missing 1 or more transaction sequences with the balance increased
Passable Blacklist	Transaction from a blacklisted card which happens due to the blacklisted parameter at the usage point not being updated.
Others (please specify)	Please provide details of the MO

[13] Refers to stored value in card-based e-money schemes

(d) Payment instrument: Cheque

Table 21: 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 a forged signature.
Alteration	A genuine cheque of which its details are illegally altered.
Others (please specify)	Please provide details of the MO

(e) Payment channel: Internet banking fraud

Any fraudulent transaction performed by a third party via internet banking services offered by any REs (including access to an internet web browser using mobile devices). Cases whereby beneficiary accounts or mule accounts are maintained at REs must 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 the ORR.

Table 22: Internet banking fraud MO

MO Level 1	MO Level 2	MO Level 3	Description
Phishing	Email	Link	An email with a malicious link, which directs the user to a malicious webpage / spoof site (e.g., login page) to steal information / credentials
		Attachment e.g., document	An email with an attachment (installed with viruses, spyware, or ransomware) to compromise the device or credentials when opened

MO Level 1	MO Level 2	MO Level 3	Description
	Fake / Malicious Website		A malicious or spoof website developed by a fraudster that looks and acts legitimately but with the intention to mislead the user to steal personal information such as via login page or viruses / malware
	Messaging services	Transaction Authorisation Code (TAC)	Messages initiated by a fraudster to steal the TAC to perform unauthorised transactions on a user's legitimate account
		Soft token	Messages initiated by a fraudster to steal the TAC via a soft token or to direct the user to approve the transaction via soft token to perform an unauthorised transaction on the user's legitimate account
		Link	A Fraudster sends text messages that contain malicious links that direct a user to a malicious webpage to steal the user’s personal information
		Messaging Applications (e.g. WhatsApp, Telegram, etc.)	A fraudster sends text messages to a user, which contains fake promises, offers or identity through a messaging application to steal personal information

MO Level 1	MO Level 2	MO Level 3	Description
		Short Messaging Service (SMS)	"Smishing" where a fraudster sends to / spams a user with fraudulent messages containing fake promises, offers or identity to steal the user's personal information
		Social Media	A fraudster sends text messages to a user, which contains fake promises or offers through social media channels (e.g., LinkedIn, Facebook, Twitter, etc.) to steal the user's personal information
	Telephone		Scam telephone calls where a fraudster steals a user's personal information by making false promises, offers, threats or pre-recorded messages (aka robocalls)
Unauthorised Internet Banking Registration			A fraudster uses stolen customer credentials for the registration of new internet banking profiles to conduct unauthorised internet banking transactions

MO Level 1	MO Level 2	MO Level 3	Description
Malware			Malicious software is unknowingly installed in customers' computers / mobile phones / other devices to ultimately obtain internet banking credentials or TACs to conduct unauthorised internet banking transactions
SIM Card Hijack			A fraudster impersonates a customer at the mobile service provider, to replace the SIM card of the registered mobile number to receive TACs in order to conduct unauthorised internet banking transactions
Browser Redirect			A fraudster uses links on search engine results to direct customers to fake internet banking websites to conduct unauthorised internet banking transactions
Others (please specify)			Please provide details of the MO

(f) Payment channel: Mobile banking fraud

Any fraudulent transaction performed by a third party on bank accounts through a mobile device via mobile banking applications (including but not limited to SMS and Unstructured Supplementary Service Data, USSD based banking platform) offered by the REs. Cases whereby beneficiary accounts or mule accounts are maintained at REs must 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 23: Mobile banking fraud MO

MO Level 1	MO Level 2	MO Level 3	Description
Phishing	Email	Link	An email with a malicious link, which directs users to a malicious webpage / spoof site (e.g., login page) to steal their information / credentials.
		Attachment e.g., document	An email with an attachment, which is installed with viruses, spyware or ransomware to compromise the device or credentials when opened.
	Fake / Malicious Mobile Application		A malicious or spoof mobile application developed by a fraudster that looks and acts legitimately but with the intention to mislead users in order for the fraudster to steal their personal information via the login page or viruses / malware.
	Messaging Services	Transaction Authorisation Code (TAC)	Messages initiated by a fraudster to steal TAC to perform unauthorised transactions on a user's legitimate account.

MO Level 1	MO Level 2	MO Level 3	Description
		Soft token	Messages initiated by a fraudster to steal TAC via a soft token or direct user to approve transaction via a soft token to perform unauthorised transactions on the user's legitimate account.
		Link	A fraudster sends text messages that contain malicious links that direct users to a malicious webpage to their steal personal information.
		Messaging Applications (e.g. WhatsApp, Telegram, etc.)	A fraudster sends text messages to users, which contain fake promises, offers or identity through a messaging application to steal their personal information.
		Short Messaging Service (SMS)	“Smishing” where a fraudster sends to / spams a user with fraudulent messages containing fake promises, offers or identity to steal the user’s personal information
		Social Media	A fraudster sends text messages to users, which contain fake promises or offers through social media channels (e.g., LinkedIn, Facebook, Twitter, etc.) to steal their personal information.

MO Level 1	MO Level 2	MO Level 3	Description
	Telephone		Scam telephone calls where a fraudster steal s users' personal information by making false promises, offers, threats or pre-recorded messages (aka robocalls).
Unauthorised Mobile Banking Registration			A fraudster uses stolen customer credentials for the registration of new mobile banking profiles to conduct unauthorised mobile banking transactions
Malware			Malicious software installed unknowingly in customers' computer / mobile phone / other devices to ultimately obtain internet banking credentials or TACs to conduct unauthorised mobile banking transactions
SIM Card Hijack			A fraudster impersonating a customer at a mobile service provider, to replace the SIM card of a registered mobile number to receive TACs in order to conduct unauthorised mobile banking transactions
Others (please specify)			Please provide details of the MO

(g) Payment channel: Mobile payment fraud

Any fraudulent transactions performed by a third party that are:

- made via mobile applications offered by a BI or a third party that is linked directly to a payment card account, current account or savings account (CASA) issued by BIs; and
- made via payment modes such as Near Field Communication (NFC), Magnetic Secure Transmission (MST), Quick Response Code (QR Code), proxy identifiers and other modes other than bank account numbers.

Examples of reportable mobile payment fraud:

(a) Fraudulent transactions performed through DuitNow QR Code using a BI's mobile applications that are linked to a customer's savings account

(b) Fraudulent transactions performed through QR Codes using a third-party mobile application that is linked to a customer's payment card account

(c) Fraudulent transactions performed through NFC/MST using a third-party mobile application that is linked to a customer's payment card account

(d) Fraudulent transactions performed through a DuitNow proxy identifier (e.g., mobile number, NRIC number) using mobile applications that is linked to a customer's savings account

Table 24: Mobile payment fraud MO

MO Level 1	MO Level 2	Description
Lost or stolen mobile devices	Lost	Mobile phone is either misplaced or lost (by accident or other means) and subsequently used fraudulently
	Stolen	Mobile phone is stolen as a result of theft, burglary, robbery or other criminal means and subsequently used fraudulently
Stolen or compromised login credentials	Stolen	Login credentials are stolen via social engineering techniques (e.g., shoulder surfing, dumpster diving, phishing via SMS / email, customer leaks information to family & friends, etc.) and is subsequently used to access the payment card account/CASA of the customer to make payment for goods or services or to transfer funds

MO Level 1	MO Level 2	Description
	Compromised	Login credentials are compromised such as via compromised devices or applications (e.g., malware infection, malicious software, keylogging, etc.) and are subsequently used to access the payment card account/CASA of the customer to make payment for goods or services or to transfer funds
Wire Tapping		Account information obtained illegally by tapping telephone lines used to make fraudulent transactions
Others (please specify)		Please provide details of the MO

Table 25: Technical Indicator applicable to frauds related to Cards, E-Money, Internet Banking & Mobile Banking, Mobile Payment Fraud and Unauthorised Cash Withdrawals

Technical Indicator	Applicable to Fraud Types
POS / Merchant compromised	• Card Fraud • E-Money Fraud • Internet Banking Fraud • Mobile Banking Fraud • Mobile Payment Fraud • Unauthorised Cash Withdrawals
RE Infrastructure Compromised	
Customer Device Compromised	
BIN Attack	
Sensitive information leaked publicly at internet	
Others (please specify)	
Phishing – Email	• Card Fraud • E-Money Fraud • Mobile Payment Fraud • Unauthorised Cash Withdrawals
Phishing – Fake Website / App	
Phishing – Messaging Service	
Phishing – Telephone	

Reporting payment-related fraud in ORR

5. **Individual Payment-related fraud events**

Table 26: Reporting guidance for individual payment related fraud events provide an overview of the reporting on individual payment related fraud events.

Table 26: Reporting guidance for individual payment related fraud events.

Category	Sub-category	Threshold	Reporting Requirement
Payment instrument	• Credit card • Charge card • Debit card	Loss amount > RM5,000	Individual event, please refer to **Tables 27 & 29.**
	E-money	N/A	Individual event, please refer to **Tables 27 & 30**
	Cheque	N/A	Individual event, please refer to **Tables 27 & 28**
Payment channels	• Internet banking • Mobile banking	N/A	• Individual event, please refer to **Tables 27 & 31** • Individual event, please refer to **Tables 27 & 32**
	• Mobile payment services	Loss amount > RM5,000	Individual event, please refer to **Tables 27 & 33**
Unauthorised cash withdrawal	N/A	N/A	Individual event, please refer to **Table 34**

REs must report the individual payment-related fraud events based on the **Tables 26** to **34**. **Table 27** lists all **generic** data fields that must be reported together with **specific** data fields for each type of payment related fraud events in **Tables 28 to 34.**

(a) Generic data fields reporting requirements for individual payment-related fraud

Category: 1. All individual payment related fraud events as provided in **Table 26**; or
2. New MO
Loss Event Classification: Actual Event and Near Miss
Applicability: REs which are BIs and payment instrument issuers.

Table 27: Generic data fields for individual payment-related fraud

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• REs must select the respective reporting entity for operational loss event *(Note: Applicable to Financial Group structure)* • Reporting entity name will be automatically displayed for a 'Single' entity
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact.

Data fields	Mandatory field	Description
		5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report individual payment related fraud event using ONLY the following selections: • **Level 1**: Fraud Event • **Level 2**: Payment Related fraud • **Level** 3: Payment Instrument -OR- Payment Channel
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event must be stated
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • Actual Event • Near Miss Event *Please refer to paragraph 16.1 for the definitions of the above-mentioned categories.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes **high** reputational impact based on REs internal framework.

Data fields	Mandatory field	Description
Boundary Event	No	REs must categorise the operational risk event as being either related to Credit, Market risk or Not Applicable with reference to **Appendix 11.** Note: This is applicable to BIs only.
Islamic Business?	Yes	REs must select 'Yes' for an event that involves Islamic products or services, which may or may not be related to shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC.
Internal Loss Event ID	No	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss; • **Non-financial impact** – No loss amount involved but there is an impact on reputation, non-compliance etc; or • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	REs must select one of the following for operational risk event with Financial Impact: • Actual Loss; or • Potential Loss

Data fields	Mandatory field	Description
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7.*
Non-Financial Impact Justification	Yes	REs to justify on the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks.
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13** *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any.*
Delivery Channel	Yes	Channels used to deliver the product / services of the operational risk events. **For REs:** • Internet • Mobile • Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event.
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15.**

Data fields	Mandatory field	Description
Date of Event Occurrence	Yes	The date on which the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date on which the REs became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Loss Event Captured in Provision Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date on which the operational risk loss is recognised based on the accounting framework of the REs. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved (RM)	Yes	This field must have a value to reflect the overall financial amount and/or transaction values associated with the reportable operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss Event Description		
Where the Event Happened?	Yes	REs must select place(s) where the incident / event occurred. Please refer to **Appendix 2.** • **On-premise** – occurs in the premise(s) of REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre

Data fields	Mandatory field	Description
		• **Off-premise** – occurs outside premise(s) of REs: To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working
Number of Business Lines Affected	Yes	Only applicable for an event that affects multiple business lines. Please refer to **Appendix 2**.
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only
How the Event Occurred	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g. name, I/C number and other personal information.
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** - For new type of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** - For OR that REs have experienced previously within the last three years.

Data fields	Mandatory field	Description
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years. *Note: **All** **External** and **Internal Fraud** **LED** events must be classified as either new or repeated MO.*
Parties Involved In / Affected By The event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. Conditionally populated; please select the relevant parties involved and the number of users involved / affected. • Customer(s) involved /affected • Staff • Third party service provider • Others (please specify)
Number of Individual(s) Involved in / Affected by the Event	Yes	Based on the '**Parties Involved In / Affected By The Event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided, and at minimum must include the underlying cause of the event.

Data fields	Mandatory field	Description
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event REs may select 'TBC' [To Be Confirmed] for remedial action plans that are not finalised during the initial reporting .
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs may input expected remediation date. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided.
Remedial Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.

Data fields	Mandatory field	Description
Mitigation Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF

(b) Specific data fields reporting requirements

Category: 1. Payment Instrument – Cheque
Loss Event Classification: Actual Event and Near Miss
Applicability: REs which are cheque issuing banks

Table 28: Specific data fields for cheque fraud

Data Fields	Mandatory field	Description
Payment Related Fraud Details		
Payment Instrument	Yes	REs must select 'Cheque'
Source of Detection	Yes	REs must select whichever applicable: • Detected by collecting bank • Detected by issuing bank • Detected by customers • Others (please specify)
Types of Cheque Issuers	Yes	REs must select whichever applicable: • Individual • Corporate • Government • Third Party • Others (please specify)
Business Activity	Yes	REs must select whichever is applicable: • Airlines or Air carriers • Travel agencies and tour operators • Telecommunication equipment including telephone sales • Utilities (electric / gas / water / sanitation) • Department stores

Data Fields	Mandatory field	Description
		• Grocery stores and supermarkets • Miscellaneous food stores • Automotive parts stores • Service stations • Automated fuel dispensers • Electronic sales • Eating places / restaurants • Bars / taverns / lounge / discos / night clubs • Jewellery / watch / clock / silverware stores • Direct marketing including insurance service / travel arrangement services / Telemarketing merchants / Subscription merchants • Insurance sales or underwriting and premiums • Lodging / hotels / motels / resorts • Professional services • Unauthorised cash withdrawals • Others (please specify)
Modus Operandi Involved	Yes	REs must select whichever applicable: • Cloning • Forgery • Alteration • Others (please specify)
Loss Incurred by Malaysian Entities	No	REs must record the loss amount incurred according to (Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries) for the following parties: • Collecting banks • Cheque issuing banks • Customers • Others (please specify) REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field)

Data Fields	Mandatory field	Description
Loss Incurred by Foreign Entities	No	REs must record the amount incurred according to Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries. REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field).

Category: 2. Payment Instrument – Card-related fraud with amount > RM5,000
Loss Event Classification: Actual Event, and Near Miss
Applicability: REs which are card issuers

Table 29: Specific data fields for card-related fraud with amount > RM5,000

Data Fields	Mandatory field	Description
Payment Related Fraud Details		
Payment Instrument	Yes	REs must select whichever is applicable: • Credit Card • Debit Card • Charge Card
Card Brands	Yes	REs must select whichever is applicable: <u>Credit card & Charge card:</u> • Visa • MasterCard • AMEX • UnionPay • Other (please specify) <u>Debit card:</u> • International debit card – Visa • International debit card – MasterCard • International debit card – Others (please specify) • E-Debit (Domestic debit, MyDebit) • Combo (Co-badge card)

Data Fields	Mandatory field	Description
Card Types	Yes	REs must select whichever is applicable: • Magnetic Stripe • Chip • Chip and PIN • Contactless • Others (please specify)
Business Activity	Yes	REs must select whichever is applicable: • Airlines or Air carriers • Travel agencies and tour operators • Telecommunication equipment including telephone sales • Utilities (electric / gas / water / sanitation) • Department stores • Grocery stores and supermarkets • Miscellaneous food stores • Automotive parts stores • Service stations • Automated fuel dispensers • Electronic sales • Eating places / restaurants • Bars / taverns / lounge / discos / night clubs • Jewellery / watch / clock / silverware stores • Direct marketing including insurance service / travel arrangement services / Telemarketing merchants / Subscription merchants • Insurance sales or underwriting and premiums • Lodging / hotels / motels / resorts • Professional services • Unauthorised cash withdrawals • Others (please specify)
Modus Operandi Involved	Yes	REs must select whichever applicable as outlined in **Table 18**
Technical Indicator	Yes	REs must select the indicator / causal of fraud occurred as shown in **Table 25**

Data Fields	Mandatory field	Description
Loss Incurred by Malaysian Entities	Yes	REs must record the amount incurred according to Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries for the following parties: • Card issuers; • Cardholders; • Acquirers / merchants; and • Others REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field)
Loss Incurred by Foreign Entities	Yes	REs must record the amount incurred according to Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries. REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field).

Category: 3. Payment Instrument – E-money
Loss Event Classification: Actual Event and Near Miss
Applicability: REs which are E-money issuers

Table 30: Specific data fields for E-money fraud

Data Fields	Mandatory field	Description
Payment Related Fraud Details		
Payment Instrument	Yes	REs must select 'E-money'
E-money Types	Yes	REs must select whichever is applicable: • Card-based – Proprietary prepaid card • Card-based – International prepaid card – Visa • Card-based – International prepaid card – MasterCard • Card-based – International prepaid card – Others (please specify) • Network-based - mobile payment • Network-based - internet (desktop/browser based)
Card Types	Yes	REs must select whichever is applicable: • Magnetic Stripe • Chip • Chip and PIN • Contactless • Others (please specify) *Note: Only applicable to card-based e-money fraud*
Business Activity	Yes	REs must select whichever is applicable: • Airlines or Air carriers • Travel agencies and tour operators • Telecommunication equipment including telephone sales • Utilities (electric / gas / water / sanitation) • Department stores • Grocery stores and supermarkets • Miscellaneous food stores • Automotive parts stores • Service stations

Data Fields	Mandatory field	Description
		• Automated fuel dispensers • Electronic sales • Eating places / restaurants • Bars / taverns / lounge / discos / night clubs • Jewellery / watch / clock / silverware stores • Direct marketing including insurance service / travel arrangement services / Telemarketing merchants / Subscription merchants • Insurance sales or underwriting and premiums • Lodging / hotels / motels / resorts • Professional services • Unauthorised cash withdrawals • Others (please specify)
Mobile Application used	Yes	REs must select whichever is applicable: • Own mobile application • Third party mobile application *Note: Only applicable to network-based mobile payment e-money fraud*
Type of Accounts Linked to The Transaction	Yes	REs must select whichever is applicable: • Transaction linked directly to payment card accounts • Transaction linked directly to saving/current accounts • Transaction linked to e-money accounts *Note: Only applicable to network-based mobile payment e-money fraud*
Types of Fraudulent Transactions	Yes	REs must select whichever is applicable: • Purchases • Bill Payments • Fund transfer (P2P) • Others (please specify) *Note: Only applicable to network-based mobile payment e-money fraud*

Data Fields	Mandatory field	Description
Types of Mobile Payment Transaction	Yes	REs must select whichever is applicable: • Near Field Communication (NFC)[14] • Magnetic Secure Transmission (MST)[15] • Quick Response Code (QR code)[16] • Proxy Identifiers[17] • Others (please specify) *Note: Only applicable to network-based mobile payment e-money fraud*
Modus Operandi Involved	Yes	REs must select whichever is applicable as outlined in **Table 19** (Network-based) and **Table 20** (Card-based)
Technical Indicator	Yes	REs must select the indicator / cause of fraud occurred as shown in **Table 25**
Loss Incurred by Malaysian Entities	Yes	REs must record the amount incurred according to Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries for the following parties: • E-money issuers • Customers; • Acquirers/ merchants; and • Others (please specify) REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field

[14] NFC is a wireless technology that allows mobile users to make payments by placing a compatible device like a smartphone or payment card within a few centimetres of another compatible device like a terminal, tablet or another smartphone.
[15] MST is mobile payment technology that emits a magnetic signal that mimics the magnetic stripe on a traditional payment card.
[16] QR code is a type of two-dimensional bar code that consists of square black modules on a white background to be read by devices such as barcode scanners and smartphones.
[17] Proxy identifiers by mobile number, NRIC number/Army number/Police number, business registration number, passport number and others.

Data Fields	Mandatory field	Description
Loss Incurred by Foreign Entities	Yes	REs must record the amount incurred according to Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries. REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field.

