BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

ORR Frequently Asked Questions (FAQ)

Issued on: 30 January 2026

Version Control / Change History

No.	Date of Issuance	Remarks / Summary of Changes
1	10 April 2025	Original Creation – ORR Frequently Asked Questions (FAQ)
2	30 January 2026	Updated and refined responses for FAQ #39 and #41 on Customer information breaches event reporting

Please note: These FAQs supersede the previous FAQs under ORION PD. The relevant FAQs under the ORION PD have been enhanced and included in these FAQs.

Contents

Glossary

Abbreviation	Full phrase
BNM	Bank Negara Malaysia
ORR	Operational Risk Reporting
PD	Policy Document
RE	Reporting Entity
SO	Submission Officer
LED	Loss Event Data
KRI	Key Risk Indicators
CISS	Cyber Incident Scoring System
BDSF	Business Disruption and System Failures
MCIPD	Management of Customer Information and Permitted Disclosures
FSA	Financial Services Act 2013
IFSA	Islamic Financial Services Act 2013
DFIA	Development Financial Institutions Act 2002
SNC	Shariah non-compliance
BCP	Business Continuity Plans

Registration of ORR users

1. **What are the types of user access an RE must create / obtain in ORR?**
   An RE must create / obtain access for the following types of user:
   i. RE Oversight Officer
   ii. RE Admin / RE Approver
   iii. Submission Officer (SO)

   Each RE must ensure the relevant staff are identified for the above roles. Please refer to Para 10 of the ORR PD for the roles and responsibilities of ORR users and Chapter 1 of ORR RE USER GUIDE DOCUMENT for the definition of each role.

2. **How many user access IDs are granted to each RE for ORR?**
   Each RE is granted the following number and type of user access IDs:
   i. Maximum of 1 ID for RE Oversight Officer
   ii. Maximum of 2 IDs for RE Admin / RE Approver
   iii. Maximum of 10 IDs for SOs.

3. **For REs that operate as part of a financial group, can a user assume the same role (i.e., RE Admin, SO) for more than 1 entity within the financial group? And how will this affect the calculation of number of roles within an entity?**
   Yes, the same user / staff can assume the same role for more than 1 entity within the financial group. The calculation of roles will be based on the number of access roles, NOT number of user / staff. Please refer to the illustration below:

ABC Bank Group comprises ABC Bank Berhad, ABC Investment Bank Berhad and ABC Islamic Bank Berhad.

SO Role

Staff Name	RE Name of the staff	SO Role		
		ABC Bank Berhad	ABC Investment Bank Berhad	ABC Islamic Bank Berhad
Staff 1	ABC Bank Berhad	√	√	√
Staff 2	ABC Bank Berhad	√		
Staff 3	ABC Bank Berhad	√		
Staff 4	ABC Bank Berhad	√		
Staff 5	ABC Bank Berhad	√		
Staff 6	ABC Investment Bank Berhad	√	√	√
Staff 7	ABC Investment Bank Berhad	√	√	√
Staff 8	ABC Investment Bank Berhad		√	
Staff 9	ABC Investment Bank Berhad		√	
Staff 10	ABC Investment Bank Berhad		√	
Staff 11	ABC Islamic Bank Berhad	√	√	√
Staff 12	ABC Islamic Bank Berhad	√	√	√
Staff 13	ABC Islamic Bank Berhad	√		√
Staff 14	ABC Islamic Bank Berhad			√
Staff 15	ABC Islamic Bank Berhad			√
	Total SO roles utilised by each RE under ABC Banking Group	10	8	8

Note: In this illustration, ABC Bank Berhad has reached the maximum number of SO roles (10) while ABC Investment Bank Berhad and ABC Islamic Bank Berhad can still allocate 2 more SO roles respectively.