Category: 4. Payment Channel – Internet Banking
Loss Event Classification: Actual Event and Near Miss
Applicability: REs which offer internet banking services

Table 31: Specific data fields for internet banking fraud

Data Fields	Mandatory field	Description
Impact, Business Line & Event Type		
Payment Channel	Yes	REs must select 'Internet Banking'
Loss Incurred By	Yes	REs must identify party(ies) that incur(s) the (Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field
Payment Related Fraud Details		
Account Type	Yes	REs must select whichever is applicable: • Individual • Corporate • Others (please specify)
Type of Fraudulent Transactions	Yes	REs must select whichever is applicable: • Intrabank fund transfers • Interbank GIRO

Data Fields	Mandatory field	Description
		• Instant transfer (IBFT) • Bill payments • JomPAY • Financial Process Exchange (FPX) • RENTAS Third Party • Reload transactions • Outward remittance/TT • DuitNow - account number • DuitNow - proxy identifiers • Others (please specify)
Modus Operandi Involved	Yes	REs must select whichever is applicable as outlined in **Table 22**
Technical Indicator	Yes	REs must select the indicator / cause of fraud occurred as shown in **Table 25**

Category: 5. Payment Channel – Mobile Banking
Loss Event Classification: Actual Event and Near Miss
Applicability: REs which are mobile banking offering banks

Table 32: Specific data fields for mobile banking fraud

Data Fields	Mandatory field	Description
Impact, Business Line & Event Type		
Payment Channel	Yes	REs must select 'Mobile Banking'
Loss Incurred By	Yes	REs must identify party(ies) that incur(s) the (Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field)

Data Fields	Mandatory field	Description
Payment Related Fraud Details		
Account Type	Yes	REs must select whichever is applicable: • Individual • Corporate • Others (please specify)
Type of Fraudulent Transactions	Yes	REs must select whichever is applicable: • Intrabank fund transfers • Interbank GIRO • Instant transfer (IBFT) • Bill payments • JomPAY • Financial Process Exchange (FPX) • RENTAS Third Party • Reload transactions • Outward remittance/TT • DuitNow - account number • DuitNow - proxy identifiers • Others (please specify)
Modus Operandi Involved	Yes	REs must select whichever is applicable as outlined in **Table 23**
Technical Indicator	Yes	REs must select the indicator / cause of fraud occurred as shown in **Table 25**

Category: 6. Payment Channel – Mobile payment fraud with amount involved > RM5,000
Loss Event Classification: Actual Event and Near Miss
Applicability: REs which are Mobile payment offering banks

Table 33: Specific data fields for mobile payment fraud

Data Fields	Mandatory field	Description
Impact, Business Line & Event Type		
Payment Channel	Yes	REs must select 'Mobile Payment Services'
Payment Related Fraud Details		
Types of Fraudulent Transaction	Yes	REs must select whichever is applicable: • Purchases • Bill Payments • Fund transfer (P2P) • Others (please specify)
Types of Mobile Payment Transaction	Yes	REs must select whichever is applicable: • Near Field Communication (NFC)[18] • Magnetic Secure Transmission (MST)[19] • Quick Response Code (QR code)[20] • Proxy Identifiers[21] • Others (please specify)
Mobile Application Used	Yes	REs must select whichever is applicable: • Own mobile application • Third party mobile application

[18] NFC is a wireless technology that allows mobile users to make payments by placing a compatible device like a smartphone or payment card within a few centimetres of another compatible device like a terminal, tablet or another smartphone.
[19] MST is mobile payment technology that emits a magnetic signal that mimics the magnetic stripe on a traditional payment card.
[20] QR code is a type of two-dimensional bar code that consists of square black modules on a white background to be read by devices such as barcode scanners and smartphones.
[21] Proxy identifiers by mobile number, NRIC number/Army number/Police number, business registration number, passport number and others.

Data Fields	Mandatory field	Description
Type of Accounts Linked to the Transaction	Yes	REs must select whichever is applicable: • Transaction linked directly to payment card accounts • Transaction linked directly to saving/current accounts
Modus Operandi Involved	Yes	REs must select whichever is applicable as outlined in **Table 24**
Technical Indicator	Yes	REs must select the indicator / cause of fraud occurred as shown in **Table 25**
Loss Incurred by Malaysian Entities	No	REs must record the amount incurred according to Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries for the following parties: • Customers • Card issuers/banks where saving or current account is held • Acquirers / merchants • Other parties REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field
Loss Incurred by Foreign Entities	No	REs must record the amount incurred according to Actual loss or Potential loss or Insurance Recoveries / Non-insurance Recoveries. REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field.

Category: 7. **Unauthorised cash withdrawal**
Loss Event Classification: Actual Event or Near Miss
Applicability: REs which are ATM acquirers

(a) Examples of **unauthorised cash withdrawals** events:

Scenario 1: Unauthorised cash withdrawal using lost / cloned card (debit or credit card)

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** External Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3:** Please select the Event Types that are most relevant

(b) **Scenario 2:** Unauthorised cash withdrawal by staff from customers account by misusing his/her system access

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Internal Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3:** Please select the event types that are most relevant

Table 34: Specific data fields for unauthorised cash withdrawal

Data fields	Mandatory field	Description
General		
Reporting Entity Name	Auto-generated	• REs must select the respective reporting entity for the operational loss event *(Note: Applicable to Financial Group structure)* • RE name will be automatically displayed for a 'Single' entity
Reporting As	Auto-generated	REs will be defined based on paragraph 2

Data fields	Mandatory field	Description
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	RE must report based on the following Reportable Operational Risk Events Level 3 below: • **Level 1:** Fraud Event • **Level 2:** Payment Related Fraud • **Level 3:** Unauthorised cash withdrawal

Data fields	Mandatory field	Description
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event must be stated
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • Actual Event; or • Near Miss *Please refer to paragraph 16.1 for the definitions of the above-mentioned categories.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes **high** reputational impact based on the REs internal framework
Boundary Event	No	REs must categorise the operational risk event as being either related to Credit, Market risk or Not Applicable with reference to **Appendix 11** Note: This is applicable to BIs only.
Islamic Business?	Yes	REs must select 'Yes' for an event that involves Islamic products or services, which may or may not be related to shariah related matters Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events

Data fields	Mandatory field	Description
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss; • **Non-financial impact** – No loss amount involved but there is an impact on reputation, non-compliance etc; or • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	REs must select one of the following for operational risk event with Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact level classification: • Low; • Medium; or • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7.*
Non-Financial Impact Justification	Yes	REs to justify on the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks.
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13.**

Data fields	Mandatory field	Description
		Please refer to specific appendix that is related to the reportable OR for the specific selection, if any.
Product / Service	Yes	Must be reported based on Level 3 Business Line selection in accordance with the taxonomy in **Appendix 13**.
Delivery Channel	Yes	Channels used to deliver the product / services of the operational risk events. **For REs <u>except</u> ITOs:** • Internet • Mobile • Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event.
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15.**
Date of Event Occurrence	Yes	The date when the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date on which the REs became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Confirmation	Yes	The date on which the REs has verified or confirmed the operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*

Data fields	Mandatory field	Description
Date of Loss Event Captured in Provision Account	No	The earliest date when the operational risk loss has been accrued in suspense, reserve or provision of REs accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date when the operational risk loss is recognised based on REs accounting framework. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved (RM)	Yes	This field must have a value to reflect the overall financial amount and/or transactions value associated with the operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss Incurred By	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields.
Loss Event Description		
Where the Event Happened?	Yes	REs must select place(s) where the incident / event occurred. Please refer to **Appendix 2.** • **On-premise** – occurs in the premise(s) of the REs:

Data fields	Mandatory field	Description
		To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre. • **Off-premise** – occurs outside the premise(s) of the REs: To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working.
Number of Business Lines Affected	Yes	Only applicable for an event that affects multiple business lines. Please refer to **Appendix 2**.
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only
How the Event Occurred?	Yes	1. General operational risk event: An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g., Name, I/C number and other personal information 2. Aggregate operational risk event: For further description and reporting format on aggregate reporting, please refer to the appendices

Data fields	Mandatory field	Description
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years *Note: **All External** and **Internal Fraud LED** events must be classified as either new or repeated MO*
Parties Involved In / Affected By The Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved /affected • Staff • Third party service provider • Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number of Individual(S) Involved In /	Yes	Based on the '**Parties Involved in / Affected By The Event**' selection,

Data fields	Mandatory field	Description
Affected by the Event		REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided, at minimum must include the underlying cause of the event.
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event REs may select 'TBC' [To Be Confirmed] for remedial action plans that are not finalised during the initial reporting .
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs may input expected remediation date. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided.
Remedial Action Plan Attachment	No	An attachment is optional, and the format allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of

Data fields	Mandatory field	Description
		recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.
Mitigation Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF
Unauthorised Cash Withdrawal Details		
Payment Instrument	Yes	REs must select whichever is applicable: • Credit Card • Debit Card • Charge Card
Card Brands	Yes	REs must select whichever is applicable: <u>Credit card & Charge card:</u> • Visa • MasterCard • AMEX • UnionPay • Other (please specify) <u>Debit card:</u> • International debit card – Visa

Data fields	Mandatory field	Description
		• International debit card – MasterCard • International debit card – Others (please specify) • E-Debit (Domestic debit, MyDebit) • Combo (Co-badge card)
Card Types	Yes	REs must select whichever applicable: • Magnetic Stripe • Chip • Chip and PIN • Contactless • Others (please specify)
Modus Operandi Involved	Yes	REs must select whichever is applicable as outlined in **Table 18**.
Technical Indicator	Yes	REs must select the indicator / cause of fraud occurred as shown in **Table 25.**

6. Aggregate reporting requirements for payment-related fraud ≤ RM5,000

Table 35 provides an overview of the aggregate reporting for payment related fraud events ≤ RM 5,000.

Table 35: Reporting guidance for aggregate payment related fraud events.

Category	Sub-category	Threshold	Reporting Requirement
Payment Instrument	• Credit card • Charge card • Debit card	Loss involved ≤ RM5,000	Aggregate event, please refer to **Tables 36 and 37**.
Payment channel	Mobile payment services	Loss involved ≤ RM5,000	Individual event, please refer to **Tables 36 and 38**.

REs must report the aggregate payment-related fraud ≤ RM5,000 events based on the **Tables 36 to 35**. **Table 36** lists all **generic** data fields that must be reported together with **specific** data fields for each type of payment related fraud events in **Tables 37** and **38**.

(a) Generic data fields for aggregate payment-related fraud

Category: 1. Card fraud and mobile payment services fraud with amount involved ≤ RM 5,000
Loss Event Classification: Actual Event
Applicability: REs which are card issuers or mobile payment offering banks

Table 36: Generic data fields for aggregate payment-related fraud

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• REs must select the respective reporting entity for operational loss event *(Note: Applicable to Financial Group structure)* • Reporting entity name will be automatically displayed for a 'Single' entity
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact.

Data fields	Mandatory field	Description
		5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report aggregate payment related fraud event using ONLY the following selections: • **Level 1**: Fraud Event • **Level 2**: Payment Related fraud • **Level 3**: Aggregate card fraud with loss amount ≤ RM5,000 -OR- Aggregate mobile payment fraud with loss amount ≤ RM5,000
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	For "Aggregate Card Fraud with Amount ≤ RM5,000, REs must choose the loss event name from the following: • Aggregate Credit Card Fraud • Aggregate Debit Card Fraud • Aggregate Charge Card Fraud For "Aggregate Mobile Payment Fraud with Amount ≤ RM5,000, the loss event name is auto-generated as "Aggregate Mobile Payment Fraud".
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function.

Data fields	Mandatory field	Description
Loss Event Classification	Yes	The reportable operational risk event must be classified as the following: • Actual Event *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
Internal Loss Event ID	No	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss; or • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	REs must select one of the following for operational risk events with Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk events with Non-Financial Impact level classification:

Data fields	Mandatory field	Description
		• Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7.*
Non-Financial Impact Justification	No	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks.
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13.** *Please refer to the specific appendix that is related to the reportable OR for the specific selection, if any.*
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event.
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15.**
Month of Event Occurrence	Yes	The month when the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Month of Event Detection	Yes	The month on which the RE became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Month of Confirmation	Yes	The month on which the REs has verified or confirmed the operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Month of Loss Event Captured	No	The month when a loss has been accrued in suspense, reserve or provision account

Data fields	Mandatory field	Description
in Provision Account		when the operational loss was first recognised in the RE's P&L accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Month of Loss Event Captured in P&L Account	No	The month when a loss is recognised in the REs P&L account. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Amount Involved (RM)	Yes	This field must have a value to reflect the overall financial amount and/or transactions value associated with the operational risk event reported.
Loss Event Description		
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only
Nature of Event	Yes	Reportable operational risk events must be classified as follows: • **Repeated** – For OR that REs have experienced previously within the last three years
Sub Nature of Event	Auto-generated	Reportable operational risk events must be classified as follows: • **Repeated MO –** For MO that REs have experienced previously within the last three years *Note: **All External** and **Internal Fraud LED** events must be classified as repeated MO*

(b) Specific data fields reporting requirements

Category: 1. Card-related fraud with amount involved ≤ RM 5,000
Loss Event Classification: Actual Event
Applicability: REs which are card issuers

Table 37: Specific data fields for card-related fraud with amount involved ≤ RM 5,000

Data Fields	Mandatory field	Description
Payment Related Fraud Details		
Aggregated loss and number of transactions by MO	Yes	REs must record the amount of losses incurred by Malaysian entities and foreign entities and the number of transactions according to the MO
Amount of losses and number of transactions by card brand	Yes	REs must record the amount of losses and number of transactions according to the brand of the card
Amount of losses and number of transactions by card type	Yes	REs must record the amount of losses and number of transactions by according to the type of the card (i.e., credit card, charge card or debit card)

Category: 2. Mobile payment fraud with amount involved ≤ RM 5,000
Loss Event Classification: Actual Event
Applicability: REs which are card issuers

Table 38: Specific data fields for mobile payment fraud with amount involved ≤ RM 5,000

Data Fields	Mandatory field	Description
Payment Related Fraud Details		
Aggregated loss and number of transactions by modus operandi	Yes	REs must record the amount of losses incurred by Malaysian entities and foreign entities and the number of transactions according to the MO
Amount of losses and number of transactions by types of mobile	Yes	REs must record the amount of losses and number of transactions according to the types of mobile payment transactions

Data Fields	Mandatory field	Description
payment transactions		
Amount of losses and number of transactions by types of fraudulent transactions	Yes	REs must record the amount of losses and number of transactions according to the types of fraudulent transactions
Amount of losses and number of transactions by types of accounts linked to the transactions	Yes	REs must record the amount of losses and number of transactions according to the types of accounts linked to the transactions

APPENDIX 8 Counterfeit Notes & Coins event reporting requirements

1. Counterfeit Malaysian Currency is defined as an imitation of any Malaysian Currencies. The counterfeit currencies consist of currency notes and coins that are printed, minted, forged or imitated with intention to deceive or defraud its recipient.

2. BIs are required to report all suspected counterfeit Malaysian currency notes and coins as fraud cases, irrespective of the event type in ORR system, under the following scenarios:

   (a) Critical Business Disruption and System Failure (BDSF); and

   (b) Physical Cash Shortage due to counterfeit notes and coins discovered over-the-counter and by outsourced service providers.

3. REs are required to report any discovery of suspected counterfeit Malaysian currency in the deposit-accepting Self-Service Terminals (SSTs) i.e. the Cash Deposit Machine (CDM) and Cash Recycler Machine (CRM) under critical BDSF only.

4. REs are required to report any discovery of suspected counterfeit Malaysian currency under Physical Cash Shortage at:

   (a) Branches (i.e. over-the-counter (OTC) service and/or internal currency processing); and

   (b) Outsourced cash-in-transit (CIT) vendor (i.e. currency processing centre of the Currency Processing Company).

5. REs are required to provide the following information for each operational risk event as guided in **Table 39** below for:

   (a) Discovery of suspected counterfeit Malaysian currency in deposit-accepting SSTs; and

   (b) discovery of suspected counterfeit Malaysian currency at RE's over-the-counter and outsourced CIT vendor.

Table 39: Counterfeit Notes & Coins reporting types and threshold

Category	Sub-category	Submission to ORR
Physical Cash Shortage	**Individual event for BDSF** due to counterfeit notes and coins accepted by deposit-accepting SSTs.	To submit loss events individually
	Aggregate by **External Fraud** due to counterfeit notes and coins discovered over-the-counter or by CIT vendors.	To submit loss events on an aggregated basis

Reporting a counterfeit note / coin accepted via SST event via ORR system

Category: Counterfeit notes / coins accepted via SST
Loss Event Classification: Actual Event
Applicability: BIs

6. Example of counterfeit notes / coins accepted via SST:

Scenario 1: RE's CIT vendor discovered one piece of RM50 counterfeit note in the CDM machine during end-of-day cash processing

- **Loss Event Classification:** Actual Event
- **Event Type Level 1:** Business disruption and system failures
- **Event Type Level 2:** System
- **Event Type Level 3:** Software – Application system bug / unpatched or event type level 3 that is most relevant

Table 40: Data fields for counterfeit notes / coins accepted via SST

Data Fields	Mandatory Field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure • REs must select the respective reporting entity for REs under "Financial Group structure"
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values.

Data Fields	Mandatory Field	Description
		3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk Event in **Table 3: ORR LED reporting types and deadlines** • **Level 1** – Critical event • **Level 2** – Technology related • **Level 3** – Critical BDSF – For counterfeit notes/ coins accepted via SSTs
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Auto-generated	Loss event name for this reportable OR is auto-generated as below: '**Suspected Counterfeit Malaysian Currency accepted via SST'**

Data Fields	Mandatory Field	Description
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked using this function
Loss Event Classification	Auto-generated	Discovery of suspected counterfeit currency accepted by SSTs should be reported as **Actual Event.** *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes **high** reputational impact based on REs internal framework
Islamic Business?	Yes	REs must select 'Yes' for an event that involves Islamic products or services, which may or may not be related to shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin
Impact, Business Line and Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual financial loss • **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc.

Data Fields	Mandatory Field	Description
		• **Both financial and non-financial impacts** – There is actual financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Auto-generated	Discovery of suspected counterfeit currency accepted by SSTs should be reported as **Actual Loss**
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk events with Non-Financial Impact level classification: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7*
Non-Financial Impact Justification	Yes	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Types of SST	Yes	REs must select from the following SSTs: • CDM (Cash Deposit Machine) • CRM (Cash Recycler Machine)
Business Lines	Auto-generated	REs must select: • **Level 1**: Retail Banking • **Level 2:** Retail Banking • **Level 3**: Deposits
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Event Types	Yes	For counterfeit notes accepted by Self-Service Terminals • **Level 1:** BDSF • **Level 2:** System

Data Fields	Mandatory Field	Description
		• **Level 3:** Software - Application issues or event type level 3 that is most relevant
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15**
Date and Time of Event Occurrence	Yes	The date and time the reportable operational risk event took place. *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Event Detection	Yes	The date on which the REs became aware of the event *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Event Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event *Please refer to paragraph 16.2 for the definition of the mentioned date*
Date of Loss Event Captured in P&L Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in Provision Account	No	The date on which the operational risk loss is recognised based on the accounting framework of the REs *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction values associated with the reportable operational risk event reported. Note: This field is mandatory if Financial Impact is selected

Data Fields	Mandatory Field	Description
Loss Incurred by	Yes	REs must identify party(ies) that incur(s) the (Actual loss or Potential loss or Recoveries / Insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field
Loss Event Disruption		
Where the event happened?	Yes	REs must select the place where the incident / event occurred. Please refer to **Appendix 2** • **On-premise** – occurs in REs premise(s): To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside REs premise(s) To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working
Number of Business Lines Affected	Yes	To provide the number of affected business lines. **For banking**: by Business Line Level 1
How the event occurred?	Yes	General operational risk event: An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g., Name, I/C number and other personal information.

Data Fields	Mandatory Field	Description
Nature of Event	Yes	Operational risk events must be classified as either one of the following: • **New** - For new types of OR impacting the REs for the first time in the last three years or for OR that re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** - For OR that REs have experienced previously within the last three years
Sub-nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years *Note: **All External** and **Internal Fraud LED** events must be classified as either new or repeated MO*
Modus operandi involved	Yes	REs must concisely define the method or manner of the reportable operational risk event occurrence. The MO involved in the LED is not limited to fraud MO. *Please refer to paragraph 17.8 for examples*
Parties involved in / affected by the event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved /affected • Staff • Third party service provider • Others (please specify)

Data Fields	Mandatory Field	Description
		Conditionally populated; please select the relevant parties involved and the number of users involved / affected
Number of individual(s) involved in / affected by the event	Yes	Based on the '**Parties involved in / affected by the event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Description of Consequence to Users	Yes	Description of he even impact to the respective parties involved
Root cause of the event	Yes	A detailed explanation on the factors leading to the event must be provided, and at minimum must include the underlying cause of the event
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event REs may select 'TBC' [To Be Confirmed] for remedial action plans that are not finalised during the initial reporting
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs must select 'TBC'. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided

Data Fields	Mandatory Field	Description
Remedial Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP
Reason (If Unresolved)	No	Justification(s) for delay(s) in resolving the operational risk event. E.g., The event root cause has been identified, however, the system / application impacted is yet to be resolved due to pending components from the vendor. Only applicable for events that are yet to recover.
Target Completion Date (If Unresolved)	No	REs must specify the target completion dateline to resolve the remedial action plans.
Mitigation action plans	Yes	A detailed explanation must be provided for the solutions to the underlying operational risk event and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'to be confirmed' for mitigation action plan that has yet to be confirmed during the initial reporting
Mitigation action implementation date	Yes	The date of mitigation action plan is implemented
Mitigation action plan attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF
Tech Related Details		
IT-related categories	Yes	REs must select one or more relevant categories of IT-related event of the following: -

Data Fields	Mandatory Field	Description
		• **AI** – Artificial Intelligent (AI) based application • **3rd Party** – Management of application / service(s) is procured / outsourced from / to external parties • **Hardware** – Physical server and / or devices • **Software** – System and / or application
RE Loss Event Severity	Yes	REs must provide its own internal event severity for each technology-related event reported in ORR
Consequence to Technology Operation	Yes	REs must select one or more types of impact to their IT infrastructure / technology operations of the following: • System / Service Unavailability • System Performance Degradation • Network Disruptions • Others
Description of Consequence to Technology Operation	Yes	REs must describe the event impact to their IT infrastructure, technology and/ or business operations
System Involved/ Impacted?	Yes	Only applicable for an event that has affected IT system REs must select one of the following for OR event with / without system involvement or impact: • Yes • No
System Involved/ Impacted (Name)	Yes	REs must select the name of the affected system(s). Applicable upon 'System Involved / Impacted' is selected
System Involved/ Impacted (Type)	Yes	REs must select one or more affected systems as the following: • SSTs

<table>
<tr><th>Data Fields</th><th>Mandatory Field</th><th>Description</th></tr>
<tr><td></td><td></td><td>• Others (please specify)

Applicable upon ‘System Involved / Impacted’ is selected</td></tr>
<tr><td>System Cumulative Event Duration (In Minutes)</td><td>Yes</td><td>REs must indicate the duration of event in minutes for each service.

If this event does not result in system / network outage or performance degradation, please indicate ‘0’.

If the event has yet to recover, REs must state the duration (from event occurrence until reporting date) and update it as and when the system has been restored.</td></tr>
<tr><td>Details of Counterfeit Notes/Coins Acceped via SST</td><td>Yes</td><td>REs must provide the following details based on the location where the counterfeit notes/coins were accepted as below:

• Branch SSTs

<table>
<tr><th>PDRM Report Number</th><th>No. of transactions</th><th>Notes/ Coins</th><th>Denomination</th><th>No. Of pieces</th><th>Serial Number (notes)</th><th>Country</th><th>State</th><th>District</th></tr>
<tr><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
</table>

• Offsite SSTs

<table>
<tr><th>PDRM Report Number</th><th>No. of transactions</th><th>Notes/ Coins</th><th>Denomination</th><th>No. Of pieces</th><th>Serial Number (notes)</th><th>Country</th><th>State</th><th>District</th></tr>
<tr><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
</table>
</td></tr>
</table>

Aggregate reporting requirement for counterfeit notes / coins via ORR system

Category: Physical cash shortages due to counterfeit notes / coins discovered at branch, over-the-counter and / or outsourced CIT vendor for offsite SSTs.
Loss Event Classification: Actual Event
Applicability: Banking Institutions

7. Example cash shortages due to counterfeit notes / coins at branch, over-the-counter and / or outsourced CIT vendor for offsite SST:

Scenario 1: A branch teller discovered two pieces of counterfeit notes during the end of day balancing

Scenario 2: A branch officer detected one piece of counterfeit note from the bundle received from the outsourced CIT vendor

- **Event Classification**: Actual Event
- **Event Type Level 1:** External Fraud
- **Event Type Level 2**: Theft and Fraud
- **Event Type Level 3:** Forgery / Counterfeit (Cover Notes, Policy Certificates, Currency, Cheque, Security Documents / Identification documents)

Table 41: Data fields for physical cash shortages due to counterfeit notes / coins discovered at branch, over-the-counter and / or outsourced CIT vendor for offsite SSTs.

Data Fields	Mandatory Field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure • REs must select the respective reporting entity for REs under "Financial Group structure"
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed

Data Fields	Mandatory Field	Description
		• Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk Event Level 3 in **Table 3: ORR LED reporting types and deadlines** • **Level 1** – Other loss event • **Level 2** – Aggregate Physical cash shortages • **Level 3** – Due to counterfeit notes/coins discovered through over-the-counter & by outsourced service provider
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.

Data Fields	Mandatory Field	Description
Loss Event Name	Auto-generated	Loss event name for this reportable OR is auto-generated as below: **'Aggregated Physical Cash Shortages Due to Counterfeit Notes/Coins Discovered Through Over-the-Counter & By Outsourced Service Provider'**
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3: ORR LED reporting types and deadlines**, the multiple LEDs must be linked by using this function
Loss Event Classification	Auto-generated	Only **Actual Event** with Actual Loss. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin
Impact, Business Line and Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual financial loss • **Both financial and non-financial** – as defined above
Financial Impact Classification	Auto-generated	Discovery of suspected counterfeit currency accepted by SSTs should be reported as **Actual Loss**
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact level classification: • Low • Medium • High

Data Fields	Mandatory Field	Description
		Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7
Non-Financial Impact Justification	No	REs must justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Business Lines	Auto-generated	REs must select: • **Level 1**: Retail Banking • **Level 2**: Retail Banking • **Level 3**: Deposits *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any*
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in Appendix 13.
Event Type	Auto-generated	REs must categorise the event as follows: <u>For counterfeit notes discovered through over-the-counter and during internal processing and/or by the outsourced service provider</u> • **Level 1**: External Fraud • **Level 2:** Theft and fraud • **Level 3:** Forgery/ Counterfeit
Causal Categories	Yes	REs must select the causal category that is most relevant to the event type up to Level 3 in accordance with the taxonomy in **Appendix 15**
Month of Event Occurrence	Yes	The month to represent the aggregate reportable operational risk events which took place in a particular month
Month of Event Detection	Yes	The month to present the aggregate reportable operational risk events which were detected in a particular month
Month of Event Confirmation	Yes	The month to represent the aggregate reportable operational risk events confirmed in a particular month

Data Fields	Mandatory Field	Description
Month of Loss Event Captured in Provision Account	No	Select date of the month to represent the date where provision (Potential Loss) is affected in Provision account for the overall events
Month of Loss Event Captured in P&L Account	No	The month to represent the aggregate reportable operational risk events captured as Actual loss in P&L account
Amount Involved	Yes	This field must have a value to reflect the overall **aggregated** financial amount and/or transaction value associated with the operational risk event reported
Loss incurred by	Yes	REs must identify party(ies) that incur(s) the (Actual loss or Insurance Recoveries / Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field
Loss Event Disruption		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: • **On-premise** – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside premise(s) of the REs: To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working
Number of Business Lines Affected	Yes	To provide the number of affected business lines. **For banking**: by Business Line Level 1

Data Fields	Mandatory Field	Description
Nature of Event	Auto-generated	Operational risk events must be classified as follows: • **Repeated -** For OR that REs have experienced previously within the last three years
Sub Nature of Event	Auto-generated	For all External and Internal Fraud, LED events must be classified as follows: • **Repeated MO -** For MO that REs have experienced previously within the last three years
Modus Operandi Involved	Yes	REs must concisely define the method or manner of the reportable operational risk event occurrence. The MO involved in the LED is not limited to fraud MO. *Please refer to paragraph 17.8 for examples*
Parties Involved Involved In / Affected by the Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved /affected • Staff • Third party service provider • Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number of Individual(s) Involved In / Affected by the Event	Yes	Based on the '**Parties involved in the event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided and at minimum, must include the underlying cause of the event.

<table>
<tr><th>Data Fields</th><th>Mandatory Field</th><th>Description</th></tr>
<tr><td colspan="3">Aggregate Reporting Details</td></tr>
<tr><td>Details of Counterfeit Notes/Coins by Location</td><td>Yes</td><td>REs must use this table below to report counterfeit notes and coins by location:
Over-the-Counter
Branch Cash Processing
Outsourced CIT vendor
Others (please specify)
<table>
<tr><th>Location</th><th>No. of transactions</th><th>Denomination</th><th>No. of pieces</th><th>Notes / Coins</th><th>Serial Number (notes)</th><th>PDRM Report Number</th><th>Country</th><th>State</th><th>District</th></tr>
<tr><td>OTC</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>Branch</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>CIT vendor</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
</table>
*Note: including events where losses were absorbed by outsourced vendors</td></tr>
</table>

APPENDIX 9 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; or

   (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 referred to as opportunistic fraud. This type of fraud occurs where a policyholder / participant / claimant exaggerates an otherwise legitimate claim. For example, when involved in a collision, an insured person / 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, either wholly or partly, or is 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; or

   (e) fake / tempered policy document / takaful contract, policy schedule, claims documents or reports.

7. Paragraphs 5 and 6 contain fraud illustrations as a guide to insurers and takaful operators. As insurance / takaful fraud can take place in various forms with different modus operandi, ITOs must 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) Premium Avoidance: Avoid paying equitable premium / contribution for risk proposed to be assumed.

   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 conditions which would have resulted in a 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 an 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:

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

(ii) 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 holds out to be a branch or representative office of a licensed insurer or takaful operator; or impersonates 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 to. In other instances, this may be done through the creation of a "fictitious" agency which is actually owned by the employee to earn commissions; or

(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 the 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 claims 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 would not otherwise be 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 reports to the insurer / takaful operator. Collaborators to a 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 an organised crime syndicate:

These are planned accidents normally orchestrated by organised crime syndicates. Accidents are usually pre-planned manoeuvres which involve self-inflicted accidents and at times, involve 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; or

(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; or

(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 10 Other Reportable Operational Risk Event Reporting Requirements

Aggregate Operational Risk Event Reporting Requirements - Non-payment related fraud and non-fraud events

1. REs must submit aggregate reporting to ORR system in accordance with the requirements and timeline set out in **Table 3: ORR LED reporting types and deadlines.**

2. REs must report aggregate events in accordance with the categories and threshold specified in **Table 42: Aggregate reporting types and threshold**.

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

Table 42: Aggregate reporting types and threshold

Category	Sub-category	Aggregate threshold	Aggregate submission to ORR
Aggregate Actual events with actual loss ≤ RM 1,000	Aggregate by event types for non-payment related fraud events: • Internal fraud • External fraud	Actual loss ≤ RM1,000	To submit: 1 submission for actual loss per event type
	Aggregate by other event types excluding fraud events: • Execution, delivery and process management (EDPM) • Employment practices and workspace safety (EPWS) • Damage to physical assets (DPA) • Business disruption and system failure (BDSF) • Clients, products and business practices (CPBP)	Actual loss ≤ RM1,000	

Category	Sub-category	Aggregate threshold	Aggregate submission to ORR
Aggregate Physical Cash Shortage	Aggregate by event types: • **EDPM:** Due to execution error • **CPBP:** Due to penalties on currency shortages / excess • **External Fraud**: Due to counterfeit notes / coins discovered over-the-counter and by outsourced service providers. **Please refer to appendix 8.** • **BDSF:** For counterfeit notes/ coins accepted via SST. **Please refer to appendix 8**.	N/A	To submit: 1 submission for each type of physical cash shortage at both branch and vendor

4. **Aggregate reporting for non-payment related fraud events ≤ RM 1,000**

Category: Non-payment related fraud events with actual loss ≤ RM 1,000 for:

1. Internal Fraud; or
2. External Fraud

Sub-category: Aggregate by event types
Loss Event Classification: Actual Event with Actual Loss
Applicability: All REs

(a) Examples of non-payment related fraud events ≤ RM 1,000:

Internal Fraud

Scenario 1: Teller embezzles petty money from branch account into his/her account

Scenario 2: RE's staff colludes with a vendor to create a fake invoice totalling to RM 950 for a service not rendered

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Internal Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3:** Please select the Event Types that are most relevant

External Fraud

Scenario 1: A fraudster forged documents to obtain financing facilities of RM 1,000

Scenario 2: A fraudster falsified insurance claim / premium to exaggerate travel insurance claim amounted to RM 800

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** External Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3**: Please select the Event Types that are most relevant

Table 43: Data fields for reporting non-payment related fraud events with aggregate actual loss ≤ RM 1,000

Data Fields	Mandatory Field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values.

Data Fields	Mandatory Field	Description
		3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 1. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3: ORR LED reporting types and deadlines** • **Level 1:** Fraud Event • **Level 2:** Non-payment Related Fraud Event • **Level 3:** Aggregate Actual Loss Event ≤ RM1,000
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	REs must select to report based on the dropdown below: • Aggregated ≤ RM 1,000 Internal Fraud • Aggregated ≤ RM 1,000 External Fraud
Submission ID Link	No	For LED which impacts two or more reportable operational risk events based on Table 3, the multiple LEDs must be linked by using this function
Loss Event Classification	Auto-generated	Only **Actual Event** with Actual Loss.

Data Fields	Mandatory Field	Description
		Please refer to paragraph 16.1 for the definition of the above-mentioned category.
Boundary Event	No	REs must categorise the reportable operational risk event as being related to either Credit risk, Market risk or Not Applicable with reference to **Appendix 11**. Note: This is applicable to BIs only.
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact –** There is an actual financial loss • **Both financial and non-financial** – There is actual / potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Auto-generated	This data field is auto-generated as **Actual Loss.**
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk events with Non-Financial Impact level classification: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7*

Data Fields	Mandatory Field	Description
Non-Financial Impact Justification	No	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Business Lines	Yes	Since this is an aggregate report, please select the business lines that are most affected. Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 13**
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Event Types	Yes	**Level 1:** Auto-generated according to the Loss Event Name selected in the General tab either: • External Fraud; or • Internal Fraud **Level 2**: Since this is an aggregate report, please select the Event Types that are most relevant **Level 3:** Since this is an aggregate report, please select the Event Types that are most relevant
Causal Categories	Yes	Please select the causal category that is most relevant to the event type up to Level 3 in accordance with the taxonomy in **Appendix 15**
Month of Event Occurrence	Yes	The month to represent the aggregate reportable operational risk events took place in a particular month.
Month of Event Detection	Yes	The month to present the aggregate reportable operational risk events which were detected in a particular month.
Month of Event Confirmation	Yes	The month to represent the aggregate reportable operational risk events confirmed in a particular month.
Date of Loss Event Captured in Provision Account	No	Select month date to represent the date where provision (Potential Loss) is affected

Data Fields	Mandatory Field	Description
		in the Provision account for the overall events.
Date of Loss Event Captured in P&L account	No	The month to represent the aggregate reportable operational risk events captured as Actual loss in P&L account.
Amount Involved	Yes	This field must have a value to reflect the overall **aggregated** financial amount and/or transactions value associated with the operational risk event reported.
Loss incurred by	Yes	REs must identify party(ies) that incur(s) the (Gross Actual loss or Insurance Recoveries or Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields.
Loss Event Description		
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.

Data Fields	Mandatory Field	Description
Nature of Event	Auto-generated	Reportable operational risk events will automatically be classified as the following: **Repeated** - For event that REs have experienced previously within the last three years.
Sub Nature of Event	Auto-generated	All aggregated fraud events < RM 1,000 must be classified as follows: **Repeated MO** - For MO that REs have experienced previously within the last three years.
Non Payment Related Fraud Details		
Event Type Level 1	Auto-generated	Auto-generated based on the Loss Event Name.
Amount	Yes	The loss amount for the event must be the same as the 'Net Actual Loss' in 'Loss Incurred By' table.
Number of Transactions	Yes	To specify total number of transactions reported under this aggregated reporting for the selected Event Type Level 1. *Please refer to **Appendix 2**.*
Number of Customers Impacted	Yes	To specify total number of customers impacted reported under this aggregated reporting for the selected Event Type Level 1. *Please refer to **Appendix 2**.*

5. Aggregate reporting for non-fraud events with actual loss ≤ RM 1,000 by Event Type Level 1

Category: Actual non-fraud events with actual loss ≤ RM 1,000 for:

1. Employment practices and workspace safety
2. Damage to physical assets
3. Business disruption and system failure
4. Clients, products and business practices
5. Execution, delivery and process management

Sub-category: Aggregate by event types
Loss Event Classification: Actual Event with Actual Loss
Applicability: All REs

(a) Examples of actual non-fraud events with actual loss ≤ RM 1,000:

Scenario 1: Dealer wrongly input incorrect FX rate causing RM 900 loss to reinstate customer's position

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Execution, delivery and process management
- **Event Type Level 2:** Transaction capture, execution and maintenance
- **Event Type Level 3:** Data entry or maintenance or loading

Scenario 2: Vandalism act to RE's premise (glass door)

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Damage to physical assets
- **Event Type Level 2:** Natural disaster & other losses
- **Event Type Level 3:** Human Losses – Vandalism

Table 44: Data fields for reporting actual non-fraud events with actual loss ≤ RM 1,000

Data Fields	Mandatory Field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 7. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 8. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 9. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 10. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 11. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 12. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be

Data Fields	Mandatory Field	Description
		changed back to **'Completed'** upon updating the details. 13. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Yes	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3**: • **Level 1:** Other Loss Event • **Level 2:** Other than Fraud Event • **Level 3:** Other Aggregate Actual Loss Event ≤ RM1,000
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	REs must select based on the dropdown below: • **Aggregated ≤ RM 1,000** Business disruption and system failure (BDSF) • **Aggregated ≤ RM 1,000** Clients, products and business practices (CPBP) • **Aggregated ≤ RM 1,000** Damage to physical assets (DPA) • **Aggregated ≤ RM 1,000** Employment practices and workspace safety (EPWS) • **Aggregated ≤ RM 1,000** Execution, delivery and process management (EDPM)
Submission ID Link	No	For LED which impacts two or more reportable operational risk events based on Table 3, the multiple LEDs must be linked by using this function
Loss Event Classification	Auto-generated	Only **Actual Event** with Actual Loss. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*

Data Fields	Mandatory Field	Description
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact –** There is an actual financial loss • **Both financial and non-financial** – There is actual / potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Auto-generated	This data field is auto-generated as **Actual Loss.**
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk events with Non-Financial Impact level classification: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7*
Non-Financial Impact Justification	No	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks

Data Fields	Mandatory Field	Description
Business Lines	Yes	Since this is an aggregate report, please select the business lines that are most affected. Must be reported up to Level 3 **Appendix 13.**
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Event Types	Yes	**Level 1:** This field will be auto-generated based on the Loss Event Name selection: • Employment practices and workspace safety • Damage to physical assets • Business disruption and system failure • Clients, products and business practices • Execution, delivery and process management **Level 2:** Since this is an aggregate report, please select the Event Types that are most relevant **Level 3:** Since this is an aggregate report, please select the Event Types that are most relevant
Causal Categories	Yes	Please select the causal category that is most relevant to the event type up to Level 3 in accordance with the taxonomy in **Appendix 15.**
Month of Event Occurrence	Yes	The month to represent the aggregate reportable operational risk events took place in a particular month.
Month of Event Detection	Yes	The month to present the aggregate reportable operational risk events were detected in a particular month.
Month of Event Confirmation	Yes	The month to represent the aggregate reportable operational risk events confirmed in a particular month.

Data Fields	Mandatory Field	Description
Month of Loss Event Captured in Provision Account	No	Select month date to represent the date where provision (Potential Loss) is affected in Provision account for the overall events.
Month of Loss Event Captured in P&L Account	No	The month to represent the aggregate reportable operational risk events captured as Actual loss in P&L account.
Amount Involved	Yes	This field must have a value to reflect the overall **aggregated** financial amount and/or transactions value associated with the operational risk event reported.
Loss incurred by	Yes	REs must identify party(ies) that incur(s) the (Gross Actual loss or Insurance Recoveries or Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields.
Loss Event Description		
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.

Data Fields	Mandatory Field	Description
Nature of Event	Auto-generated	Reportable operational risk events will automatically be classified as the following: **Repeated** - For event that REs have experienced previously within the last three years
Sub Nature of Event	Auto-generated	For <u>all</u> aggregated fraud events < RM 1,000 must be classified as follows: **Repeated MO** - For MO that REs have experienced previously within the last three years
Aggregate Reporting Details		
Event Type Level 1	Auto-generated	This field is auto-generated based on the Loss Event Name selection.
Amount	Yes	The net actual losses for the event must be the same as the 'Net Actual Loss' in 'Loss Incurred by' table.
Number of Transactions	Yes	To specify total number of transactions reported under this aggregated reporting for the selected Event Type Level 1. Please refer to **Appendix 2**.
Number of Customers Impacted	Yes	To specify total number of customers impacted reported under this aggregated reporting for the selected Event Type Level 1. Please refer to **Appendix 2**.

6. Aggregate reporting for physical cash shortage due to EDPM & CPBP

Category: Physical cash shortage

1. **EDPM**: Due to execution error
2. **CPBP**: Due to penalties on cash discrepencies
3. **External Fraud**: Due to counterfeit notes / coins discovered over-the-counter and by outsourced service providers. **Please refer to Appendix 8.**
4. **BDSF**: For counterfeit notes/ coins accepted via SST. **Please refer to Appendix 8**.

Loss Event Classification: Actual Event with Actual Loss
Applicability: BIs

(a) Examples of Aggregate cash shortage penalty and execution error shortage

Scenario 1: Branch teller found cash imbalance or discrepancy of RM 500 in ATM during end-day balancing

- **Event Type Level 1**: Execution, delivery and process management
- **Event Type Level 2:** Transaction capture, execution and maintenance
- **Event Type Level 3**: Other task miss-performance

Scenario 2: CIT vendor is penalised by the Bank for two pieces of RM 20 denomination that do not tally with its report

- **Event Type Level 1**: Clients, products and business practices
- **Event Type Level 2**: Suitability, disclosure and fiduciary
- **Event Type Level 3**: Fiduciary breaches / guideline violations

Table 45: Data fields for reporting physical cash shortage due to EDPM and CPBP

Data Fields	Mandatory Field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".

Data Fields	Mandatory Field	Description
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Yes	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3**: **<u>For execution errors</u>** • **Level 1**: Other loss event

Data Fields	Mandatory Field	Description
		• **Level 2:** Aggregated Physical cash shortages • **Level 3**: Due to execution errors **<u>For penalties on cash shortages / cash excess</u>** • **Level 1**: Other loss event • **Level 2**: Aggregated Physical cash shortages • **Level 3**: Due to penalties on currency shortages/ excess
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Auto-generated	This field is auto-populated based on Level 3 Operational Risk reportable event selected: ➢ Aggregated Physical Cash Shortages Due to Execution Error ➢ Aggregated Physical Cash Shortages Due to Penalties on Currency Shortages / Excess
Submission ID Link	No	For LED which impacts two or more reportable operational risk events based on Table 3, the multiple LEDs must be linked by using this function
Loss Event Classification	Auto-generated	Only **Actual Event** with Actual Loss. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
Internal Loss Event ID	Yes	REs are required to provide its own ID for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.

Data Fields	Mandatory Field	Description
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact –** There is an actual financial loss • **Both financial and non-financial** – There is actual / potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Auto-generated	This data field is auto-generated as **Actual Loss.**
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk events with Non-Financial Impact level classification: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7*
Non-Financial Impact Justification	No	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Business Lines	Yes	Since this is an aggregate report, please select the business lines that are most affected. Must be reported up to Level 3 based on **Appendix 13**
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Event Type	Yes	REs must categorise the event as follows:

Data Fields	Mandatory Field	Description
		<u>For execution errors</u> • **Level 1:** EDPM • **Level 2:** Transaction capture, execution & maintenance • **Level 3:** Other Task miss-performance **<u>For penalties on cash shortages / cash excess</u>** • **Level 1:** CPBP • **Level 2:** Fiduciary • **Level 3:** Fiduciary breaches/guideline violations
Causal Categories	Yes	Please select the causal category that is most relevant to the event type up to Level 3 in accordance with the taxonomy in **Appendix 15.**
Month of Event Occurrence	Yes	The month to represent the aggregate reportable operational risk events which took place in a particular month.
Month of Event Detection	Yes	The month to present the aggregate reportable operational risk events which were detected in a particular month.
Month of Event confirmation	Yes	The month to represent the aggregate reportable operational risk events confirmed in a particular month.
Month of Loss Event Captured in Provision account	No	Select month date to represent the date where provision (Potential Loss) is affected in Provision account for the overall events.
Month of loss event captured in P&L account	No	The month to represent the aggregate reportable operational risk events captured as Actual loss in P&L account.
Amount Involved	Yes	This field must have a value to reflect the overall **<u>aggregated</u>** financial amount and/or transactions value associated with the operational risk event reported.
Loss incurred by	Yes	REs must identify party(ies) that incur(s) the (Gross Actual loss or Insurance Recoveries

Data Fields	Mandatory Field	Description
		or Non-insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields.
Loss Event Description		
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.
Nature of Event	Auto-generated	Reportable operational risk events will automatically be classified as the following: **Repeated** - For event that REs have experienced previously within the last three years
Sub Nature of Event	Auto-generated	For <u>all</u> aggregated fraud events < RM 1,000 must be classified as follows: **Repeated MO** - For MO that REs have experienced previously within the last three years.