RE Admin Role

Staff Name	RE Name of the staff	RE Admin/Approver role		
		ABC Bank Berhad	ABC Investment Bank Berhad	ABC Islamic Bank Berhad
Staff 66	ABC Bank Berhad	√	√	√
Staff 77	ABC Investment Bank Berhad		√	
Staff 99	ABC Islamic Bank Berhad	√		√
	Total RE Admin/Approver roles utilised by each RE under ABC Banking Group	2	2	2

Note: In this illustration, all entities in the financial group (ABC Bank Berhad, ABC Investment Bank Berhad, and ABC Islamic Bank Berhad) have reached the maximum number of RE Admin / Approver roles.

4. **Can the same user (i.e., the same staff) be an RE Admin and an SO?**
   No, the same user (i.e., the same staff) cannot be an RE Admin / Approver and an SO at the same time due to the role segregation of maker (i.e., SO) and checker (i.e., Admin / Approver).

5. **How to register as an RE Admin due to a change of staff assuming the role?**
   If there is a change in RE Admin, please
   i. Notify BNM via the designated Microsoft Forms which can be accessed via 'Regulatees Reporting' page > 'Regulatees Reporting Technical Support' > 'Report Issue'. In the 'Type of Enquiry' field, select 'RE Admin Change Request'.
   ii. The new designated RE Admin to complete self-registration process on Kijang.Net. Please refer to Chapter 3 of ORR RE USER GUIDE DOCUMENT for more details.

   The request will be routed to BNM for approval within 3-4 working days.

   Note: The Microsoft Forms on the nomination of RE Admin must be submitted prior to requesting for access via ORR. If the Microsoft Forms is not submitted, the request will be rejected.

6. **How do I check the status of my RE Admin / Approver request?**
   You may check the status by checking ‘My Workspace’ > ‘My Tray’ > ‘My Request’.

7. **How to register as an SO?**
   The new SO to complete the self-registration process on Kijangnet. Please refer to Chapter 4 of ORR RE USER GUIDE DOCUMENT for more details. The request will be routed to your RE Admin for approval.

   REs are not required to notify BNM for any changes to SOs as BNM's approval is not required for the registration of SOs. It is the RE Admin's responsibility to manage and assign the SOs accordingly.

8. **I have recently resigned from an RE to join another RE. I would like to create a new Kijang.Net account with the new RE. How should I do this?**
   A user's Kijang.Net account is tied to his / her NRIC and mobile phone number that were used during the registration process (not email address). As such, if a user needs to create a new Kijang.Net account in a new RE after resigning from the previous RE, the user's existing account has to be deprovisioned first by the RE Admin from the user's previous RE. Once deprovisioned, user can now create a new Kijang.Net account.

Technical troubleshooting

9. **How do we communicate with BNM on technical enquiries pertaining to ORR?**
   For technical issues in accessing Kijang.Net (e.g., log in issues) please direct your queries / communications to kijangnet_help@bnm.gov.my
   For technical issues within the ORR module (e.g., submission errors), please submit them via the designated Microsoft Forms which can be accessed via 'Regulatees Reporting' page > 'Regulatees Reporting Technical Support' > 'Report Issue'. In the 'Type of Enquiry' field, select 'Technical Issue'.

10. **How do I access the ORR system?**
    To access the ORR system, log in to Kijang.Net > 'Regulatees Reporting'. If you have not already completed the registration process, please refer to ORR RE USER GUIDE DOCUMENT for more details.

11. **How do I access the LED and KRI modules for submission in the ORR System?**
    To create / submit LED, the LED module can be accessed either via:
    i. 'Regulatees Reporting' page > 'Create New LED'; or
    ii. 'My Workspace' > 'Submission Summary' > 'Submission Monitoring Screen' > select 'Loss Event Data' in the 'Regulatees Subject Area' > Search
    Please refer to Chapter 9 of ORR RE USER GUIDE DOCUMENT for more details.

    To create / submit KRI, the KRI module can be accessed via:
    i. 'My Workspace' > 'Submission Summary' > 'Submission Monitoring Screen' > select 'Key Risk Indicator' in the 'Regulatees Subject Area' > Search
    Please refer to Chapter 10 of ORR RE USER GUIDE DOCUMENT for more details.