Data Fields	Mandatory Field	Description
Aggregate Reporting Details		
Cash Shortage	Auto-generated	Categories of physical cash shortages are auto-generated based on the Reportable OR Level 3 selection: ➢ Due to EDPM o Over-the-counter o CIT Vendor ➢ Due to penalties / CPBP o Penalty by BNM due to cash discrepancy
Aggregate Net Actual Loss Amount	Yes	The net actual losses for the event must be the same as the 'Net Actual Loss' in 'Loss Incurred by' table.
Number of Transactions	Yes	To specify total number of transactions reported under this aggregated reporting for the selected Event Type Level 1. Please refer to **Appendix 2**.
Number of Customers Impacted	Yes	To specify total number of customers impacted reported under this aggregated reporting for the selected Event Type Level 1. Please refer to **Appendix 2**.

Individual Operational Risk Event Reporting Requirements - Non-payment related fraud and non-fraud events

7. REs must submit individual reporting to ORR system in accordance with the requirements and timeline set out in **Table 2: Operational risk information reporting deadlines** and **Table 3: ORR LED reporting types and deadlines.**

8. REs must report individual events in accordance with the categories and threshold specified in **Table 46: Individual reporting types and threshold**.

9. Events with new MO and / or with amount that are above the threshold specified in **Table 2: Operational risk information reporting deadlines,** must NOT be aggregated and must be reported as a single event in ORR according to **Table 3: ORR LED reporting types and deadlines.**

10. Near Miss application fraud events (e.g. banking facilities/financing application, opening of account) are not required to be reported as loss event unless if it is a new MO to the REs. Nonetheless, the number of application fraud Near Miss events would need to be reported as KRI.

Table 46: Individual reporting types and threshold

Category	Sub-category	Threshold	Submission to ORR
Individual non-payment related fraud event	Individual event for event types:	Based on the loss amount below:	To submit 1 individual submission for Actual or Near Miss event
	Physical Robbery	Amount Involved ≥ RM 200,000	
		Amount Involved < RM 200,000	
	SST Robbery	N/A	
	External Fraud	• Actual or Potential Loss > RM1,000 is reported individually • Near Miss is reported individually	To submit 1 individual submission for Actual, Potential or Near Miss event
	Internal Fraud		
	New external and internal fraud MO **excluding** payment fraud, physical robbery, SST robbery and cyber event	N/A	
Event with financial losses	Individual event for these event types: • Employment practices and workspace safety • Execution, delivery and process management • Damage to physical assets • Business disruption and system failure • Clients, products and business practices	Actual Loss > RM1,000	To submit 1 individual submission for Actual event with Actual Loss
Event with no financial losses		N/A	To submit 1 individual submission for Actual event

11. **Individual reporting for physical robbery in FIs**

Category: Physical robbery

1. For loss amount ≥ RM 200,000
2. For loss amount < RM 200,000

Loss Event Classification: Actual Event or Near Miss

Applicability: REs which are FIs

(a) Examples of physical robbery in FIs

Scenario 1: An actual robbery at a bank's branch where the robbers managed to break into the branch vault and took away RM 300,000. The robbery was featured in local news where public expressed concern on the safety of their deposit

- **Loss Event Classification:** Actual Event
- **Loss Event Impact classification:** Both financial and non-financial
- **Event Type Level 1:** External Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3:** Theft / Robbery

Scenario 2: An attempted robbery at a bank's branch where the robbers managed to break into the branch but were shot dead by the security guard.

- **Loss Event Classification:** Near Miss
- **Loss Event Impact classification:** Both financial and non-financial
- **Event Type Level 1:** External Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3:** Theft / Robbery

Table 47: Data fields for reporting physical robberies with loss amount ≥ RM200,000 and < RM200,000

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure • REs must select the respective reporting entity for REs under "Financial Group structure"
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and

Data fields	Mandatory field	Description
		must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3**: • **Level 1**: Critical Event • **Level 2**: Robbery and Theft • **Level 3:** Physical Robbery ≥ RM 200k **OR** • **Level 3:** Physical Robbery < RM 200k
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the robbery.
Submission ID link	No	For LED which impacts to two or more reportable OR events based on **Table 3**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • **Actual Event:** On and off-premise robbery. This includes cash robbery to REs' cash managed by CIT vendor • **Near Miss Event:** Failed attempted robbery *Please refer to paragraph 16.1 for the definitions of the above-mentioned categories.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes high reputational impact based on REs internal framework
Islamic Business?	Yes	RE must select '**Yes**' for events that involve Islamic products or services, which

Data fields	Mandatory field	Description
		may or may not involve shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC.
Internal Loss Event ID	No	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss; • **Non-financial impact** – No loss amount involved but there is an impact on reputation, non-compliance etc; or • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	REs must select one of the following for reportable operational risk event with Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for reportable operational risk event with Non-Financial Impact: • Low • Medium • High

Data fields	Mandatory field	Description
		Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7
Non-Financial Impact Justification	Yes	REs to justify on the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13** *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any*
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14**: • **Level 1**: External Fraud • **Level 2:** Fraud and Theft • **Level 3:** Theft / Robbery **OR** • **Level 1**: Internal Fraud • **Level 2:** Theft and fraud • **Level 3**: Theft or extortion or embezzlement or robbery
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15.**
Date of Event Occurrence	Yes	The date when the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date on which the RE became aware of the event.

Data fields	Mandatory field	Description
		Please refer to paragraph 16.2 for the definition of the mentioned date.
Date of Confirmation	Yes	The date on which the RE verified or confirmed the operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Loss Event Captured in Provision account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L account	No	The date on which the operational risk loss is recognised based on the accounting framework of the REs. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction values associated with the reportable operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss incurred by	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'

Data fields	Mandatory field	Description
Loss Event Description		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • **On-pemise** – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside premise(s) of REs: To describe the speific places i.e. outsourced service provider, legal firm, customer premise, remote working **b) <u>For ITOs only</u>** • **On premise**: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service ➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance

Data fields	Mandatory field	Description
		➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • **Off-premise**: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster.
Number of Business Lines Affected	Yes	Only applicable for event that affects multiple business lines. Please refer to **Appendix 2**.
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.
How the event occurred?	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential

Data fields	Mandatory field	Description
		information e.g., Name, I/C number and other personal information.
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years.
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years. *Note: **All External** and **Internal Fraud LED** events must be classified as either new or repeated MO.*
Modus Operandi Involved	Yes	RE must concisely define the method or manner of the occurrence of the OR event. The modus operandi involved in the LED must be stated and is not limited to fraud modus operandi. For examples, please refer to paragraph 17.8.
Parties Involved In / Affected By The Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved /affected • Staff • Third party service provider

Data fields	Mandatory field	Description
		• Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number of Individual(s) Involved In / Affected By the Event	Yes	Based on the '**Parties involved in / affected by the event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided and at minimum, must include the underlying cause of the event.
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event REs may select 'TBC' [To Be Confirmed] for remedial action plans that are not finalised during the initial reporting
Remedial Action Implementation Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs must select 'TBC'. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided
Remedial Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint

Data fields	Mandatory field	Description
		4. PDF 5. JPEG / PNG / BMP
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.
Mitigation Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

12. Individual reporting for SST robbery in BIs

Category: SST robbery
Loss Event Classification: Actual Event or Near Miss
Applicability: BIs

Examples of SST robbery in FIs

Scenario 1: An actual ATM robbery at a gas station where the robbers yanked the ATM machine and took away RM 150,000.

- **Loss Event Classification**: Actual Event
- **Loss Event Impact classification:** Financial Impact
- **Event Type Level 1**: External Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3**: Theft / Robbery

Scenario 2: An attempted ATM robbery at a bank's branch where the robbers used the oxytorch method to break the ATM machine but the alarm was triggered and the nearby police station was alerted. The robbers were captured nearby the scene. The case went viral in social media.

- **Loss Event Classification:** Near Miss
- **Loss Event Impact classification:** Both financial and non-financial impact
- **Event Type Level 1:** External Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3:** Theft / Robbery

Table 48: Data fields for reporting SST Robbery

Data fields	Mandatory field	Description
General		
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as one of the following: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values.

Data fields	Mandatory field	Description
		3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. 6. For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. 7. '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3**: • **Level 1**: Critical Event • **Level 2**: Robbery and Theft • **Level 3:** SST Robbery
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the SST robbery.
Submission ID link	No	For LED which impacts to two or more reportable OR events based on **Table 3**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • **Actual Event:** On and off-premise successful SST robbery. • **Near Miss Event:** Failed attempted SST robbery.

Data fields	Mandatory field	Description
		Please refer to paragraph 16.1 for the definitions of the above-mentioned categories
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes a high reputational impact based on the REs' internal framework.
Boundary Event	No	REs must categorise the reportable operational risk event as being related to either Credit risk, Market risk or Not Applicable with reference to **Appendix 11**. Note: This is applicable to BIs only.
Islamic Business?	Yes	REs must select 'Yes' for an event that involves Islamic products or services, which may or may not be related to shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC.
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Type of SST Robbery	Yes	To specify the exact method of robbery or attempted robbery: • Gas or explosives (Bombing) • Steel-cutting torch (Oxy Torch) • Force Open (Yanking) • Malware • Vandalism • Others (please specify)
Type of SST	Yes	REs must select from the following for SST(s): • ATM (Automated Teller Machine)

Data fields	Mandatory field	Description
		• CDM (Cash Deposit Machine) • CRM (Cash Recycler Machine)
Number of SSTs Affected	Yes	Number of SSTs that are impacted due to this reportable OR.
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss • **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc. • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.
Financial Impact Classification	Yes	REs must select one of the following for operational risk event with Financial Impact: • Actual Loss; or • Potential Loss
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7.*
Non-Financial Impact Justification	Yes	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks.

Data fields	Mandatory field	Description
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13.** *Please refer to specific appendix that is related to the reportable OR for the specific selection, if any.*
Product / Service	Yes	Must be reported based on Business Line Level 3 selection in accordance with the taxonomy in **Appendix 13**.
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14**: • **Level 1**: External Fraud • **Level 2:** Theft and fraud • **Level 3:** Theft / Robbery **OR** • **Level 1:** Internal Fraud • **Level 2:** Theft and fraud • **Level 3:** Theft or extortion or embezzlement or robbery
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15.**
Date of Event Occurrence	Yes	The date on which the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date on which the REs became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*

Data fields	Mandatory field	Description
Date of Loss Event Captured in Provision Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date on which the operational risk loss is recognised based on the accounting framework of the REs. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and / or transaction values associated with the reportable operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss Incurred By	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'
Loss Event Description		
Where the event happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: • **On-pemise** – occurs in the premise(s) of the REs:

Data fields	Mandatory field	Description
		To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside premise(s) of REs: To describe the speific places i.e. outsourced service provider, legal firm, customer premise, remote working
Number of Business Lines Affected	Yes	To provide the number of affected business lines. **For banking**: by Business Line Level 1
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.
How the Event Occurred?	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g. name, I/C number and other personal information.
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or

Data fields	Mandatory field	Description
		• **Repeated** – For OR that REs have experienced previously within the last three years.
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years. *Note: **All** **External** and **Internal Fraud LED** events must be classified as either new or repeated MO.*
Modus Operandi Involved	Yes	RE must concisely define the method or manner of the OR events occurrence. The modus operandi involved in the LED must be stated and is not limited to fraud modus operandi. For examples, please refer to paragraph 17.8.
Parties Involved In / Affected by the Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved / affected • Staff • Third party service provider • Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number of Individual(s) Involved In / Affected by the Event	Yes	Based on the '**Parties involved in / affected by the event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs

Data fields	Mandatory field	Description
		may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided, at minimum must include the underlying cause of the event.
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event. REs may select 'TBC' [To Be Confirmed] for remedial action plan(s) that are not finalised during the initial reporting.
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs must select 'TBC'. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided.
Remedial Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.

Data fields	Mandatory field	Description
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.
Mitigation Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

13. Individual reporting for non-payment related fraud event

Category:

1. Individual non-payment related fraud event > RM 1,000
2. Individual non-payment related fraud event with new MO

Loss Event Classification: Actual Event, Potential Event or Near Miss
Applicability: All REs

(a) Application fraud Near Miss events (e.g., banking facilities / financing application, opening of account) are not required to be reported as loss event unless it is a new MO to the REs. Nonetheless, the number of application fraud Near Miss events would need to be reported as KRI.

(b) Examples of non-payment related fraud events > RM 1,000:

Scenario 1: Teller embezzles RM 2,000 petty money from branch account into his/her account

Scenario 2: RE's staff colludes with a vendor to create fake invoice totalling to RM 2,500 for service not rendered

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Internal Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3:** Please select the Event Types that are most relevant

(c) Examples of non-payment related fraud events > RM 1,000:

Scenario 1: A fraudster forged documents to obtain personal financing facilities of RM 10,000

Scenario 2: A fraudster falsified insurance claim / premium to exaggerate claim for vehicle accident amounted to RM 5,500

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** External Fraud
- **Event Type Level 2:** Theft and Fraud
- **Event Type Level 3**: Please select the Event Types that are most relevant

(d) Examples of fraud events with new MO excluding payment fraud, physical robbery, SST robbery and cyber event:

Scenario 1: A fraudster forged documents to support financing application that appeared to be genuine using a new falsifying technique

- **Loss Event Classification:** Actual Event
- **Event Type Level 1:** External Fraud
- **Event Type Level 2:** Theft and Fraud

- **Event Type Level 3**: Forgery / Counterfeit (Cover Notes, Policy Certificates, Currency, Cheque, Security Documents / Identification documents)

Scenario 2: A new MO impacted the RE for the first time where internal staff of front and back office colluded to mask market losses

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Internal Fraud
- **Event Type Level 2:** Unauthorised activity
- **Event Type Level 3**: Please select the Event Types that are most relevant

Table 49: Data fields for reporting non-payment related fraud

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure • REs must select the respective reporting entity for REs under "Financial Group structure"
Reporting As	Auto-generated	REs will be defined based on paragraph 2
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact.

Data fields	Mandatory field	Description
		4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. *6.* For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. *7.* '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3**: • **Level 1**: Fraud Event • **Level 2**: Non-payment Fraud • **Level 3**: Individual event
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the fraud event.
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • Actual Event • Potential Event • Near Miss Event *Please refer to paragraph 16.1 for the definitions of the above-mentioned categories.*

Data fields	Mandatory field	Description
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes a high reputational impact based on the RE's internal framework.
Boundary Event	No	REs must categorise the reportable operational risk event as being related to either Credit risk, Market risk or Not Applicable with reference to **Appendix 11**. Note: This is applicable to BIs only.
Islamic Business?	Yes	REs must select '**Yes**' for an event that involves Islamic products or services, which may or may not be related to shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC.
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Lines & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual or potential financial loss • **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc. • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.

Data fields	Mandatory field	Description
Financial Impact Classification	Yes	REs must select one of the following for operational risk event with Financial Impact: • Actual Loss; or • Potential Loss.
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7.*
Non-Financial Impact Justification	Yes	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with explanation of the related non-financial risks
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13.** *Please refer to the specific appendix that is related to the reportable OR for the specific selection, if any.*
Product / Service	No	Must be reported based on Level 3 Business Line selection in accordance with the taxonomy in **Appendix 13**.
Delivery Channel	No	Channels used to deliver the product / services of the operational risk events. **For REs <u>except</u> ITOs:** • Internet • Mobile • Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A

Data fields	Mandatory field	Description
		For ITOs only: • Direct Clients – Walk In • Direct Clients – Internet • Direct Clients – Direct Mailing • Direct Clients – Marketing Staff • Direct Clients – Others • Telemarketing • Franchise Holders / Dealers (for GITOs only) • Registered Individual Agents • Registered Corporate Agents • E-Commerce Marketplace • Partners in Digital Platforms • Financial Advisers • Bancassurance / Bancatakaful • Co-Insurer / Co-Takaful • Insurance / Takaful Brokers • Reinsurance / Retakaful Accepted • Others (please specify)
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in Appendix 14 based on the primary impact of the operational risk event. REs must categorise the event using ONLY the following selection of event types: • Level 1: External Fraud or Internal Fraud • Level 2: Any event type that is most relevant based on the event type level 1 selected • Level 3: Any event type that is most relevant based on the event type level 1 selected
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15.**

Data fields	Mandatory field	Description
Date of Event Occurrence	Yes	The date on which the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date on which the REs became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Loss Event Captured in Provision Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date on which the operational risk loss is recognised based on the accounting framework of the REs. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction values associated with the reportable operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss Incurred By	Yes	REs must select party(ies) that incur(s) the (Actual or Potential or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party

Data fields	Mandatory field	Description
		REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance / non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'.
Loss Event Description		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • **On-pemise** – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside premise(s) of REs: To describe the speific places i.e. outsourced service provider, legal firm, customer premise, remote working **b) <u>For ITOs only</u>** • **On premise**: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service ➢ Data centre

Data fields	Mandatory field	Description
		➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance ➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • **Off-premise**: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster.
Number of Business Lines Affected	Yes	Only applicable for event that affects multiple business lines. *Please refer to **Appendix 2**.*
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia.

Data fields	Mandatory field	Description
		• **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.
How the Event Occurred?	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g. name, I/C number and other personal information.
Nature of Event	Yes	Operational risk events must be classified as either one of the following: • **New** - For new type of OR impacting the REs for the first time in the last three years or re-occurs after three years. Please refer to paragraph 17.9. • **Repeated - For OR that REs have experienced within the last three years**
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years.
Modus Operandi Involved	Yes	RE must concisely define the method or manner of the OR events occurrence. The modus operandi involved in the LED, not limited to fraud modus operandi. For examples, please refer to paragraph 17.8.
Parties Involved In / Affected by the Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved /affected

Data fields	Mandatory field	Description
		• Staff • Third party service provider • Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number of Individual(s) Involved In / Affected by the Event	Yes	Based on the '**Parties involved in / affected by the event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided, at minimum must include the underlying cause of the event
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event. REs may select 'TBC' [To Be Confirmed] for remedial action plan(s) that are not finalised during the initial reporting.
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs must select 'TBC'. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plan(s) is provided.
Remedial Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel

Data fields	Mandatory field	Description
		2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.
Mitigation Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

14. Reporting for individual non fraud event in reporting entities

Category: Event with financial loss > RM 1,000 for:

1. Employment practices and workspace safety
2. Damage to physical assets
3. Business disruption and system failure
4. Clients, products and business practices
5. Execution, delivery and process management

Loss Event Classification: Actual Event with actual loss
Applicability: All REs

(a) Examples of actual non-fraud events with actual loss >RM 1,000:

Scenario 1: Dealer wrongly inputs incorrect foreign exchange (FX) rate causing RM 2,000 loss to reinstate customer's position

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Execution, delivery and process management
- **Event Type Level 2:** Transaction capture, execution and maintenance
- **Event Type Level 3**: Data entry or maintenance or loading

Scenario 2: Vandalism act to RE's premise (glass door) causing RM 2,500 loss to the RE

- **Loss Event Classification:** Actual Event with Actual Loss
- **Event Type Level 1:** Damage to physical assets
- **Event Type Level 2:** Natural disaster & other losses
- **Event Type Level 3**: Human Losses – Vandalism

Table 50: Data fields for reporting individual non fraud event

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values.

Data fields	Mandatory field	Description
		3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact. 4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. *6.* For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. *7.* '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3**: • **Level 1**: Other loss event • **Level 2**: All other actual individual events • **Level 3**: Event with financial losses > RM1,000
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event.
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3**, the multiple LEDs must be linked by using this function.

Data fields	Mandatory field	Description
Loss Event Classification	Yes	The reportable operational risk event must be classified as the following: • **Actual Event:** OR event that occurred and identified by the REs *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes high reputational impact based on REs internal framework.
Boundary Event	No	REs must categorise the reportable operational risk event as being related to either Credit risk, Market risk or Not Applicable with reference to **Appendix 11**. Note: This is applicable to BIs only.
Islamic Business?	Yes	REs must select '**Yes'** for an event that involves Islamic products or services, which may or may not be related to shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC.
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual financial loss • **Both financial and non-financial** – There is actual/potential financial loss and an impact on reputation, non-compliance etc.

Data fields	Mandatory field	Description
Financial Impact Classification	Yes	Res must select one of the following for reportable operational risk event with Financial Impact: • Actual Loss
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact: • Low • Medium • High *Note: the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and others. Please refer to paragraphs 16.6 and 16.7*
Non-Financial Impact Justification	Yes	REs to justify the reason behind the selection of High / Medium / Low for the non-financial impact with an explanation of the related non-financial risks
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13.** *Please refer to the specific appendix that is related to the reportable OR for the specific selection, if any.*
Product / Service	Yes	Must be reported based on Level 3 Business Line selection in accordance with the taxonomy in **Appendix 13**.
Delivery Channel	Yes	Channels used to deliver the product / services of the operational risk events. **For REs <u>except</u> ITOs:** • Internet • Mobile • Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A

Data fields	Mandatory field	Description
		For ITOs only: • Direct Clients – Walk In • Direct Clients – Internet • Direct Clients – Direct Mailing • Direct Clients – Marketing Staff • Direct Clients – Others • Telemarketing • Franchise Holders / Dealers (for GITOs only) • Registered Individual Agents • Registered Corporate Agents • E-Commerce Marketplace • Partners in Digital Platforms • Financial Advisers • Bancassurance / Bancatakaful • Co-Insurer / Co-Takaful • Insurance / Takaful Brokers • Reinsurance / Retakaful Accepted • Others (please specify)
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event. **Level 1 Event:** • Employment practices and workspace safety • Damage to physical assets • Business disruption and system failure • Clients, products and business practices • Execution, delivery and process management
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15**

Data fields	Mandatory field	Description
Date of Event Occurrence	Yes	The date on which the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date on which the REs became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Loss Event Captured in Provision Account	No	The earliest date on which the operational risk loss has been accrued in suspense, reserve or provision of REs accounts. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Date of Loss Event Captured in P&L Account	No	The date on which the operational risk loss is recognised based on the accounting framework of the REs. *Please refer to paragraph 16.2 for the definition of the mentioned date and only applicable if Financial Impact is selected.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction values associated with the reportable operational risk event reported. Note: This field is mandatory if Financial Impact is selected.
Loss Incurred By	Yes	REs must select party(ies) that incur(s) the (Actual or Insurance Recoveries / Non-insurance Recoveries) loss from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Gross Actual Loss' field. REs must provide insurance /

Data fields	Mandatory field	Description
		non-insurance recoveries in the indicated fields. Applicable when 'Financial Impact' is selected under the 'Loss Event Impact'.
Loss Event Description		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • **On-pemise** – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside premise(s) of REs: To describe the speific places i.e. outsourced service provider, legal firm, customer premise, remote working **b) <u>For ITOs only</u>** • **On premise**: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service ➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries

Data fields	Mandatory field	Description
		➢ Finance ➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • **Off-premise**: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster.
Number of Business Lines Affected	Yes	Only applicable for event that affects multiple business lines. *Please refer to **Appendix 2**.*
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.

Data fields	Mandatory field	Description
How the Event Occurred?	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include customer / individual confidential information e.g. name, I/C number and other personal information.
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years.
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years. *Note: **All External** and **Internal Fraud LED** events must be classified as either new or repeated MO.*
Modus Operandi Involved	Yes	RE must concisely define the method or manner of the OR events occurrence. The modus operandi involved in the LED, not limited to fraud modus operandi. For examples, please refer to paragraph 17.8.
Parties Involved In / Affected By The Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved / affected • Staff

Data fields	Mandatory field	Description
		• Third party service provider • Others (please specify) Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number Of Individual(s) Involved In / Affected by the Event	Yes	Based on the 'Parties involved in / affected by the event' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided, at minimum must include the underlying cause of the event
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event. REs may select 'TBC' [To Be Confirmed] for remedial action plan(s) that are not finalised during the initial reporting.
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs must select 'TBC'. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plan(s) is provided.
Remedial Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint

Data fields	Mandatory field	Description
		4. PDF 5. JPEG / PNG / BMP
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.
Mitigation Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

15. Reporting for individual actual event with no financial loss with medium or high non-financial impact level.

Category: Event with no financial impact for:
1. Employment practices and workspace safety
2. Damage to physical assets
3. Business disruption and system failure
4. Clients, products and business practices
5. Execution, delivery and process management

Loss Event Classification: Actual Event with actual loss
Applicability: All REs

(a) In principle, Actual Event with no financial impact is to be reported if the non-financial impact level is rated as 'Medium' or 'High' by an RE's internal assessment with reference to paragraphs 16.6 and 16.7. As a guidance, these events may include, but not be limited to the following:

- OR event with amount > RM 1 million involved
- Critical non-technology related / physical BDSF
- Non-compliance cases with no monetary penalty
- OR events that attract / are likely to attract media attention
- OR events that pose a threat to public confidence and trust in the financial system

(b) Examples of actual non-financial events

Scenario 1: Disruption to RE's business operations in the whole state of Johor due to power shortage / riot / flood / disruption at critical third-party service providers

Scenario 1: Flash flood in KL area for two consecutive days where RE's headquarters and data centres are not accessible

Scenario 2: Widespread pandemic impacting large number of staff in critical business functions

- **Loss Event Classification**: Actual Event with no financial impact
- **Reportable Operational Risk Event Level 1:** Other loss event
- **Reportable Operational Risk Event Level 2:** All other actual event
- **Reportable Operational Risk Event Level 1:** Event with no financial losses
- **Loss Event Classification:** Actual Event with no financial impact
- **Event Type Level 1:** Business disruption and system failures
- **Event Type Level 2:** Non-system
- **Event Type Level 3:** Please select the event types that are most relevant
- **Non-Financial Impact Level:** Medium or High

(c) Examples of actual non-financial events

Scenario 1: Customer lashed out discontent on social media due to RE staff mistreatment in attending to his/her financial needs

Scenario 2: RE received reprimand for unethical behaviour / regulatory non-compliance despite no monetary penalties imposed

- **Loss Event Classification**: Actual Event with no financial impact
- **Event Type Level 1:** Clients, products and business practices
- **Event Type Level 2**: Suitability, disclosure and fiduciary / Improper business or market practices
- **Event Type Level 3:** Please select the event types that are most relevant
- **Non-Financial Impact Level:** Medium or High

(d) Examples of actual non-financial events

Scenario 1: Chemical intoxication in a district in Sarawak that caused multiple branch closure over a one week period

Scenario 2: Power outage in a state in Malaysia that caused a one day disruption to all businesses including bank branches

- **Loss Event Classification:** Actual Event with no financial impact
- **Event Type Level 1:** Business disruption and system failures
- **Event Type Level 2:** Non-system
- **Event Type Level 3:** Please select the event types that are most relevant
- **Non-Financial Impact Level:** Medium or High

Table 51: Data fields for reporting individual actual event with no financial impact

Data fields	Mandatory field	Description
		General
Reporting Entity Name	Auto-generated	• Reporting entity name will be automatically displayed for a 'Single' entity structure. • REs must select the respective reporting entity for REs under "Financial Group structure".
Reporting As	Auto-generated	REs will be defined based on paragraph 2.
Loss Event Status	Auto-generated	Reportable operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn **Note:** 1. '**New**' for all initial submissions will be captured as '**New**' prior to approval by RE Approver. 2. **'Completed'** for Actual Event with Actual Loss (financial impact) where all mandatory data fields have values. 3. **'Completed'** for Actual Event with all mandatory fields captured for Non-Financial Impact.

Data fields	Mandatory field	Description
		4. **'Completed'** for Near Miss Event with all mandatory fields captured for Non-Financial Impact. 5. Actual Event with Potential Loss will be tagged as **'WIP**' status, as the losses are yet to be actualised. *6.* For LED with '**Completed'** status, the RE can re-open the LED form to update the event details. By doing that, the LED status will change to **'WIP'** and must be changed back to **'Completed'** upon updating the details. *7.* '**Withdrawn**' for LED events that are removed from ORR due to erroneous or duplicate submissions.
Reportable Operational Risk Events Selection	Auto-generated	REs must report based on the following Reportable Operational Risk event Level 3 in **Table 3**: • **Level 1**: Other loss event • **Level 2**: All other actual individual events • **Level 3:** Event with no financial losses
Submission ID	Auto-generated	The submission ID will be auto-generated for the reportable operational risk events upon submission for approval or the event being saved as a draft.
Loss Event Name	Yes	Clear and concise name that summarises the nature of the loss event.
Submission ID Link	No	For LED which impacts two or more reportable OR events based on **Table 3**, the multiple LEDs must be linked by using this function.
Loss Event Classification	Yes	The reportable operational risk event must be classified as either one of the following: • **Actual Event:** OR event that occurred and identified by the REs. *Please refer to paragraph 16.1 for the definition of the above-mentioned category.*

Data fields	Mandatory field	Description
High Reputation Impact?	Yes	REs must select **'Yes'** if the event causes high reputational impact based on REs internal framework.
Boundary Event	No	REs must categorise the reportable operational risk event as being related to either Credit risk, Market risk or Not Applicable with reference to **Appendix 11**. Note: This is applicable to BIs only.
Islamic Business?	Yes	REs must select '**Yes'** for an event that involves Islamic products or services, which may or may not be related to shariah related matters. Note: SNC must be reported using Shariah related matter – reporting requirement to report PSNC.
Internal Loss Event ID	Yes	REs are required to provide its own Internal Identification (ID) for each operational risk event reported in ORR. The ID must be unique and not be duplicated for other OR events.
Date of Event Reporting	Auto-generated	The date of reporting will be auto generated upon the submission approval done by RE Admin.
Impact, Business Line & Event Type		
Loss Event Impact	Auto-generated	For the reportable operational risk event, the loss event impact(s) will be auto-populated with the following: • **Non-financial impact** – No loss amount involved but has impact on reputation, non-compliance etc.
Non-Financial Impact Level	Yes	REs must select one of the following for operational risk event with Non-Financial Impact: • Medium • High ***Note:*** *the non-financial impact is not confined to reputation risk but includes legal risk, compliance risk, conduct risk and*

Data fields	Mandatory field	Description
		others. Please refer to paragraphs 16.6 and 16.7.
Non-Financial Impact Justification	Yes	REs to justify on the reason behind the selection of High / Medium for the non-financial impact with explanation of the related non-financial risks.
Business Lines	Yes	Must be reported up to Level 3 based on **Appendix 13.** *Please refer to the specific appendix that is related to the reportable OR for the specific selection, if any.*
Product / Service	Yes	Must be reported based on Level 3 Business Line selection in accordance with the taxonomy in **Appendix 13**.
Delivery Channel	Yes	Channels used to deliver the product / services of the operational risk events. **For REs <u>except</u> ITOs:** • Internet • Mobile • Branch • Agency • Bancassurance / Bancatakaful • Kiosk • Others (please specify) • N/A **For ITOs only:** • Direct Clients – Walk In • Direct Clients – Internet • Direct Clients – Direct Mailing • Direct Clients – Marketing Staff • Direct Clients – Others • Telemarketing • Franchise Holders / Dealers (for GITOs only) • Registered Individual Agents • Registered Corporate Agents • E-Commerce Marketplace • Partners in Digital Platforms

Data fields	Mandatory field	Description
		• Financial Advisers • Bancassurance / Bancatakaful • Co-Insurer / Co-Takaful • Insurance / Takaful Brokers • Reinsurance / Retakaful Accepted • Others (please specify)
Event Types	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 14** based on the primary impact of the operational risk event. **Level 1 Event:** • Employment practices and workspace safety • Damage to physical assets • Business disruption and system failure • Clients, products and business practices • Execution, delivery and process management
Causal Categories	Yes	Must be reported up to Level 3 in accordance with the taxonomy in **Appendix 15.**
Date of Event Occurrence	Yes	The date on which the event happened or took place. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Detection	Yes	The date on which the REs became aware of the event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Date of Event Confirmation	Yes	The date on which the REs have verified or confirmed the reportable operational risk event. *Please refer to paragraph 16.2 for the definition of the mentioned date.*
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and / or

Data fields	Mandatory field	Description
		transaction values associated with the reportable operational risk event reported.
Loss Event Description		
Where the Event Happened?	Yes	REs must provide the following details of the place(s) where the incident / event occurred: **a) <u>REs except ITOs</u>** • **On-pemise** – occurs in the premise(s) of the REs: To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside premise(s) of REs: To describe the speific places i.e. outsourced service provider, legal firm, customer premise, remote working **b) <u>For ITOs only</u>** • **On premise**: To select which unit(s) / function(s) caused the event as follows: ➢ Actuarial ➢ Administration ➢ Branch ➢ Claims ➢ Corporate communication / marketing ➢ Customer service ➢ Data centre ➢ Disaster recovery centre ➢ Distribution channels and intermediaries ➢ Finance

Data fields	Mandatory field	Description
		➢ Human resource ➢ Information technology ➢ Investment ➢ Legal ➢ New business ➢ Operations ➢ Product development ➢ Property / procurement ➢ Reinsurance ➢ Shariah ➢ Strategic ➢ Underwriting ➢ Others (please specify) • **Off-premise**: To describe which party(ies) caused the event, e.g. third party claimant, workshop, adjuster.
Number of Business Lines Affected	Yes	Only applicable for event that affects multiple business lines. *Please refer to **Appendix 2**.*
Location(s) of Event	Yes	REs must select location(s) by country, state(s) and district(s) where the event occurred: • **Country** – Country where the loss was incurred. • **State** – Conditionally populated for reportable operational risk event which occurred in or outside Malaysia. • **District** – Conditionally populated for reportable operational risk event which occurred in Malaysia only.
How the event occurred?	Yes	An executive summary of the chronology of the operational loss event. The executive summary must not include

Data fields	Mandatory field	Description
		customer / individual confidential information e.g. name, I/C number and other personal information.
Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New** – For new types of OR impacting the REs for the first time in the last three years or OR which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** – For OR that REs have experienced previously within the last three years.
Sub Nature of Event	Yes	Reportable operational risk events must be classified as either one of the following: • **New MO –** For new type of MO impacting the REs for the first time in the last three years or MO which re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO –** For MO that REs have experienced previously within the last three years. *Note: **All External** and **Internal Fraud LED** events must be classified as either new or repeated MO.*
Modus operandi involved	Yes	RE must concisely define the method or manner of the OR events occurrence. The modus operandi involved in the LED must be stated and is not limited to fraud modus operandi. For examples, please refer to paragraph 17.8.
Parties Involved In / Affected By The Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. • Customer(s) involved /affected • Staff • Third party service provider • Others (please specify)

Data fields	Mandatory field	Description
		Conditionally populated; please select the relevant parties involved and the number of users involved / affected.
Number Of Individual(s) Involved In / Affected by the Event	Yes	Based on the '**Parties involved in / affected by the event**' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.
Root Cause of the Event	Yes	A detailed explanation on factors leading to the event must be provided, at minimum must include the underlying cause of the event
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and REs must implement the change immediately to resolve the operational risk event. REs may select 'TBC' [To Be Confirmed] for remedial action plans that are not finalised during the initial reporting.
Remedial Action Completion Date	Yes	REs must provide the remedial action completed date. If the remedial action has not been completed, REs must select 'TBC'. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed. Applicable when the 'Remedial Action Plans' are provided.
Remedial Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

Data fields	Mandatory field	Description
Mitigation Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying reportable operational risk events and to ensure prevention of recurrence of similar incidents in the future. REs may indicate 'To be confirmed' for mitigation action plan(s) that are not finalised during the initial reporting.
Mitigation Action Completion Date	Yes	The date of the mitigation action plan is completed. If the mitigation action has not been completed, REs must select 'TBC' [To Be Confirmed]. REs are required to update the LED with the latest date in the ORR system once the remedial action plan is completed.
Mitigation Action Plan Attachment	No	An attachment is optional, and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF 5. JPEG / PNG / BMP

APPENDIX 11 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 ORR system and flag this as a 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 ORR system 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 12 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 3: ORR LED reporting types and deadlines**

2. REs must report these losses in aggregate according to **Table 52: Overseas loss event reporting requirements**.

3. Events with amount ≥ RM 1 million according to **Table 52,** must NOT be aggregated and must be reported as a single event in ORR system.

Table 52: Overseas loss event reporting requirements

Category	Sub-category	Amount	Submission to ORR
Overseas losses	Event ≥ RM 1million	All actual events with actual loss	To submit loss events individually
	Aggregate by country for event < RM 1million	All actual events with actual loss	To submit the loss events aggregated by country and event type (1 event for ALL actual events with actual loss)

4. Examples of overseas OR reporting

(a) REs to submit loss event individually by country for events ≥ RM1 million. If there were 3 loss events ≥ RM1 million that occurred from 1 January to 31 January as per below:

- Thailand – RM2.5 million
- Singapore – RM1.5 million
- Singapore – RM1.7 million

RE must submit 3 reports to ORR by 15 February or earlier (1 to 14 February).

- Report 1: Thailand RM2.5 million;
- Report 2: Singapore RM1.5 million;
- Report 3: Singapore RM1.7 million.

In ORR, please select the relevant Level 1 ‘Business Line’ and Level 1 ‘Event Type’. The chronology of the event detailing how the event occurred, root cause along with the remedial actions and mitigation action plans must be provided accordingly.

(b) For events < RM1 million, REs to submit the loss event aggregated by country. If there were 5 loss events < RM 1 million that occurred from 1 January to 31 January as per below:

- Thailand – RM20k
- Singapore – RM2k
- Singapore – RM3k
- Vietnam – RM3k
- Vietnam – RM1k

RE must submit 3 reports to ORR by 15 February or earlier (1 to 14 February).

- Report 1: Thailand RM20k;
- Report 2: Singapore RM5k;
- Report 3: Vietnam RM4k

REs must select the most relevant Level 1 'Business Line' and Level 1 'Event Type' for the aggregate overseas reporting of events < RM1 million.

Reporting overseas operational risk events in ORR

5. Overseas loss event reporting requirements

Category: Overseas operational risk events
Loss Event Classification: Actual Event with Actual loss
Applicability: All REs

Table 53: Data fields for reporting overseas operational events

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
Reporting Entity Name	Auto-generated	• REs must select the respective reporting entity for operational loss event *(Note: Applicable to Financial Group structure)* • Reporting entity name will be automatically displayed for a 'Single' entity	• REs must select the respective reporting entity for operational loss event *(Note: Applicable to Financial Group structure)* • Reporting entity name will be automatically displayed for a 'Single' entity

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
Loss Event Classification	Auto-generated	Only **Actual Event** with actual loss Please refer to **Appendix 2** for the definition	Only **Actual Event** with actual loss Please refer to **Appendix 2** for the definition
Loss Event Status	Auto-generated	Operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn Please refer to **Appendix 2** for the definitions	Operational risk events will be automatically tagged as: • New • WIP • Completed • Withdrawn Please refer to **Appendix 2** for the definitions
Reportable Operational Risk Events Selection	Yes	REs must report based on the following Reportable Operational Risk event in **Table 3**: • Level 1: Overseas Loss Event • Level 2: Individual event ≥ RM1 million	REs must report based on the following Reportable Operational Risk event in **Table 3**: • Level 1: Overseas Loss Event • Level 2: Aggregate by country and event type < RM1 million
IT Related	No	(√) – If the operational risk event is relating to IT/System	N/A
Loss Event Name	Yes	Auto-populated [Country name] Overseas Loss **≥ RM1 million**	Auto-populated [Country name] Overseas Losses **< RM1 million**
Internal Loss Event ID	No	REs may provide its own Internal	REs may provide its own Internal

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
		Identification ID for **each** operational risk event reported in ORR	Identification ID for the **aggregated** operational risk events reported in ORR
High Reputational Risk	Yes	REs must select **'Yes'** if the event causes high reputational impact based on REs internal framework	N/A
Loss Event Impact	Yes	For the reportable operational risk event, REs must choose the loss event impact(s) from the following: • **Financial impact** – There is an actual financial loss • **Both financial and non-financial** – as defined above	Auto-populated: • **Financial impact** – There is an actual financial loss
Business Lines	Yes	For individual loss event reporting, please select the Business Line (Level 1-3) that are most affected.	For an aggregate reporting, please select the Business Line (up to Level 1) that is most affected.
Event Type	Yes	For individual loss event reporting, please select the Event Type (Level 1-3) that are most affected.	For an aggregate reporting, please select the Event Type (up to Level 1) that is most affected.

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
Nature of Event	Yes	Operational risk events must be classified as either one of the following: • **New** - For new types of OR impacting the REs for the first time in the last three years or re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated** - For OR that REs have experienced previously within the last three years	N/A
Sub Nature of Event	No	For all External and Internal Fraud LED events must be classified as either one of the following: • **New MO -** For new types of MO impacting the REs for the first time in the last three years or re-occurs after three years. Please refer to paragraph 17.9; or • **Repeated MO -** For types of MO that REs have experienced previously within	N/A

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
		the last three years	
Causal Categories	Yes	For individual loss event reporting, please select the Causal Category (Level 1-3) that are most affected.	For an aggregate reporting, please select the Causal Category (up to Level 1) that is most relevant.
Date / Month of Event Occurrence	Yes	The date of the reportable operational risk event took place	The month to represent the aggregate reportable operational risk events took place in a particular month
Date / Month of Event Detection	Yes	The date of reportable operational risk event was detected	The month to present the aggregate reportable operational risk events were detected in a particular month
Date / Month of Event Confirmation	Yes	The date of reportable operational risk event confirmation is obtained	The month to represent the aggregate reportable operational risk events confirmed in a particular month
Date / Month of Loss Event Captured in P&L Account	No	The date when the operational risk loss is recognised based on REs accounting framework	The month to represent the aggregate reportable operational risk events captured as Actual loss in P&L account
Loss Event Detailed Breakdown	Yes	N/A	RE must provide the following loss event details based on the event type & business line selection:

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
			• No of Transactions • Actual Loss Amount
Where the Event Happened? **>> Description of the location**	Yes	REs must select place(s) where the incident / event occurred. Please refer to Appendix 2 • **On-premise** – occurs in REs premise(s): To describe the specific places i.e. branch, HQ, Data Centre, Training Centre, Disaster Recovery Centre • **Off-premise** – occurs outside REs premise(s) To describe the specific places i.e. outsourced service provider, legal firm, customer premise, remote working.	N/A
Country of Events	Yes	Countries where the loss incurred.	Countries where the losses incurred
State of Events	Yes	REs must select the states where the reportable operational risk event took place based on the countries selected.	N/A

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
How the event occurred	Yes	An executive summary of the chronology of the operational loss event and modus. Note: The executive summary must not include customer / individual confidential information e.g. Name, I/C number and other personal information.	N/A
Modus Operandi Involved	Yes	RE must concisely define the method or manner of the OR events occurrence. The modus operandi involved in the LED, not limited to fraud modus operandi. For examples, please refer to paragraph 17.8.	N/A
Parties Involved In / Affected by the Event	Yes	The parties involved in / affected by a reportable operational risk event must be reported. Conditionally populated; please select the relevant parties involved and the number of users involved / affected • Customer(s) involved /affected • Staff • Third party service provider	N/A

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
		• Others (please specify)	
Number of individual(s) involved in / affected by the event	Yes	Based on the 'Parties involved in / affected by the event' selection, REs must provide the number of individuals involved / affected. In the event REs are unable to determine the actual number of users affected, REs may strive to provide an estimate based on sound basis. If this event has not affected any users, please indicate as '0'.	N/A
Root cause of the event	Yes	A detailed explanation on factors leading to the event must be provided, at minimum must include the underlying cause of the event	N/A
Remedial Action Plans	Yes	A detailed explanation must be provided for the solutions to the underlying operational risk event and implement the change immediately to resolve the operational risk event. REs may indicate 'To be confirmed' for remedial action plans that are not finalised	N/A

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
		during initial reporting.	
Remedial Action Completion Date	Yes	The date the remedial action is implemented. If the remedial action has not been implemented, REs may input 'TBC'. REs are to update the reported case with the date in the ORR system, once the remedial action plan is implemented.	N/A
Remedial Action Plan Attachment	No	An attachment is optional and the formats allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF	N/A
Mitigation action plans	Yes	A detailed explanation must be provided for the solutions to the underlying operational risk event and to ensure prevention of recurrence of similar incident in the future. REs may indicate 'to be confirmed' for mitigation action plan that has yet to be confirmed during initial reporting.	N/A
Mitigation action implementation date	Yes	The date the mitigation action plan is implemented.	N/A

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
Mitigation action plan attachment	No	An attachment is optional and the format allowed are: 1. Excel 2. Word 3. PowerPoint 4. PDF	N/A
Amount Involved	Yes	This field must have a value to reflect the overall financial amount and/or transaction value associated with the operational risk event reported.	This field must have a value to reflect the overall **aggregated** financial amount and/or transactions value associated with the operational risk event reported
Loss incurred by	Yes	REs must identify party(ies) that incur(s) the (Actual loss or Potential loss or Recoveries / Insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field).	REs must identify party(ies) that incur(s) the (Actual loss or Recoveries / Insurance Recoveries) from the event: • Reporting Entity • Customer • 3rd Party REs must not use losses net of insurance recoveries as an input to the 'Net Actual Loss' field. Instead, recovered amount must be recorded in the 'Recovery Amount' field)
Request to withdraw	No	RE can request to delete the LED submitted due to	RE can request to delete the LED submitted due to

Field Name	Mandatory field	Individual ≥ RM 1 million	Aggregated < RM 1 million
		erroneous or duplicate submission.	erroneous or duplicate submission.
Reason of withdrawal	Yes	Justification(s) for deleting the LED from ORR system must be provided. The justification is required as soon as the withdrawal process is initiated. The Bank has the discretion to approve or reject such request, or to require further information for such request.	Justification(s) for deleting the LED from ORR system must be provided. The justification is required as soon as the withdrawal process is initiated. The Bank has the discretion to approve or reject such request, or to require further information for such request.