    Note: The LED module for submission can be accessed from either the 'Regulatees Reporting' page or 'Submission Monitoring' page but the KRI module can only be accessed from 'Submission Monitoring' page.

12. **I am not able to log in on my Kijang.Net account as I have forgotten my password. What should I do to recover my forgotten password or create a new password?**
    Please select 'Forgot password' at the login page. A temporary password will be sent to your registered mobile phone number. Please log in with the temporary password immediately after receiving it as it has a time limit. Once the temporary password has expired, you will not be able to log in with it anymore and you will need to select 'Forgot password' again.

13. **My Kijang.Net account has been locked. Why did this happen and what should I do next?**
Your account may be locked due to:
   i. user inactivity (i.e., user has not logged in for more than 90 days); or
   ii. 3 attempts of incorrect password

If you are an SO, please request your RE Admin to unlock your account.
If you are an RE Admin, please email to oprisku@bnm.gov.my to unlock your account.

14. **I have SO access for LED submission but I'm not able to see some / any portfolio in my LED submission monitoring screen.**
It is likely that you have not been assigned to the portfolios under the LED. Please check your portfolio screen. If the relevant portfolio is not there, please liaise with your RE Admin to assign the relevant portfolio to SO. Kindly refer to ORR RE USER GUIDE DOCUMENT for more details.

15. **Some dropdown selections are empty in the LED / KRI submission fields. What should I do next?**
Please clear your browser cache and try again. If that doesn't work, try browsing in a private window. If that still doesn't work, it could be a system issue. Please raise it via the designated Microsoft Forms.

16. **Is there an audit trail of the changes made in previous submissions?**
Yes. Please refer to Chapter 8 of ORR RE USER GUIDE DOCUMENT for more details.

17. **How do REs amend previous submissions?**
   i. To amend previous LED submissions, please refer to Chapter 9 of ORR RE USER GUIDE DOCUMENT
   ii. To amend previous KRI submissions, please refer to Chapter 10 of ORR RE USER GUIDE DOCUMENT

18. **Do REs need to notify BNM of the changes to previous submissions made in ORR?**
No.

General

19. **How do we communicate to BNM on any enquiries pertaining to ORR policy requirements?**
For queries / communication on policy requirements, please submit them via the same designated Microsoft Forms. In the 'Type of Enquiry' field, select 'Feedback or Query on Operational Risk Reporting ORR) Policy Document'. Alternatively, please email to oprisku@bnm.gov.my

20. **There is a high volume of data this month. Can we request for an extension of the LED / KRI submission deadline?**
There will be no extension granted. Please email to oprisku@bnm.gov.my to notify BNM of the late submission and please provide justifications.

Bulk Submission

21. **What is bulk submission channel?**
Bulk submission channel allows REs to submit LEDs in bulk instead of performing individual LED submission in ORR system. For example, REs have the option to submit LEDs about voluminous credit card frauds in bulk to minimise the time and efforts needed should the information be submitted individually to ORR System. For REs that wish to participate in bulk submission for ORR, please notify oprisku@bnm.gov.my

22. **How do I submit LEDs via the bulk submission channel?**
Please refer to Chapter 9 of ORR RE USER GUIDE DOCUMENT for more details.

23. **I'm getting an error when performing bulk submission. What should I do next?**
It could be that you are not utilising the latest technical specification file for ORR bulk submission channel. Please check your email as the latest file will be shared with the existing bulk submission participants via oprisku@bnm.gov.my from time to time. Bulk submission participants may also reach out to oprisku@bnm.gov.my to validate your technical specification file.

LED reporting

General

24. **I can't find the reporting categories in Table 2 – 'Operational risk information reporting deadlines' in the ORR system for me to select when I want to submit a new LED. Only the reporting categories in Table 3 – 'ORR LED reporting types and deadlines' are available. How do REs report loss event categories in Table 2 then?**
Categories under Table 2 are not meant to be separate standalone categories from Table 3, where the reporting format would still follow Table 3. The main purpose of Table 2 is to provide guidance for REs to determine the reporting deadline for certain operational loss events that may warrant an accelerated reporting (earliest deadlines of Table 2 or Table 3).