APPENDIX 13 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 Institution

Table 54: Business lines for banking institutions

Business line level 1	Business line level 2	Business line level 3	Product / Service
Commercial Banking	Corporate Banking	Trade Finance	Export Finance
			Bills of Exchange
			Letter of Credit (LC) or Banker's Acceptance (BA) or Trust Receipt (TR)
		Lending / Financing	Project Finance
			Non-Individual Mortgage
			Non-Individual Hire Purchase
			Term Loan (TL) or Overdraft (OD) etc.
			Lending / Financing
		Factoring	
		Leasing	
		Deposits / Funding	Current Account
			Fixed Deposit
			Savings
			Negotiable Instruments of Deposit (NID)
			CP / Medium Term Note (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.

Business line level 1	Business line level 2	Business line level 3	Product / Service
			Lending / Financing
		Factoring	
		Leasing	
		Deposits / Funding	Current Account
			Fixed Deposit
			Savings
			NID
			CP / MTN
		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
Retail Banking	Retail 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 / Service
			Structured Deposits
	Private Banking	Mortgage	Residential
			Non-Residential
		Personal Loan / Financing	
		Hire Purchase	
		Wealth Management	
		Deposits	Current Account
			Fixed Deposits
			Savings
			NID
			Structured Deposits
	Card Services	Cards	Credit Card
			Debit Card
			Charge Card
	E Money	Card Based	
		Network Based	
Trading and Sales	Trading (Treasury, Asset Liability Management (ALM), Proprietary Positions)	Fixed income	
		Rates	
		Equity	
		Foreign exchange	
		Commodities	
		Credit	
		Funding	
		Own position securities	
		Lending and repos	
		Brokerage	
		Debt	
		Prime brokerage	
		Others	
	Sales	Fixed income	
		Rates	
		Equity	
		Foreign exchanges	
		Commodities	
		Credit	
		Funding	
		Lending and repos	
		Brokerage	

Business line level 1	Business line level 2	Business line level 3	Product / Service
		Debt	
		Others	
	Market Making	Prime brokerage	
		Rates	
		Equity	
		Foreign exchange	
		Commodities	
		Credit	
		Funding	
		Own position securities	
		Lending and repos	
		Brokerage	
		Debt	
		Others	
Agency Services	Custody	Escrow	
		Depository receipts	
		Securities lending (customers) corporate actions	
	Corporate Agency	Issuer and paying agents	
	Corporate Trust		
Asset Management	Discretionary Fund Management	Retail	
		Wholesale	
	Non-Discretionary Fund Management	Retail	
		Wholesale	
Payment and Settlement Note: Payment and Settlement losses related to a bank's own activities would be incorporated in the loss experience of the respective affected nine Business Line	Fund Transfer	Interbank	
		Intrabank	
		Local Remittances	
		Overseas Remittances	
	Payment & Collection		
	Clearing and Settlements		
Investment Banking	Advisory Services	Equity	Equity Capital Market
			Flotation

Business line level 1	Business line level 2	Business line level 3	Product / Service
			Bonus Issue
			Merger & Acquisition (M&A)
			Initial Public Offering (IPO)
			Private Placement
			Corporate Restructuring
		Debt	Fund Raising
			Structured financing
	Underwriting	Equity	Equity Capital Market
			Flotation
			Bonus Issue
			M&A
			IPO
			Private Placement
			Corporate Restructuring
		Debt	Fund Raising
			Structured financing
Brokerage	Broking	Equity Broking – Margin	
		Equity Broking– Non Margin	
	Futures Broking	Equity Broking – Margin	
		Equity Broking– Non Margin	
Merchant Acquiring Services	Merchant Acquiring Services	Merchant Acquiring Services	

Insurance and Takaful

3. For ITOs, Business Line Level 1 refers to type of ITOs sector. Business Line Level 2 and Business Line Level 3 refers to fund and product that was impacted by the LED respectively.

4. For Business Line Level 3, the selection of 'Others' is referring to the type of product that is not listed in the selection. The selection of 'Not applicable' is referring to LEDs that is not related to product such as tax-related issues, fines or public reprimand.

Table 55: Business lines for insurance and takaful

Business line level 1	Business line level 2	Business line level 3
Life Insurance	Shareholders' fund	Participating - Individual ordinary life long-term (>1 year)
		Participating - Individual ordinary life short-term (<=1 year)
		Participating - Credit-related products
		Participating - Individual medical & health
		Participating - Group medical & health
		Participating - Group term life
		Participating - Group ordinary life - others
		Participating - Annuity
		Participating - Riders
		Participating - Others
		Non-participating - Individual ordinary life long-term (>1 year)
		Non-participating - Individual ordinary life short-term (<=1 year)
		Non-participating - Credit-related products
		Non-participating - Individual medical & health
		Non-participating - Group medical & health
		Non-participating - Group term life
		Non-participating - Group ordinary life - others
		Non-participating - Annuity
		Non-participating - Riders
		Non-participating - Others
		Investment-linked - Individual
		Investment-linked - Group
		Investment-linked - Riders
		Universal life - Individual
		Universal life - Group
		Universal life - Riders
		Others (please specify)

Business line level 1	Business line level 2	Business line level 3
		Not applicable
	Ordinary life par fund	Participating - Individual ordinary life long-term (>1 year)
		Participating - Individual ordinary life short-term (<=1 year)
		Participating - Credit-related products
		Participating - Individual medical & health
		Participating - Group medical & health
		Participating - Group term life
		Participating - Group ordinary life - others
		Participating - Riders
		Participating – Others (please specify)
	Ordinary life non-par fund	Non-participating - Individual ordinary life long-term (>1 year)
		Non-participating - Individual ordinary life short-term (<=1 year)
		Non-participating - Credit-related products
		Non-participating - Individual medical & health
		Non-participating - Group medical & health
		Non-participating - Group term life
		Non-participating - Group ordinary life - others
		Non-participating - Riders
		Non-participating - Others
		Universal life - Individual
		Universal life - Group
		Universal life - Riders
		Others (please specify)
	Annuity par fund	Participating - Annuity
	Annuity non-par fund	Non-participating - Annuity
	Investment-linked operating fund	Investment-linked - Individual
		Investment-linked - Group
		Investment-linked - Riders
	Investment-linked unit fund	Investment-linked - Individual
		Investment-linked - Group
		Investment-linked - Riders
		Others (please specify)

Business line level 1	Business line level 2	Business line level 3
Family Takaful	Shareholders' fund	Individual ordinary family short-term (>1 year)
		Individual ordinary family short-term (<=1 year)
		Credit-related products
		Individual medical & health
		Group medical & health
		Group term takaful
		Group ordinary family - others
		Annuity
		Ordinary family - Riders
		Investment-linked - Individual
		Investment-linked - Group
		Investment-linked - Riders
		Others (please specify)
		Not applicable
	Ordinary family PA fund	Individual ordinary family short-term (>1 year)
		Individual ordinary family short-term (<=1 year)
		Credit-related products
		Individual medical & health
		Group medical & health
		Group term takaful
		Group ordinary family - others
		Others (please specify)
	Ordinary family PSA fund	Individual ordinary family short-term (>1 year)
		Individual ordinary family short-term (<=1 year)
		Credit-related products
		Individual medical & health
		Group medical & health
		Group term takaful
		Group ordinary family - others
		Others
	Ordinary family GFTA fund	Individual ordinary family short-term (>1 year)
		Individual ordinary family short-term (<=1 year)
		Credit-related products
		Individual medical & health
		Group medical & health

Business line level 1	Business line level 2	Business line level 3
		Group term takaful
		Group ordinary family - others
		Others (please specify)
	Annuity PA fund	Annuity
	Annuity PSA fund	Annuity
	Annuity GFTA fund	Annuity
	Annuity WAQAF fund	Annuity
	Investment-linked risk fund	Investment-linked - Individual
		Investment-linked - Group
		Investment-linked - Riders
	Investment-linked unit fund	Investment-linked - Individual
		Investment-linked - Group
		Investment-linked - Riders
General Insurance	Shareholders' fund	Fire
		Motor
		Medical and Health
		Marine Hull
		Marine Cargo
		On-shore and Off-shore oil related
		Personal accident
		Workmen’s compensation and Employees Liability
		Contractors all risk and engineering
		Bonds
		Liabilities
		Others (please specify)
		Not applicable
	General fund	Fire
		Motor
		Medical and Health
		Marine Hull
		Marine Cargo
		On-shore and Off-shore oil related
		Personal accident
		Workmen’s compensation and Employees Liability
		Contractors all risk and engineering
		Bonds

Business line level 1	Business line level 2	Business line level 3
		Liabilities
		Others (please specify)
General Takaful	Shareholders' fund	Fire
		Motor
		Medical and Health
		Marine Hull
		Marine Cargo
		On-shore and Off-shore oil related
		Personal accident
		Workmen’s compensation and Employees Liability
		Contractors all risk and engineering
		Bonds
		Liabilities
		Others (please specify)
		Not applicable
	General fund	Fire
		Motor
		Medical and Health
		Marine Hull
		Marine Cargo
		On-shore and Off-shore oil related
		Personal accident
		Workmen’s compensation and Employees Liability
		Contractors all risk and engineering
		Bonds
		Liabilities
		Others (please specify)
Reinsurance	Shareholders' fund	Proportional treaty
		Proportional facultative
		Non-proportional treaty
		Non-proportional facultative
		Others (please specify)
		Not applicable
	Life fund	Proportional treaty
		Proportional facultative
		Non-proportional treaty
		Non-proportional facultative
		Others (please specify)
	General fund	Proportional treaty

Business line level 1	Business line level 2	Business line level 3
		Proportional facultative
		Non-proportional treaty
		Non-proportional facultative
		Others (please specify)
Retakaful	Shareholders' fund	Proportional treaty
		Proportional facultative
		Non-proportional treaty
		Non-proportional facultative
		Others (please specify)
		Not applicable
	Family fund	Proportional treaty
		Proportional facultative
		Non-proportional treaty
		Non-proportional facultative
		Others (please specify)
	General fund	Proportional treaty
		Proportional facultative
		Non-proportional treaty
		Non-proportional facultative
		Others (please specify)

Note: In the event ITOs have exhausted all means and are unable to identify any relevant fund that was impacted by the non-financial impact LED event, ITOs may select Shareholders' Fund (Business Line level 2) and Not applicable (Business Line level 3)

Payment System Regulatees

A. E- Money Issuers

Table 56: Business lines for e-money Issuers

Business line level 1	Business line level 2	Business line level 3
E-Money	E-Money	Card Based
		Network Based

B. Payment System Operators (excluding Payments Network Malaysia Sdn. Bhd. (Company No.: xx))

Table 57: Business lines for payment system operators

Business line level 1	Business line level 2	Business line level 3
Payment System Operator	Payment System Operator	Payment System Operator

C. Payment System Operators (Payments Network Malaysia Sdn. Bhd. (Company No.: xx) only)

Table 58: Business lines for other payment system operators

Business line level 1	Business line level 2	Business line level 3
Payment System Operator	Real-time retail payments platform (RPP)	Domestic
	Interbank Giro (IBG)	
	Direct Debit	
	FPX	
	JomPAY	
	e-SPICK	
	MyDebit	
	Instant transfer (IBFT)	
	Shared ATM Network (SAN)	
	Real-time retail payments platform (RPP)	Cross-border
	Interbank Giro (IBG)	
	Direct Debit	
	FPX	
	JomPAY	
	e-SPICK	
	MyDebit	
	Instant transfer (IBFT)	
	Shared ATM Network (SAN)	
	Others, please specify	

D. Merchant Acquirers - Non-Banking Institutions

Table 59: Business lines for merchant acquirers

Business line level 1	Business line level 2	Business line level 3
Merchant Acquiring Services	Merchant Acquiring Services	Merchant Acquiring Services

E. Card Issuers – Non- Banking Institutions

Table 60: Business lines for card issuers

Business line level 1	Business line level 2	Business line level 3
Card Services	Card Services	Card

APPENDIX 14 Event types taxonomy

Banking / Payment Instrument Issuers / Payment System Operators / Merchant Acquirers

Table 61: Event type taxonomy for banking / payment instrument issuers / payment system operators / merchant acquirers

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
		Application / System password sharing/ stolen
		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)

Event type level 1	Event type level 2	Event type level 3
		Fraudulent billing by suppliers
		Cheque kiting
		Card Related Fraud
		Internet Banking fraud
		Mobile Banking fraud
		Mobile Payment fraud
		E-money / Prepaid card fraud
		Fraudulent account opening
		Fraudulent application for banking products / facilities
	Systems security	Hacking / cracking damage
		Theft of information
		Unauthorised changes to programs or data by external parties
		Misuse of system access by external parties
		Sabotage by external parties
		Social engineering targeting institution
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 issues
		Hardware - Storage Platform issues
		Network/ Security devices or tools/appliances issues
		Hardware- Others
		Software - Application issues
		Software - Operating system issues
		Software - Database issues
		Software - System interfaces / linkages issues

Event type level 1	Event type level 2	Event type level 3
		Software- Others
		Telecommunication - Telecommunication network issue
		Telecommunication - Internet Service providers issue
		Telecommunication - International and Local Switches issues (VISA, MasterCard, MEPS & My Clear)
		Security Breach - Virus / Malware infection
		Security Breach - Denial of Service / Distributed Denial of Service
		Security Breach - Web defacement
	Non systems	Business Disruption – Fire
		Business Disruption – Earthquake
		Business Disruption – Flood
		Business Disruption – Pandemic
		Business Disruption – Civil Unrest
		Business Disruption – Others
		Utility Disruption – Electrical Supply
		Utility Disruption – Water Supply
6. Clients, products and business practices	Suitability, affordability, disclosure and selling practices	Suitability / Affordability assessment issues
		Aggressive sales / Force selling
		Misleading / Unauthorised Sales Materials
		Misleading / Misrepresentation of facts / Mis-selling by Staff / Intermediaries
		Product bundling
		Poor transparency and disclosure
	Fiduciary	Fiduciary breaches / guideline violations
		Retail customer disclosure violations
		Breach of privacy
		Account churning
		Misuse of confidential information
		Lender liability
		Insider trading (on firm's account)
		Unlicensed activity
		Antitrust
		Market manipulation
		Insider trading (on firm’s account)
		Money laundering
	Improper business or	Improper trade / market practices
		Mis-informing of Underlying Shariah contract

Event type level 1	Event type level 2	Event type level 3
	market practices	Poor servicing by agents
	Product flaws	Product defects
		Model errors (design, implementation, application)
		Product defects from Shariah perspective
	Selection, sponsorship and exposure	Failure to investigate client per guidelines
		Exceeding client exposure limits
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
	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 and Takaful

Table 62: Event types for Insurance and Takaful

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
		Application/System password sharing/ stolen
		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

Event type level 1	Event type level 2	Event type level 3
		Fraudulent application for products / facilities
	Systems security	Hacking / cracking damage
		Theft of information
		Unauthorised changes to programs or data by external parties
		Misuse of system access by external parties
		Sabotage by external parties
		Social engineering targeting institution
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 issues
		Hardware - Storage Platform issues
		Network/ Security devices or tools/appliances issues
		Hardware- Others
		Software - Application issues
		Software - Operating system issues
		Software - Database issues
		Software - System interfaces / linkages issues
		Software- Others
		Telecommunication - Telecommunication network issue
		Telecommunication - Internet Service providers issue
		Telecommunication - International and Local Switches issues (VISA, MasterCard, MEPS & My Clear)
		Security Breach - Virus / Malware infection

Event type level 1	Event type level 2	Event type level 3
		Security Breach - Denial of Service / Distributed Denial of Service
		Security Breach - Web defacement
	Non systems	Business Disruption – Fire
		Business Disruption – Earthquake
		Business Disruption – Flood
		Business Disruption – Pandemic
		Business Disruption – Civil Unrest
		Business Disruption – Others
		Utility Disruption – Electrical Supply
		Utility Disruption – Water Supply
6. Clients, products and business practices	Selling practices and disclosure	Aggressive sales/ Force selling
		Misleading/ Unauthorised Sales Materials
		Misleading / Misrepresentation of facts / Mis-selling by Staff / Intermediaries
		Replacement of Policy / Certificate
		Product bundling
		Poor transparency and disclosure
	Fiduciary	Fiduciary breaches / guideline violations
		Regulatory compliance of appointed representatives
		Breach of privacy
		Unlicensed activity
		Misuse of confidential information
		Insider trading (on firm's account)
		Antitrust
		Market manipulation
		Insider trading (on firm's account)
		Money laundering
	Improper business or market practices	Improper trade / market practices
		Mis-informing of underlying Shariah contract
		Poor servicing by agents
	Product Flaws	Product defects
		Model errors (design, implementation, application)
		Product defects from Shariah perspective
		Unintentional guarantees
	Selection, sponsorship and exposure	Failure to investigate client per guidelines
		Exceeding client exposure limits
		Miscommunication

Event type level 1	Event type level 2	Event type level 3
7. Execution, delivery and process management	Transaction capture, execution and maintenance	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)
	Customer intake and documentation	Client permissions / disclaimers missing
		Legal documents missing / incomplete
		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 15 Causal categories taxonomy

Table 63: Causal categories taxonomy

Causal categories level 1	Causal categories level 2	Causal categories level 3
1. People	Lack of adequate training/competency	Poor quality of recruits
		Unintentional/ accidental error
		Insufficient training provided
		Misinterpretation of information / procedures/ tasks
		Poor relationship management
		Lack of communication
		Not meeting customers reasonable expectations
		Lack of security awareness
		Staff negligence
	Inefficient culture / Behaviour	Lack of awareness
		Staff knowledge
	Inadequate resources	Product too complex
		Insufficient resourcing level
		Poor succession planning
		Process is highly technical
		Key person / knowledge dependency
	Malicious acts	Intentional/ Deliberate mistakes
		Fraudulent behaviour
		Provide misleading/false information / advice
	Lack of supervision	
	Others	Others (Please specify)
2. Process	Process / procedure failure/ issue	Dealing with change
		Procedure/process design failure
		Procedure/process implementation failure
		Unclear/absence of manual workarounds

Causal categories level 1	Causal categories level 2	Causal categories level 3
		Lack of proper documentation
		Lack of due diligence
	Inadequate monitoring / reporting	Poor contract / service level agreement
		Lack of oversight / verification by checker
	Inadequate IT/ Cyber strategy	Inadequate IT investment
		Lack of planning
		Lack of foresight
	Inadequate Process change / implementation	Management decision / change not implemented
		Management information inadequate
		Inadequate checks & balances in change management
		Inadequate testing
		Poor maintenance
	Inadequate/unclear policies & procedures	Inadequate checks/balances in written documentation
		Gaps in the policies / procedures
	Governance failure	Inadequate or Ineffective segregation of duties
		Management Control failure
	Others	Others (Please specify)
3. System (IT)	Software (IT application/ OS/ DB) (include Network & Security)	Application Defect
		Application vulnerabilities
		Others (Please specify)
	Hardware failure (include Network & Security devices)	Hardware Defect
		Others (Please specify)
4. External Event	Trade counterparty	Lack of understanding of third-party data

Causal categories level 1	Causal categories level 2	Causal categories level 3
	Customer related issues	Third-party situation beyond firm control (power / telephony / water / services)
		Unrealistic customer expectation
		Others (Please specify)
	Regulatory and legislative environment	Complex regulatory or legislation requirements
		Misinterpretation of regulatory requirements
		Reliance on third-party data
	Infrastructure failure	Power Outage
		Lack of understanding of implications of change to third-party systems
		Others (Please specify)
	Unreliable/ Incompetent third party service providers/ vendors/ suppliers/ Counterparty	Increase in transaction volume
		Increase in complexity of services rendered
		Insufficient capacity or resources
		Not meeting service delivery agreement
		Service/ system disrupted due to cyber-attack (due to external factors)
		Service/ system disrupted due to non-cyber-attack (due to external factors)
		Lack of training provided
		Lack of product/services understanding
		Malice/ Deliberate mistakes
		Unintentional/ accidental error
		Service / system disruptions by service provider(s).
		Others (Please specify)
		Riot / Demonstration