25. For event reporting categories with financial losses threshold (refer examples below), what is the basis of the threshold? Is it based on Gross Actual Loss, Net Actual Loss, or Amount Involved?

Examples:

Table 2

- *≥ RM1 mil*

Table 3

- *≤ RM5K (Aggregate card / mobile payment fraud)*
- *≤ RM1,000 or >RM1,000 (other loss event)*
- *≥ RM200k or <RM200k (physical robbery)*
- *≥ RM1 mil or < RM1 mil (overseas loss event)*
- *Event with no financial losses*

For all categories except payment-related fraud, the threshold is based on Gross Actual Loss amount before recovery. Please refer to the illustrations below on other loss event for additional clarity:

No.	Scenario	Reportable category	Rationale
1	Gross Actual Loss of RM700	Other loss event →Other than Fraud events→ Other Aggregate Actual Loss Event ≤ RM1000	Gross Actual Loss ≤ RM1,000
2	Gross Actual Loss of RM2,000 and recovered RM800, with Net Actual Loss of RM1,200	Other loss event →All other actual individual event →Event with financial losses > RM1,000	Gross Actual Loss >RM1,000
3	Gross Actual Loss of RM2,000 and recovered RM1,500, with Net Actual Loss of RM500	Other loss event→All other actual individual event→Event with financial losses > RM1,000	Gross Actual Loss >RM1,000
4	Gross Actual Loss of RM2,000 and fully recovered with Net Loss RM0	Other loss event→All other actual individual event→Event with financial losses > RM1,000	Gross Actual Loss >RM1,000 Although Net Actual Loss is 0, this is still considered a financial event, and should not be reported as 'Event with no financial losses' (even if non-financial impact is medium or high)
5	Gross Actual Loss of RM0 (no financial impact), with medium or high non-financial impact	Other loss event→All other actual individual event→Event with no financial losses	This is a genuine event with no financial impact as Gross Actual Loss is 0

For payment-related fraud, the threshold is based on Amount Involved. For example, a credit card fraud with Amount Involved RM7,500 and Gross Actual Loss of RM3,200 must not be aggregated as the Amount Involved is > RM5k. Instead, this event must be reported as single event to ORR.

26. It is noted that some OR events are only reportable for 'Actual Event with Actual Loss' (refer examples below) whereby REs must confirm the event to be an Actual Event first before reporting in ORR. However, if the reporting deadline is based on the date of detection of the event (i.e., by the 15th calendar day of the following month from the date of detection of the event), how should REs report this event since there is a possibility that confirmation of the event can only take place after the deadline?

Examples:

- *Fraud Event→Non-payment related fraud event→Aggregate Actual Loss Event ≤ RM1,000*
- *Other loss event→Other than fraud events→Other Aggregate Actual Loss - Event ≤ RM1,000*
- *Other loss event→All other actual individual event→Event with financial losses > RM1,000*
- *Overseas loss events→Individual event ≥ RM1 million*

Based on Table 3, all the events above have a reporting deadline by the 15th calendar day of the following month from the date of detection of the event.

The reporting deadline is based on the date of detection to encourage REs to promptly investigate and confirm the occurrence of OR events (Actual event) and report them accordingly. Generally, this deadline should provide enough time for REs to complete the investigation.

In terms of actual loss, as long as REs can already confirm that an actual loss is incurred (without finalising the amount yet), REs should already be reporting it in ORR. REs can update the amount in ORR upon finalisation of the amount.

Nevertheless, for events that may require more time for REs to investigate which may cause REs to exceed the stipulated deadline, REs are advised to report the event as Actual Event first in the ORR system before confirmation of its event classification. If the event is subsequently confirmed to be a Near Miss Event, REs can withdraw the event from ORR system. Otherwise, if the event is reported after the deadline, please provide clear justifications in the LED report on the reason for late reporting (e.g., due to investigation / pending client response, etc).