Causal categories level 1	Causal categories level 2	Causal categories level 3
	Political/ economic/ social instability	Others (Please specify)
	Environmental factors	Natural disaster (e.g. pandemic, earthquakes, floods etc.)
	Disgruntled employee, agents, union & others	Picket / Hartal
		Others (Please specify)
	Others	Others (Please specify)

APPENDIX 16 Key risk indicators taxonomy

1. Generic indicators

Table 64: Generic key risk indicators

KRI	Applicability	Description	Cycle
1. Number of application fraud Near Miss	REs except payment system operators	Number of fraudulent application detected and thwarted for secured / unsecured facility, account opening, insurance proposal submission etc. *Note: Remittance/cheque book/trading bill applications should not be included in the KRI.*	Monthly*
2. Number of reprimands received from other regulators/ enforcement agencies/ operator of designated payment systems	REs except payment system operators and merchant acquirers	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, Payments Network Malaysia Sdn. Bhd. (Company No.: xx) etc.)	Monthly*
3. Number of new litigation cases initiated against the REs	REs	Number of new cases initiated against the REs, where the RE was served with Letter of Demand / letter from a lawyer/law firm within that quarter. The number includes orders received from Industrial Court.	Quarterly*
4. Staff attrition rate	REs except payment system operators	**Attrition rate for permanent staff** $\left[\frac{\text{No of turnover in current quarter}}{\text{No of staff beginning of current quarter}}\right] \times 100$	Quarterly*

KRI	Applicability	Description	Cycle
5. Number of customers' names in the freeze orders received from enforcement agency without prior STR raised	REs except payment system operators	Number of customers' names in the freeze orders received from enforcement agency that does not match against internal list of STR raised	Quarterly*
6. Number of new audit findings	REs	Number of new audit findings from internal and / or external auditor engaged for non-financial audits to the entity which have never been raised in the last three years. Any recurring issues across different business lines must be excluded	Quarterly*
7. Number of new litigation cases initiated against the FI with SNC implications	REs except payment system operators and merchant acquirers	Number of new cases that have SNC implications, where the FI was served with a Letter of Demand / letter from a lawyer/law firm within that month	Semi-annual*
8. Number of new Shariah-related complaints	REs except payment system operators and merchant acquirers	Complaints lodged by customers on potential non-compliance with Shariah requirements in product implementation, legal documentation, product brochures, transparency, etc.	Semi-annual*

** ALL licensed professional reinsurers and retakaful operators are to report these KRIs on a yearly basis.*

2. Technology KRIs

Table 65: Technology key risk indicators

KRI	Applicability	Description	Cycle
1. Number of instances of critical services downtime exceeding Recovery Time Objective (RTO)	REs	Tracks specific critical system availability as outlined in **Appendix 4 Table 10.**	Monthly
2. Number of instances of network utilisation exceed threshold of 80%	REs	Tracks network bandwidth utilisation to identify potential threats to Denial-of-Service attack (DDoS)	Monthly
3. Number of instances response time for critical services exceeded predetermined threshold / SLA	REs	Tracks specific critical system availability as outlined in **Appendix 4 Table 10.**	Monthly
4. Number of hacking attempts on IT infrastructure	REs	The number of hacking attempt on IT infrastructure that includes any cyber event detected on REs' internal and external environment such as but not limited to scanning or probing on networks and systems, isolated malware detection lying dormant in a computer, phishing attempt targeting the employees and mitigated DDoS attacks.	Monthly
5. Number of instances of storage or memory utilisation exceeding maximum threshold of 80%	REs	Tracks specific critical system availability as outlined in **Appendix 4 Table 10.**	Quarterly
6. Numbers of batch overrun incidents	REs	Tracks specific critical system availability as outlined in **Appendix 4 Table 10.**	Quarterly

KRI	Applicability	Description	Cycle
7. Number of instances of failed Disaster Recovery Plan (DRP) tests for critical systems	REs	To ascertain the reliability of the DRP and readiness of the FI in the event of a system failure	Annually
8. Number of DRP tests planned but not conducted for the year	REs	To ascertain the reliability of the DRP and readiness of the FI in the event of a system failure	Annually
9. Number of scheduled core system maintenance not conducted	REs	To ascertain system integrity	Annually
10. Number of incidents relating to transactional reporting or updating errors of critical system	REs	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 the Bank. The transactional updating error refers to the error in the financial or customer information database. Errors due to human intervention is excluded	Annually
11. Number of Critical Systems impacted by End of Life (EOL) • Production • Disaster Recovery	REs	Tracks discontinued / unsupported components i.e., OS, Database, Hardware and Software of specific critical systems as outlined in **Appendix 4 Table 10** to identify REs obsolescence risk level. Note: "EOL" refers to the technology systems and appliances which are no longer supported and developed by the vendor and developer. Hence, extended support by developer e.g., Microsoft is considered as supported system.	Quarterly

KRI	Applicability	Description	Cycle
12. Number of Critical Systems running on unsecured version of software • Production • Disaster Recovery	REs	Tracks unsecured system version i.e., OS, Database and Application version of specific critical system as outlined in **Appendix 4 Table 10** to identify REs system vulnerabilities for potential cyber-attack(s) Note: "Unsecured version" refers to software version that are exposed to known vulnerabilities arising from undeployed patches.	Quarterly

3. Complaint KRIs for Non-Bank Payment Instrument Issuers, Payment System Operators, Merchant Acquirers

Table 66: Complaint key risk indicators for non-bank payment instrument issuers, payment system operators, merchant acquirers

KRI	Applicability	Description	Cycle
1. Number of new complaints on Sales and Marketing	• Payment Instrument Issuers • Merchant Acquirers	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) For the avoidance of doubt, complaints to be reported are complaints lodged by: • customers on payment instrument issuers (for reporting by payment instrument issuers) • merchants on merchant acquirers (for reporting by merchant acquirers) and do not include periodic reporting provided by merchants to merchant acquirers regarding complaints by merchants' customers on the merchants	Semi-annual

KRI	Applicability	Description	Cycle
2. Number of new complaints on Services	• Payment Instrument Issuers • Merchant Acquirers	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 / delay in processing, delay in disbursement, unprofessional conduct / behaviour, wrongful advice / info, sharing of customer data without consent)	Semi-annual
3. Number of new complaints on Operations	• Payment Instrument Issuers • Merchant Acquirers	Complaints on inefficiency of the internal process, system, control and procedure to ensure fair and equitable business practices (e.g. system offline, freezing / opening / closing of accounts / processing errors, customer information breaches due to operational lapses, refund processing, delay in settlement, withholding of settlement funds, dispute in agreement / document)	Semi-annual
4. Number of new complaints on Products	• Payment Instrument Issuers • Merchant Acquirers	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, issues with payment devices)	Semi-annual
5. Number of new complaints on Fees & Charges	• Payment Instrument Issuers • Merchant Acquirers	Complaints on terms and conditions relating to fees and charges, unreasonable and unfair imposition of fees and charges to prevent customers 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,	Semi-annual

KRI	Applicability	Description	Cycle
		interest, fees charged by merchant or merchant acquirer without consent)	
6. Total number of complaints received	• Payment System Operator	Complaints lodged by clients on PSOs in relation to the following: • Sales and Marketing • Services • Operations • Products • Fees & Charges For the avoidance of doubt, these do not include periodic reporting provided by clients to PSOs regarding complaints by clients' customers on the clients.	Semi-annual

4. Complaint KRIs for Banking

Table 67: Complaint key risk indicators for banking

Type of Complaints by Products		Applicability	Description	Cycle
Marketing and Sales	Deposits	BIs	Complaints lodged by customers relating to the RE's marketing and sales process for Deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers relating to the RE's marketing and sales process for Investment products	Semi-Annual
	Financing	BIs	Complaints lodged by customers relating to the RE's marketing and sales process for Financing products	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers relating to the RE's marketing and sales process for Bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers relating to the RE's marketing and sales process for payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers relating to the RE's marketing and sales process for other banking services	Semi-Annual
	Other Products	BIs	Complaints lodged by customers relating to the RE's marketing and sales process for other banking products	Semi-Annual
Fees and charges	Deposits	BIs	Complaints lodged by customers relating to the fees and charges imposed by REs on deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers relating to the fees and charges imposed by REs on investment products	Semi-Annual

Type of Complaints by Products		**Applicability**	**Description**	**Cycle**
	Financing	BIs	Complaints lodged by customers relating to the fees and charges imposed by REs on financing products	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers relating to the fees and charges imposed by REs on bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers relating to the fees and charges imposed by REs on payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers relating to the fees and charges imposed by REs on other services	Semi-Annual
	Other Products	BIs	Complaints lodged by customers relating to the fees and charges imposed by REs on other products	Semi-Annual
Terms and Conditions	Deposits	BIs	Complaints lodged by customers relating to the terms and conditions imposed by REs on deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers relating to the terms and conditions imposed by REs on Investment products	Semi-Annual
	Financing	BIs	Complaints lodged by customers relating to the terms and conditions imposed by REs on financing products	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers relating to the terms and conditions imposed by REs on bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers relating to the terms and conditions imposed by REs on payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers relating to the terms and conditions imposed by REs on other services	Semi-Annual

Type of Complaints by Products		**Applicability**	**Description**	**Cycle**
	Other Products	BIs	Complaints lodged by customers relating to the terms and conditions imposed by REs on other products	Semi-Annual
Operational	Deposits	BIs	Complaints lodged by customers on the RE's operations relating to deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers on the RE's operations relating to investment products	Semi-Annual
	Financing	BIs	Complaints lodged by customers on the RE's operations relating to financing products	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers on the RE's operations relating to bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers on the RE's operations relating to payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers on the RE's operations relating to other services	Semi-Annual
	Other Products	BIs	Complaints lodged by customers on the RE's operations relating to other products	Semi-Annual
Disputes	Deposits	BIs	Complaints lodged by customers relating to disputes on deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers relating to disputes on investment products	Semi-Annual
	Financing	BIs	Complaints lodged by customers relating to disputes on financing products	Semi-Annual

Type of Complaints by Products		**Applicability**	**Description**	**Cycle**
	Bancassurance	BIs	Complaints lodged by customers relating to disputes on bancassurance	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers relating to disputes on payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers relating to disputes on other services	Semi-Annual
	Other Products	BIs	Complaints lodged by customers relating to disputes on other products	Semi-Annual
Debt recovery issues	Financing	BIs	Complaints lodged by customers relating to RE's debt collection activities on financing products	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers relating to RE's debt collection activities on bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers relating to RE's debt collection activities on payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers relating to RE's debt collection activities on other services	Semi-Annual
	Other Products	BIs	Complaints lodged by customers relating to RE's debt collection activities on other products	Semi-Annual
Customer Service	Deposits	BIs	Complaints lodged by customers relating to RE's customer service for deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers relating to RE's customer service for investment products	Semi-Annual

Type of Complaints by Products		**Applicability**	**Description**	**Cycle**
	Financing	BIs	Complaints lodged by customers relating to RE's customer service for financing products	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers relating to RE's customer service for bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers relating to RE's customer service for payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers relating to RE's customer service for other services	Semi-Annual
	Other Products	BIs	Complaints lodged by customers relating to RE's customer service for other products	Semi-Annual
Fraud and Scams	Deposits	BIs	Complaints lodged by customers on fraud and scams relating to deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers on fraud and scams relating to investment products	Semi-Annual
	Financing	BIs	Complaints lodged by customers on fraud and scams relating to financing products	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers on fraud and scams relating to bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers on fraud and scams relating to payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers on fraud and scams relating to other services	Semi-Annual

Type of Complaints by Products		**Applicability**	**Description**	**Cycle**
	Other Products	BIs	Complaints lodged by customers on fraud and scams relating to other products	Semi-Annual
Safeguarding of customer information	Deposits	BIs	Complaints on RE's management of data and financial consumers' information relating to deposit products	Semi-Annual
	Investments	BIs	Complaints on RE's management of data and financial consumers' information relating to investment products	Semi-Annual
	Financing	BIs	Complaints on RE's management of data and financial consumers' information relating to financing products	Semi-Annual
	Bancassurance	BIs	Complaints on RE's management of data and financial consumers' information relating to bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints on RE's management of data and financial consumers' information relating to payment instruments	Semi-Annual
	Other Services	BIs	Complaints on RE's management of data and financial consumers' information relating to other services	Semi-Annual
	Other Products	BIs	Complaints on RE's management of data and financial consumers' information relating to other products	Semi-Annual
Channel Related	Deposits	BIs	Complaints lodged by customers on RE's delivery channels relating to deposit products	Semi-Annual
	Investments	BIs	Complaints lodged by customers on RE's delivery channels relating to investment products	Semi-Annual
	Financing	BIs	Complaints lodged by customers on RE's delivery channels relating to financing products	Semi-Annual

Type of Complaints by Products		**Applicability**	**Description**	**Cycle**
	Bancassurance	BIs	Complaints lodged by customers on RE's delivery channels relating to bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers on RE's delivery channels relating to payment instruments	Semi-Annual
	Other Services	BIs	Complaints lodged by customers on RE's delivery channels relating to other services	Semi-Annual
	Other Products	BIs	Complaints lodged by customers on RE's delivery channels relating to other products	Semi-Annual
Abandoned housing project	Financing	BIs	Complaints lodged by customers relating to the financing of houses involved in abandoned projects	Semi-Annual
Access to Financing	Deposits	BIs	Complaints on access to financing relating to deposit products	Semi-Annual
	Investments	BIs	Complaints on access to financing relating to investment products	Semi-Annual
	Financing	BIs	Complaints on access to financing relating to financing products	Semi-Annual
	Bancassurance	BIs	Complaints on access to financing relating to bancassurance products	Semi-Annual
	Payment Instruments	BIs	Complaints on access to financing relating to payment instruments	Semi-Annual
	Other Services	BIs	Complaints on access to financing relating to other services	Semi-Annual

Type of Complaints by Products		**Applicability**	**Description**	**Cycle**
	Other Products	BIs	Complaints on access to financing relating to other products	Semi-Annual
Others	Deposits	BIs	Complaints lodged by customers relating to deposit products not specified in any of the above categories	Semi-Annual
	Investments	BIs	Complaints lodged by customers relating to investment products not specified in any of the above categories	Semi-Annual
	Financing	BIs	Complaints lodged by customers relating to financing products not specified in any of the above categories	Semi-Annual
	Bancassurance	BIs	Complaints lodged by customers relating to bancassurance products not specified in any of the above categories	Semi-Annual
	Payment Instruments	BIs	Complaints lodged by customers relating to payment instruments not specified in any of the above categories	Semi-Annual
	Other Services	BIs	Complaints lodged by customers relating to other services not specified in any of the above categories	Semi-Annual
	Other Products	BIs	Complaints lodged by customers relating to other products not specified in any of the above categories	Semi-Annual

5. Complaint KRIs – ITOs

Table 68: Complaint key risk indicators for insurance and takaful operators

Type of Complaints		Applicability	Description	Cycle
Benefits & Claims	Delay in Claim Payment	ITOs (Family, General, Life) *	Complaints relating to RE's delay in claim payment	Semi-Annual
	Delay in Processing	ITOs (Family, General, Life) *	Complaints relating to RE's delay in processing	Semi-Annual
	Dispute on Bonus, GCP, & Survival Benefits	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to dispute on bonus, GCP, & survival benefits	Semi-Annual
	Dispute on Claim Amount	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to dispute on claim amount	Semi-Annual
	Dispute on Maturity / Surrender Value	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to dispute on maturity/surrender value	Semi-Annual
	Fraudulent Claims	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to fraudulent claims	Semi-Annual
	Repudiation of Claims	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to repudiation of claims	Semi-Annual
	Unsatisfactory Repair Works	ITOs (General only) *	Complaints lodged by policy holders and takaful participants relating to unsatisfactory repair works	Semi-Annual

Type of Complaints		Applicability	Description	Cycle
	Others	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants not specified in any of the above categories	Semi-Annual
Marketing & Sales	Force Selling	ITOs (Family, General, Life) *	Complaints relating to RE's marketing and sales process that involve force-selling	Semi-Annual
	Misleading Sales Materials	ITOs (Family, General, Life) *	Complaints relating to RE's marketing and sales process that involve misleading sales materials	Semi-Annual
	Misleading / Misrep / Mis-selling by Staff / Intermediaries	ITOs (Family, General, Life) *	Complaints relating to RE's marketing and sales process that involve misleading / misrepresentation / mis-selling by staff/intermediaries	Semi-Annual
	Replacement of Policy / Certificate	ITOs (Family, General, Life) *	Complaints relating to RE's marketing and sales process involving replacement of policy/certificate	Semi-Annual
	Others	ITOs (Family, General, Life) *	Complaints relating to RE's marketing and sales process that is not specified in any of the above categories	Semi-Annual
Product Features	High Premiums or Fees / Charges	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to high premiums or fees and charges	Semi-Annual
	Revision of MHI Premium	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to the revision of MHI premium (applicable to MHI product only)	Semi-Annual

Type of Complaints		Applicability	Description	Cycle
	Unfair Product Features	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to unfair product features	Semi-Annual
	Others	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants relating to product features that is not specified in any of the above categories	Semi-Annual
Underwriting	Dispute on NCD	ITOs (General) *	Complaints lodged by policy holders and takaful participants on the RE's underwriting process relating to disputes on NCD	Semi-Annual
	Refuse to Insure	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's underwriting process relating to refusal to insure	Semi-Annual
	Refuse to renew	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's underwriting process relating to refusal to renew existing policy/cert	Semi-Annual
	Unfair Condition Imposed – Exclusion / Loading / Excess	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's underwriting process relating to unfair additional conditions imposed	Semi-Annual
	Others	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's underwriting process not specified by any of the above categories	Semi-Annual
Customer Related Services	Delay in cancelling policy / cert	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's customer related services relating to delay in cancelling policy/certificate	Semi-Annual

Type of Complaints		Applicability	Description	Cycle
	Delay in or No Refund / Compensation	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's customer related services relating to delay in or no refund/compensation	Semi-Annual
	Delay in or Non-Issuance of Guarantee Letter	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's customer related services relating to delay in or non-issuance of Guarantee Letter	Semi-Annual
	Delay in or Non-Issuance of Policy Documents/Notices	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's customer related services relating to delay in or non-issuance of policy documents/notices/takaful certificate	Semi-Annual
	Unprofessional Behaviour of Staff / Intermediaries	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's customer related services relating to unprofessional behavior of staff/intermediaries	Semi-Annual
	Wrongful advice / info by staff	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's customer related services relating to wrongful advice/info by staff	Semi-Annual
	Others	ITOs (Family, General, Life) *	Complaints lodged by policy holders and takaful participants on the RE's customer related services not specified in any of the above categories	Semi-Annual
Mishandling of Client Money		ITOs (Family, General, Life) *	Complaints relating to the handling of any client monies or funds, by any authorised or unauthorised parties, within or separate from a RE.	Semi-Annual

Type of Complaints	Applicability	Description	Cycle
Personal Data Protection	ITOs (Family, General, Life) *	Complaints relating to the management of data and customer information that includes any violations of data protection laws or guidelines. Examples are misuse of or unauthorised leaks of customers' information	Semi-Annual

** ALL licensed professional reinsurers and retakaful operators are excluded from reporting the Complaint KRIs*

6. Generic Insurance and Takaful KRIs

Table 69: Generic insurance and takaful key risk indicators

KRI	Applicability	Description	Cycle
1. Instances of delay in issuance of policies	ITOs *	Number of policy issuance exceeding 30 days for Motor and 60 days for Non-motor from the acceptance of risk until issuance of policies or Takaful certificates	Monthly
2. Instances of delay in registering claims	ITOs *	Number of claim registration > 7 working days from receipt of claims notification	Monthly
3. Instances of delay in payment of claims	ITOs *	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.	Monthly
4. Number of replacement of life policy / certificate	ITOs (Life / Family business)*	Number of life policies / certificates replaced in a particular month.	Monthly

KRI	Applicability	Description	Cycle
5. Number of occurrences of holding cover prior to facultative placement	ITOs *	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	ITOs *	Number of: • claims recovery disputed and repudiated from reinsurers • claims recovery disputed and repudiated from subrogation **Note: This applies to all Reinsurance arrangements which include Treaty and Facultative.*	Monthly
7. Number of delay in death claims	ITOs *	Number of death claims paid > 60 days after the notification date.	Monthly
8. Instances of delay in appointing licensed / in-house adjuster	ITOs (General) *	Appointment of licensed / in-house adjuster was done >7 working days from receipt of completed claims documents.	Monthly

** ALL licensed professional reinsurers and retakaful operators are excluded from reporting the KRIs*

7. Treasury KRIs

Table 70: Treasury key risk indicators

KRI	Applicability	Description	Cycle
Treasury Processes : Deal Capture/Input			
1. Number of Off-Premise Trades/Deals with Immediate Trade Capture/Input	BIs	Number of trades/deals executed outside the treasury dealing room where immediate deal capture/input into the bank's front end treasury system is performed.	Monthly
2. Number of Off-premise Trades/Deals Without Immediate Trade Capture/Input	BIs	Number of deals / trades executed outside the dealing room, where immediate deal capture/input into the bank's front end treasury systems is **NOT** performed.	Monthly
3. Number of Late Trade/ After Hours deals	BIs	Number of trades/deals with delayed input into front-end treasury systems and after-hours trades	Monthly
4. Number of trade / deal cancellations and amendments (C&As)	BIs	Number of C&A trades / deals amended or cancelled by trader / dealer. *Note: C&A must include both same day and post-dated C&A.*	Monthly
5. Total Number of Trades / Deals	BIs	Total number of trades/deals (transaction count) executed in the reporting period.	Monthly

KRI	Applicability	Description	Cycle
		Note: Statistics must exclude any duplication such as cancelled and amended deals, and multiple counts of different legs of a single transaction.	
Treasury Processes: Payment and Settlement			
6. Number of mismatches during the confirmation process	BIs	Number of instances of mismatches between the bank's trade details vis-à-vis their counterparties trade details during the confirmation process	Monthly
7. Number of unconfirmed trade / deals	BIs	Number of trades / deals that have not been confirmed by counterparties as of the trade/deal settlement date.	Monthly
8. Number of failed trade reconciliations between Front Office and Back Office	BIs	Number of unreconciled deals / trades between Front Office and Back Office.	Monthly
9. Number of payment and settlement disputes by customers and counterparties	BIs	Number of payment and settlement transactions disputed by customers and counterparties	Monthly
Treasury Risk Management			
10. Number of treasury room limit breaches : Board-approved limits	BIs	Number of Board-approved limits breaches on all dealing / trading activities	Monthly

KRI	Applicability	Description	Cycle
		Note: Limit breaches are reportable for both trading and non-trading activities e.g., liquidity/corporate treasury business activities.	
11. Number of instances – ad hoc request to increase Board-approved trading limits	BIs	Number of specific request to increase and/or reallocate Board-approved trading limits.	Monthly
12. Number of dealer mandate breaches	BIs	Number of instances of dealers executing trades outside of their pre-approved mandates such as, but not limited to : • Trading products or in portfolios outside of designated mandates • Trading products without approved limits in place.	Monthly
Flexible Working Arrangements			
13. Average Breakdown of dealer's Working from Home (WFH)	BIs	Number of dealers Working from Home as percentage of total number of dealer (average for the month) *Note: The formula is (Total number of dealers WFH/ Total number of dealers) * 100*	Monthly
14. Average Breakdown of dealer's Working from Alternative Sites (WFA)	BIs	Number of dealers Working from Alternate Sites such as from Disaster Recovery (DR) or Business	Monthly

KRI	Applicability	Description	Cycle
		Continuity Planning (BCP) sites as percentage of total number of dealer (average for the month) *Note: The formula is (Total number of dealers WFA/ Total number of dealers) * 100*	
15. Number of incidences/disruptions during flexible working arrangements	BIs	No. of incidences/disruptions (e.g. failure in straight-through-process, payment and settlement failures, other disruptions) for trades concluded outside of the bank's main dealing room.	Monthly
Conduct Risk			
16. Number of Trade and Communication Surveillance Cases	BIs	Number of trade/deals which require further investigation post initial review.	Quarterly
17. Number of consequence actions taken against dealers	BIs	Number of consequence actions taken against dealers for breaches in the bank's policy and procedure.	Quarterly

All trades and deals of the products that shall be counted in these KRIs are covered in Appendix 17 for Treasury and Corporate Advisory KRIs.

8. Corporate Advisory KRIs

Table 71: Corporate advisory key risk indicators

KRI	Applicability	Description	Cycle
1. Number of Qualified Persons and Senior Officers resignation	BIs	To monitor minimum number of Qualified Persons and Senior Officers as per Securities Commission Malaysia's (SC) guidelines.	Monthly
2. Number of submissions rejected / returned by SCM	BIs	Number of submissions not meeting SCM's standards. *Note: Any submissions to SCM for capital market business activities e.g., security issuances, mergers as per SCM's Guidelines on Submission of Corporate and Capital Market Product Proposals. Number of instances where submissions were returned/rejected must be included even if this was approved upon re-submission.*	Monthly
3. Number of breaches in handling of confidential information policy and procedures	BIs	Number of breaches in the banking institution's relevant policy and procedures relating to handling of confidential information/ Material Non-Public Information (MNPI).	Quarterly
4. Number of breaches in Personal Account Dealing policy and procedure	BIs	Number of breaches to the banking institutions' personal account dealing policy and procedure.	Quarterly

APPENDIX 17 Key risk indicators reporting details

1. This appendix illustrates the example and explanations of the key risk indicators tabled in **Appendix 16**.
2. There are six types of KRI categories in Appendix 16 namely Generic KRIs, Technology KRIs, Complaint KRIs, Generic Insurance and Takaful KRIs, Treasury KRIs and Corporate Advisory KRIs where each KRI is reported according to their respective timelines on a monthly, quarterly, semi-annual and annual basis.
3. REs may refer to the table of each KRI category to determine applicability of REs that are required to report the KRIs.
4. REs can only amend each KRI submission up to three times. All late KRI submissions and amendments made to the prior submission (up to three times) will prompt REs to provide justifications.
5. The following paragraphs are examples and types of information that warrant for the count to respective KRI reporting:

Generic KRIs

1. Scope for reporting generic KRI #1 “Number of application fraud near-miss”

   (a) For BIs :

   Remittance/cheque book/trading bill applications must not be included in the KRI.

   (b) For ITOs:

   (i)“Application” here refers to insurance proposal (proposal form);

   (ii) The KRI includes new policy, upgraded policy application, reinstatement of insurance, endorsement, claim applications etc.;

   (iii) The KRI only captures confirmed fraud cases;

   (iv) New agent application / registration or employee application / staff recruitment must not be included in this KRI

2. For generic KRI #2 “number of reprimands received from other regulators/ enforcement agencies/ operator of designated payment systems”, the type of reprimands to be reported as KRI:

   (a) Includes only severe formal and/or official written reprimands from other regulators that are substantiated with documentation are to be reported as KRI in ORR system irrespective of monetary or non-monetary penalty imposed. Reprimands received directly from the Bank (e.g. Statistical Department, Consumer Market Conduct) are not required to be reported in this KRI.

   (b) Excludes all administrative penalties / reprimands from other regulators such as penalty for late tax payment.

3. Scope of reporting for generic KRI #3 “Number of New Litigation Cases Initiated against the FI”:

   (a) Where FI was served with Letter of Demand (LOD), to report in the KRI;

(b) Where the reported LOD is translated into a real litigation, FIs are not required to include in the following quarter;

(c) Where FI was served with a court order without prior LOD, FIs are to report this in the KRI;

(d) Industrial Court related cases - For cases initiated by staff / ex-staff, only cases which are unable to be resolved through reconciliation proceedings and subsequently referred to the Court are deemed litigation cases that has to be reported under this KRI; and

(e) Insurance claims - related litigation are not required to be reported.

4. For generic KRI #4 “staff attrition rate, the turnover rate calculation also includes deceased and/or staff that has retired in the quarter.

5. For generic KRI #6 “new audit findings”, any supervisory / regulatory findings are not included in the KRI count. The timeframe for ‘new’ audit findings involves new audit raised for the first time in last three years.

SNC related KRIs

1. FIs must submit to the Bank on a semi-annual basis, the following leading KRIs pertaining to SNC aspects arising from their business operations and activities:

   (a) For generic KRI #7 “Number of new litigation cases initiated against the FI with SNC implications”:

   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 requirements.

   (b) For generic KRI #8 “Number of new Shariah-related 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).

Technology KRIs

1. Definition of Critical Systems and Critical Services are:

   (a) Critical services = critical business function.

   (b) Critical systems are those systems supporting the critical services.

2. Technology KRI #3 “Number of instances response time for critical services exceeded predetermined threshold / SLA” refers to system response time (from the moment an instruction is entered into the system until the user gets the system response). This KRI intends to capture the delay in the response time for SLA between the RE and their customers (outsourcing contracts SLA are excluded).

3. Technology KRI #10 “Number of incidents relating to transactional reporting or updating errors of critical system” is to capture incidents related to errors caused by production system. Any errors caused by human intervention must not be included in this KRI, such as but is not limited to:

(a) Erroneous financial or transactional reporting computed by staff which could affect decision making, analysis or general understanding of the business by anyone who have access to the report.

(b) Errors in computation or processing of financial transactions by staff which result in customers' accounts being wrongly credited or debited.

(c) Material errors in the total outstanding loan figures or total premiums income reported in the annual report by staff.

(d) Material errors in the financial reporting to the Bank due to wrong computation by staff as at a specific reporting period.

(e) Customers' statements (whether in electronic or paper form) showing wrong account balances or transaction history due to incorrect data maintenance by staff.

(f) Incorrect interest or dividend amounts were credited into customers' accounts due to errors in batch jobs processing by staff.

(g) Customers' policies/statements (whether in electronic or paper form) showing the wrong sum insured, premium amount or transaction history of payments made, where such policies/ statements are maintained by staff - if this is due to programming errors, this can be reported as one incident even though it affects many customers.

Insurance and Takaful KRI

1. The scope of reporting for insurance KRI #1 “Instances of delay in issuance of policies” for number of policy issuances exceeding 30 calendar days for Motor and 60 calendar days for Non-motor calculated from the acceptance of risk until issuance of policies as follows:

   (a) for Motor, acceptance of risk refers to the date the cover note was issued;

   (b) for Non-motor, acceptance of risk refers to the policy inception date; and

   (c) the 30 days for Motor and 60 days for Non-motor refers to calendar days.

2. The scope of reporting for insurance KRI #2 “Instances of delay in payment of claims” is referring to the payment of claims >35 working days from receipt of the last supporting document for the claim assessment. For example, receipt of medical reports and/or final adjusters’ report until issuance of a payment voucher includes the issuance of claim advice which can be the last checkpoint if it is regarded the same as a payment voucher. The KRI is applicable to all recipients of claims paid out, including third party claimants (except payment made by the medical claim administrator). The KRI also includes Life and Personal Accident Death claim cases.

3. The scope of reporting for insurance KRI #4 “Number of replacement of life policy / certificate (ROP / ROC)” applies to:

   (a) internal and external ROP / ROC which shall be counted under this KRI; and

   (b) BIs that engage in bancassurance / bancatakaful activity i.e. marketing insurance on behalf of 3rd parties.

4. For the reporting for insurance KRI #7 “Number of delay in death claims” where number of death claims paid > 60 days after the notification date:

   (a) this KRI is applicable to Life and Personal Accident Death claims including Foreign Workers Compensation Scheme; and

   (b) the 60 calendar day timeline will commence upon receipt of notification of the claim irrespective of complete documentation received.

   Please refer to -

   (i) paragraph 12(1) of Schedule 10 of the FSA read together with section 130 FSA; and

   (ii) paragraph 12(1) of Schedule 10 of the IFSA read together with section 142 IFSA.

5. KRI #8 on “Instances of delay in appointing licensed / in-house adjuster” where the appointment was done >7 working days from receipt of completed claims document[22]. This is only applicable for cases that require REs to appoint licensed adjusters / in-house adjusters, based on the internal policies and procedures of REs.

Complaint KRIs for Banking and Insurance & Takaful Operators

In addition to the Policy Document on Reporting Requirements on Statistical Report of Complaints Statistics issued on 31 October 2019 and effective from 1 January 2020, REs must comply with the following requirements:

1. For “Others” types of complaint, REs must specify the main type of complaint that contributed to “Others”;
2. For all Complaint KRIs, REs must specify the main type of services that contributed to “Other Services”, and for “Other Services” to be reported under “Others”, REs must specify the nature/type of the complaint;
3. For all Complaint KRIs, REs must specify the main type of products that contributed to “Other Products” and for “Other Products” to be reported under “Others”, REs must specify the nature / type of the complaint; and
4. REs must ensure that the “Total number of complaints closed within SLA” does not exceed the “Total number of complaints received”.

Treasury and Corporate Advisory KRIs

1. Transactions in the following products are reportable for Treasury KRIs

   (a) Foreign Exchange and Foreign Exchange Derivatives;

   (b) Fixed Income Securities i.e., Government related and Private Debt Securities (including Exchange-Traded Bonds);

[22] Refer to the requirement in the BNM/RH/GL 003-9 Guideline on Claims Settlement Practices (Consolidated) and BNM/RH/GL004-17 Guideline on Claims Settlement Practices (Consolidated) Takaful

(c) Money Market Instruments;

(d) Equity i.e., both Over the Counter (OTC) Derivatives and Exchange Traded Equity and Equity Derivatives e.g. Shares, Warrants, Funds, Index Futures, Options. For avoidance of doubt, this excludes retail and institutional broking transactions;

(e) Commodity i.e., both Over the Counter (OTC) Derivatives and Exchange Traded Commodity e.g. Futures, Options; and

(f) Exchange Traded Financial Derivatives e.g., KLIBOR and Malaysian Government Securities (MGS) Futures.

2. Transactions reportable for Corporate Advisory KRIs cover all capital market business activities and/or activities which involve Material Non-Public Information (MNPI) in general. This will include conventional banks that have investment banking businesses and exposure to MNPI.

3. Further details in relation to reporting Treasury KRIs are as stated below:

Table 72: Further details for reporting treasury key risk indicators

Treasury KRIs	Notes and Examples
Number of Off-Premise Trades / Deals with Immediate Trade Capture / Input	This KRI is reportable for: • Trades concluded by dealers outside dealing rooms, but with access to the banking institutions' front office treasury dealing systems (via Virtual Private Network [VPN] or Remote-Dial In) that enables immediate capture/input of trades into the systems. • Immediate is defined as inputting deals into the front-end treasury platforms as soon as dealers are able to and must be at least within the same day. Anything which is not immediate would be considered as late trade. • Working from home is considered off premise dealing. Hence, trades executed by dealers working from home or any other off premise location and are able to immediately capture the trade into the front-end system should be reportable here. • Trades concluded by dealers who are authorised to execute trades off-premise. All unauthorised trades should only be reported under KRI on Number of Dealer Mandate Breaches. • Trades concluded at alternative sites e.g., Disaster Recovery and Business Continuity Plan sites, where the infrastructure (supervision and oversight of dealers, record-keeping of communication channels, trading policy,

Treasury KRIs	Notes and Examples
	procedure and controls) of these sites differ from the banking institutions' main dealing sites. If Alternate Site mirrors main site (infrastructure, supervision etc.), then it is not considered as an off-premise location and would not be reportable under this KRI.
Number of Off-premise Trades / Deals Without Immediate Trade Capture / Input	• For clarity, this refers to trades concluded by dealers outside dealing rooms but are unable to immediately capture/input trades into the banking institutions' front office treasury dealing systems for any reason (such as but not limited to no access to VPN/Remote dial-in at the time of concluding the trade). • Immediate is defined as inputting deals into the front-end treasury platforms as soon as dealers are able to and must be at least within the same day. Anything which is not immediate would be considered as late trade. • Trades concluded by dealers who are authorised to execute trades off-premise are also reportable under this KRI. All unauthorised trades should only be reported under KRI on Number of Dealer Mandate Breaches. • Working from home is considered off-premise dealing. Hence, trade executed by dealers working from home or any other off-premise location where such trade cannot be immediately captured into the front-end system should be reportable here. Examples: 1. Dealer A is working from home. He does not have access to the banking institution's front-end treasury deal capture system. Upon executing a trade via his mobile phone, he contacts a colleague in the office to capture this trade in the front-end treasury dealing system on his behalf. This instance should be reported under this KRI. 2. Dealer A concludes a trade outside the dealing room. He does not have access to the banking institution's front-end treasury deal capture system. He then waits until the next day when he is back in office to capture the trade in front end system. This instance should be reported under this KRI as it is considered an off-premise trade. Additionally, it must be reported under KRI

Treasury KRIs	Notes and Examples
	relating to after-hours/ late trade input/capture should it also be considered an after-hours/late trade input.
Number of Late Trade/ After Hours deals	• Delay in input is defined as any trade that is not captured into the front-end system at least within the same day of the trade. • After hours are deals / trades executed outside individual banking institution's permitted trading hours. • All instances of after-hours or late trade input regardless of whether approval was received or not is reportable under this KRI. • Trades arising from servicing Appointed Overseas Offices (AOO) trades after-hours are not reportable under this KRI. Example: Banking institution A has in place a policy for trade execution and capture between 8 a.m. and 6.30 p.m. daily. As such, any trades executed and/or inputted into treasury dealing and trading platforms before 8 a.m. and after 6.30 p.m. must be reported under this KRI.
Number of trade / deal cancellations and amendments (C&As)	Examples of C&As that must be **excluded** are: • C&As due to 3rd party e.g. customer, broker and/or counterparty instructions. * • Duplicative C&As caused by multiple entries into various front, middle and back treasury systems. • Product-driven C&As i.e., multiple or duplicative C&As for the same trade/deal with multiple legs and/or associated transactions. *C&As due to 3rd party customer instructions that is indicative of suspicious activity must be included in this KRI reporting (e.g., frequent C&A arising from customer instructions with same dealer)
Number of mismatches during the confirmation process	Note: • Banking institutions must report instances regardless of their status i.e., mismatches carried over from previous reporting period if still outstanding and/or new mismatches whether

Treasury KRIs	Notes and Examples
	outstanding or was rectified during the current reporting period.
Number of failed trade reconciliations between Front Office and Back Office	Note: • This KRI is intended to capture breaks in straight through processing of trades/deals between the bank's Front Office and Back Office. • Banking institutions must report instances regardless of their status i.e., outstanding failed reconciliations carried over from previous reporting period and/or new unreconciled trades whether outstanding or was rectified during the current reporting period.
Number of instances – ad hoc request to increase Board-approved trading limits	To include instances: • Where dealers share limits with other dealers • Reallocation of limits between branches • All ad-hoc requests regardless of whether it was approved or not approved must be reported in this KRI. • This refers to ad-hoc request to increase any and all limits that are approved by the Board, regardless of whether that limit is at Group/Entity/Department level. • Refers to both trading and non-trading activity limits e.g. liquidity/corporate treasury business activities.
Number of dealer mandate breaches /unauthorised trading	• This must exclude instances of limit breaches, which is presently captured in other KRIs. • Any unauthorized trading must be captured under this KRI. • Breaches as a result of test transactions or other similar circumstances which are executed with approval from higher authority must be excluded as this does not constitute a breach of a dealers' mandate. Higher authority typically refers to the Head of Department or oversight committees such as asset and liability committee etc. • Technical breaches must be included and reported under this KRI.

Treasury KRIs	Notes and Examples
Average Breakdown of dealer's Working from Home (WFH)	• Banking institutions must ensure that the percentages reported in KRIs relating to WFH and Work from Alternative Sites (WFA) and percentage of dealers working from main dealing site equate to 100%. • For example, in the event dealer's WFH is 30% and dealers WFA is 20%, it would consequently imply that 50% of dealers are Working from Office (Main Dealing Site). • There are various operational and conduct risks associated with flexible working arrangements. Given the move towards accommodating such arrangements on a more permanent basis for dealers, this KRI will allow on-going and consistent tracking of the extent of that risk, and whether internal policies and processes suffice vis-à-vis the extent of flexible working arrangements for banking institutions.
Average Breakdown of dealer's Working from Alternative Sites (WFA)	• Banking institutions must ensure that the percentages reported in KRIs relating to WFH and WFA and percentage of dealers working from main dealing site equate to 100%. • For example, in the event dealer's WFH is 30% and dealers WFA is 20%, it would consequently imply that 50% of dealers are Working from Office (Main Dealing Site). • WFA covers all the bank's alternate working sites apart from the main office and WFH. • There are various operational and conduct risks associated with flexible working arrangements. Given the move towards accommodating such arrangements on a more permanent basis for dealers, this KRI will allow on-going and consistent tracking of the extent of that risk, and whether internal policies and processes suffice vis-à-vis the extent of flexible working arrangements for banking institutions.
Number of incidences/disruptions during flexible working arrangements	• All operational incidences and disruptions to trading activities throughout the trade cycle (i.e., front middle and back office) during flexible working arrangements must be reported under this KRI, regardless of whether it has resulted in a Loss Event.

Treasury KRIs	Notes and Examples
	• All incidences whether severe, minor (e.g., temporary electricity black outs, temporary VPN connection issues etc), internal, external, or intermittent are reportable. Banking institutions should put in place policies to track such instances.
Number of Trade and Communication Surveillance Cases	• Amongst others, this KRI must include cases arising from off market rate reports, position parking, insider dealing, wash trading and front running. • Further investigation typically entails reviewing other sources for more information such as communication channels and other surveillance reports (e.g., securities holding period reports) for potential market abuse or misconduct. Where a trade surveillance alert is further investigated for AML/CFT concerns, it also represents an alert that is further investigated and hence is reportable under this KRI. • This is typically alerts which are Level 2 and above and includes all trade and communication surveillance performed by the banking institution. This requires surveillance analysts to conduct further checking e.g., to enquire from dealers etc. • Banking institutions must provide a summary of the instances reported for that period in the description box i.e., scenario detected, outcome of further review/investigation and status of the case.
Number of consequence actions taken against dealers	• All consequence actions must be included in this KRI, whether it relates to wholesale conduct or not e.g., breaches of the banking institutions' code of ethics and professionalism. • Examples of consequence actions include, but are not limited to verbal and written reminders, letters of caution, verbal and written warnings, any impact to remuneration and/or dismissal and termination of employment, etc.

4. Further details in relation to reporting Corporate Advisory KRIs are as stated below:

Table 73: Further details for reporting corporate advisory key risk indicators

Corporate Advisory KRIs	Notes and Examples
Number of breaches in handling of confidential information policy and procedures	• For clarity, these are breaches involving the relevant policies and procedures to govern the flow of information within the banking institution, which include, but are not limited to, the Chinese Wall policy, Wall-Crossing procedures, delay or non-classification of securities on the banking institutions' Watch, Grey and/or Restricted Lists outside permitted thresholds, breaches of the bank's Conflict of Interest frameworks, as well as breaches involving potential Insider Dealing and/or Front Running. • Watch, Grey and/or Restricted List refers to a list of securities maintained by banks whereby the bank is in possession of potential Material Non-Public Information (MNPI) in relation to the issuer, by virtue of its advisory business. Typically, relevant employees are prohibited from trading securities on these lists depending on their exposure to MNPI. • This KRI is reportable for all entities and staff that the confidential information policy or MNPI policy is applicable to. The KRI reporting source must originate from the policy owner or owner of MNPI.
Number of breaches in Personal Account Dealing policy and procedure	• For clarity, these are breaches involving policies and procedures that have been set by banking institutions themselves to govern employee's personal dealing activities which include, but are not limited to: a. maintenance of brokerage accounts (if any restrictions apply as per bank's internal policy); b. requirements to obtain pre-approvals prior to dealing (e.g. breaches to amount approved, validity of approval period); and c. periodic declaration of holdings (e.g. absence or incomplete declarations).

Corporate Advisory KRIs	Notes and Examples
	• This KRI is reportable for all entities and staff that the Personal Account Dealing Policy is applicable to. The KRI reporting source must originate from the policy owner or the custodian of the personal account dealing process.