27. If an OR loss was driven by an activity that involves processing of remittance, should REs select the business line category 'Payment & Settlement'?

REs must select the business line category that most accurately describe the business that bears the loss. Nevertheless, it should be noted that the business line category selected must be an income-generating function for the REs. In this regard, 'Payment & Settlement' business line should only be selected by REs if it is an income-generating function e.g., the REs' payment and settlement business charges fees for its service.

28. **Do events that occurred outside REs' premises need to be reported too?**
Yes, as long as the OR event is within the context of Table 2 – 'Operational risk information reporting deadlines' or Table 3 – 'ORR LED reporting types and deadlines'.

29. **In an event which causes / involves multiple different reportable operational risk events in the ORR system, should REs report as one or multiple separate events?**
REs to report each event as separate reportable OR events. The 'Submission ID Link' function can be used to link those reportable events. Please refer to Para 17.5 and 17.6 of the ORR PD for some examples.

30. **Are regulatory actions such as fines, penalties, or reprimands – whether monetary or non-monetary – reportable to ORR?**
Yes, all regulatory fines and monetary penalties are operational losses for REs regardless of the underlying cause and must be reported. This includes all monetary penalties imposed by BNM or other regulators, enforcement agencies, or authorities such as Securities Commission, Inland Revenue Board, Personal Data Protection Commission, city halls and city councils, etc.
Reprimands received by REs that do not involve monetary penalties must also be reported under the category 'event with no financial loss' if the non-financial impact is assessed to be medium or high
If the regulatory actions arise from another reportable OR event, please report each event as separate reportable OR events and link those events using the 'Submission ID Link' function.

31. **Do REs need to report gains?**
No.

Cyber incident and event reporting

32. **Is it necessary to submit an ORR report if REs have already sent a CISS form to mylod@bnm.gov.my?**
Yes, as of now, REs are still required to submit an ORR report on cyber incidents in addition to a CISS form submission.

33. **Are REs required to submit the total count of all spam emails that was identified by spam filter but did not get through?**
Yes, please refer to Appendix 3 - Para 6 under cyber incident and event reporting types for examples of cyber events reportable under the technology KRI reporting.

34. **Can REs utilise the same severity level definitions for both cyber incident and cyber event?**
No, the definition for a 'cyber incident' is distinct from that of a 'cyber event'. Please refer to Appendix 3 - Para 4 in ORR PD for the interpretation of these definitions and examples, which provide guidance on classifying which cyber events need to be reported.

35. Should malware, malicious files, failed logins, and similar incidents that have been blocked be reported to BNM as near-miss cyber events if they have been identified as actions performed by high-profile threat actors?

The high volume of day-to-day alerts / blocking activity by cyber security solutions should be reported as aggregated value under technology KRI reporting requirement (Appendix 16, Table 65). Nevertheless, if any of these cyber attempts fits the examples provided in the PD (that includes attempts performed by high profile threat actor), they will need to be reported under Appendix 3 – Cyber incident and event reporting requirement.

BDSF event reporting

36. If a system disruption has impacted both conventional and Islamic entities, how would the reporting of such event be done in ORR?

Please submit two separate LED reporting for each entity. Any financial loss resulted from the event must be split accordingly.

37. Are 'minimal' system failures resulting from batch overruns for few minutes required to be reported in ORR?

Yes, system failures resulting from batch overruns regardless of short or long duration, is required to be reported in ORR.

38. What is the definition of 'Main Branch' or 'Processing Hub' in reporting a business disruption event in ORR?

For ORR reporting purposes, RE's main branch or processing hub refers to a unit or function where there are significant business operations taking place and / or dependence to support the functionality of the RE's operations i.e., centralised operations centres.

Customer information breaches event reporting

39. What is the applicable timeline for reporting of incident on "Breach of the MCIPD" as it is not considered as customer information breaches whereby no tabling to the Board is required? Should it be treated the same as other loss event timeline i.e., By the 15th calendar day of the following month from the date of detection of event?

Under the MCIPD, customer information breaches are defined to be incidences of theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information. Should any of the above occur, REs must investigate and table the detailed investigation report to the Board. If the customer information breach falls under any of the three (3) following scenarios, REs must submit the detailed investigation report to BNM on T+1, where T is the date where the investigation is tabled to the Board:

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.

There is no difference in timeline for reporting a customer information breach, regardless of whether it is deemed to be a breach of the MCIPD, breach of the FSA / IFSA / DFIA or breach of both.

40. Should each customer information breach incident be reported on individual submission regardless of the non-financial impact which could be assessed as low impact as per REs' internal policies.

Each customer information breach is to be reported on individual submission regardless of the non-financial impact.

41. Regarding a customer information breach that warrants an immediate notification to BNM as per MCIPD, does the ORR reporting deadline still remain as 1 working day after tabling of investigation to Board (investigation can take up to 3 months upon detection of breach as per Para 11.8 of MCIPD)

REs must investigate and report the incident on T+1, where T is the date where the investigation is tabled to the Board. Where the customer information breach is likely to pose reputational risk to REs or a threat to public confidence and trust, REs must notify BNM immediately upon discovery of the breach, followed by the submission of the details of the incident via ORR on T+1.

42. Should REs report the date of investigation tabled to Board in the ORR system?

In ORR system, there is no data field to capture the date of investigation tabled to the Board. Therefore, REs are required to only report the date of occurrence, date of detection and date of confirmation as per the definition under the ORR PD.

43. Is disclosure of customer information to an appointed consultant considered a breach of MCIPD or FSA / IFSA / DFIA?

The disclosure of customer information to an appointed consultant will not be considered a customer information breach if the disclosure to the consultant has been approved by BNM or falls under the list of permitted disclosures under Schedule 11 of the FSA and Part C of the MCIPD. If the disclosure to the consultant has not been approved, or does not fall under any of the permitted disclosures, it will be a breach of both the FSA / IFSA / DFIA and the MCIPD. Any further disclosure by the unauthorised consultant will also be a breach of both the FSA / IFSA / DFIA and MCIPD.

<u>SNC event reporting</u>

44. On the requirement to conduct ad-hoc Board meeting to meet the 30-day period to obtain Board's approval on the rectification plan, can it be in the form of circularisation?

No. A formal meeting or discussion session must take place. Board's approval in the form of circularisation and/or memorandum is not permissible.

45. On the requirement to submit rectification plan approved by the Board within 30 calendar days, can it be a principle-based / brief plan?

In order to meet the 30-day period, the rectification plan that has to be submitted does not have to be a full-blown plan and it can be of a principle-based plan approved by the Board. However, the detailed rectification plan must be submitted and updated in ORR later.

46. Can REs request for extension should they fail to table the potential SNC event to Shariah Committee within the 14 working days timeline?

REs are strictly required to observe the timeline of the 14 working days. However, any request for time extension needs to be supported with strong justifications and it has to be through a formal request to BNM.

Payment-related fraud event reporting

47. What are some examples of scenario for payment-related fraud that are reportable as Near Miss?

The following are some examples of scenario for payment-related fraud and whether or not they are reportable as Near Miss:

Scenario	Description	Reportable as Near Miss?	Remarks
A	RE implement cooling-off period for transactions that exhibit high risk pattern	Yes	Mitigating control is only applied to specific group of customers that exhibit high risk pattern.
	RE managed to stop transactions as customer did not proceed as cooling-off period kicks-in		
B	RE adopted in-app authentication and migrate away from using SMS OTP authentication	No	Mitigating control is applied to all customers.
	RE noticed reduction in fraud losses involving SMS-related phishing fraud		RE is not able to quantify the amount saved from adoption of in-app OTP because only reduction in actual losses is visible.
C	RE freeze several accounts due to suspicion of involvement as mule account	No	Reporting is applicable to outgoing payment and not applicable to incoming payment.
	RE managed to stop transactions crediting into these accounts.		
D	RE employed fraud detection system and identify account involved in fraudulent transactions	Yes	For payment-related fraud, both the amount involved in fraudulent transactions and account balance is reportable.
	RE blocked the account and saved the remaining balance in the account from further fraud losses		
E	RE employed fraud detection system that detect outgoing transactions potentially to be involved in fraud	Yes	Mitigating control is only applied to specific group of customers that exhibit high risk pattern.
	RE managed to intervene or stopped the transactions		

F	RE implemented mobile shielding application or RASP* that block and prevent application take over. **Runtime Application Self-Protection*	Yes	Mitigating control is only applied to specific group of customers whose device has been compromised

48. If a customer disputes 10 credit card transactions, should it be reported to ORR on a per transaction basis or per customer basis?

The reporting must be per transaction basis. Transactions with Amount Involved ≤ RM5k must be aggregated for reporting to ORR. Transactions with Amount Involved > RM5k threshold must be submitted as a single event to ORR.

49. For events involving fraudulent altered cheque in which the collecting bank has tagged as Non-Conformance Flag in CTCS and fraud did not take place, are these Near Miss events required to be reported to ORR?

No, unless there are additional mitigation actions (e.g. calling up customers to verify on those cheques that are suspected to be fraudulent) taken by the issuing bank to verify if these altered cheques that have been tagged as Non-Conformance by the collecting bank are fraudulent or genuine.

50. Who should report cheque fraud events? Issuing banks or collecting banks?

The issuing bank must report cheque fraud irrespective of whether the loss is borne by the issuing bank or collecting bank. Please input the loss amount accordingly in the designated table fields in ORR system based on whether it is borne by the issuing bank or the collecting bank. You may provide the details of the incident including acquirer's involved (if any) in the loss event description.

51. How do REs report credit card cases (loss and chargeback) whereby the REs can fully recover losses from the Acquirer / Merchant (if it complies with the relevant requirements of Visa / MasterCard)?

Report as Actual Event. Please input the loss amount tied to acquirer / merchant accordingly in the designated table in ORR system.

52. Are REs expected to submit a separate aggregate report by MO or it is to be filled up according to MO, card brand, type of mobile payments, etc in the template / form provided in the system.

REs are expected to submit a separate aggregate report according to type of Card (i.e. Credit Card, Debit Card or Charge Card) and Mobile Payment, each for Actual Event with Actual Loss and Actual Event with Potential Loss (refer to Appendix 7, Table 17).

Overseas loss event reporting

53. For an Overseas loss events ≥ RM1 million, should REs follow the timeline stipulated in Table 3 (by the 15th calendar day of the following month from the date of detection of the event) or Table 2 under 'All reportable OR events' > 'RM1 mil losses' (by T+2 working days, T being the date of event confirmation)

For all operational risk events except for Overseas loss reporting, REs must read Table 2 and Table 3 together to determine the reporting deadline. For Overseas loss reporting, REs only have to follow Table 3. Therefore, all overseas loss reporting deadline is by the 15th calendar day of the following month from the date of detection of the event.

KRI Reporting

Treasury KRI

KRI 2 – Number of Off-Premise Trades / Deals without Immediate Trade Capture / Input

KRI 3 - Number of Late Trade / After-Hours deals

54. **Are these KRIs reportable for instances where dealer executes a trade after hours outside the dealing room and trades are captured on the next business day?**
Any trades that meet the definition of "Off-Premise" and "Late Trade / After-Hours" KRIs as per Appendix 17, Table 72 should be reported under these KRIs.

KRI 3 - Number of Late Trade / After-Hours deals

55. **Is this KRI reportable only for instances where there was a delay inputting the trade e.g., due to oversight or is it reportable under all instances where a trade was inputted late / after-hours e.g., due to counterparty and / or system issues? If internal approval has been received to execute an after-hour / late trade, is this KRI still reportable?**
KRI is reportable for all instances that result in a trade being inputted late and/or after hours as defined in the bank's internal policies. This is regardless of whether internal approval was obtained for such trades.

KRI 4 - Number of trade / deal cancellations and amendment (C&As)

56. **Is this KRI reportable for C&A arising from trader/dealer errors only?**
KRI is reportable for all C&As except those that arise from exclusions specified as per Appendix 17, Table 72 of the ORR PD.

KRI 5 - Total Number of Trades / Deals

57. **Are internal trades e.g., trades undertaken between sales and trading desks reportable?**
For the purpose of this KRI, internal trades i.e., trades undertaken between desks within an entity is not reportable under the total trade count.

58. Is the trade volume for Structured Warrant (SW) Trades listed on Bursa Malaysia required to be reported under this KRI, in terms of the number of purchases on all issued warrants?

KRI is reportable if the SW exposures and trades are booked at the RE.

KRI 6 - Number of mismatches during the confirmation process

59. Is the KRI reportable if trade mismatches are resolved within the same day e.g., due to errors by dealers?

KRI is reportable for any instance of trade mismatch regardless of when it was resolved.

KRI 7 - Number of unconfirmed trade / deals

60. In the scenario where the contract has been affirmed with the client, has already matured, and the counterparty has settled the contract accordingly, but the bank has not received the signed trade confirmation letter, are these instances required to be reported under this category?

This KRI is reportable for circumstances where confirmation (by any means) as required by the bank's internal policy and procedure was not obtained.

KRI 10 - Number of treasury room limit breaches: Board-approved limits

61. Does this KRI encompass only trading activities or both trading and non-trading activities?

This KRI is reportable for all Board-approved limits breaches for both trading and non-trading activities.

KRI 13 - Average Breakdown of dealer's Working from Home (WFH)

KRI 14 - Average Breakdown of dealer's Working from Alternative Sites (WFA)

62. If the WFH / WFA arrangement involves only 1-2 working days, should this be counted in these KRIs? Is there a minimum requirement / threshold for these KRIs?

Reporting of the average breakdown of dealer's WFH KRI is based on the bank's internal policy and procedure. For example, Bank A, based on the bank's internal policy and procedure determines that a dealer WFH for more than 10 days in a calendar month is considered as a full headcount (1) in computing this KRI.

63. Are trades executed from WFH / WFA sites as part of Business Continuity Plans (BCP) reportable?

Any trades executed in WFH / WFA sites are reportable, regardless of the circumstances.

KRI 15 - Number of incidences/ disruptions during flexible working arrangements

64. **If dealers experience issues accessing the treasury booking system, resulting in disruptions to trade booking (this impacts both those working outside the dealing room and those within it), should this also be reported under this KRI category? Does this KRI also apply to trades concluded while WFA, where the setup and controls mirror the bank's main dealing room, or is it only applicable to trades concluded while WFH?**
Any incident that causes disruption to the trading / dealing activities that are undertaken "Off Premises" as defined in Appendix 17, Table 72 is reportable under this KRI.

<u>Corporate Advisory KRI</u>

KRI 2 – Number of submissions rejected / returned by SCM

65. **Should submission under Lodge and Launch Framework or the submission pertains to corporate advisory such as Mergers & Acquisitions (M&A), Initial Public Offering (IPO) & etc be reported under this KRI?**
KRI is reportable for all corporate advisory submissions that have been rejected or returned by Securities Commission Malaysia.

KRI 3 – Number of breaches in handling of confidential information policy and procedures

KRI 4 - Number of breaches in Personal Account Dealing policy and procedure

66. **If instances of Customer Information breaches are already reported under ORR – LED, should this be reported under these KRIs as well?**
Yes, any breach relating to the handling of confidential information or personal account dealing policy and procedure is to be reported under these KRIs.