



**BANK NEGARA MALAYSIA**  
CENTRAL BANK OF MALAYSIA



# Wholesale Market Conduct Practices

Guidance Document

# Contents

## Part A: Overview

1. Introduction .....	1
2. Objective .....	1
3. Applicability .....	2
4. Legal Provisions .....	2
5. Effective Date .....	2
6. Related Legal Instruments and Policy Documents .....	2
7. Documents Superseded .....	2
8. Interpretation .....	3

## Part B: Risk Identification and Surveillance

9. Risk Identification and Assessment .....	6
10. Surveillance .....	9
Trade Surveillance .....	9
Threshold and Parameter Setting .....	10
Communications Surveillance .....	12
Analysis / Investigation .....	14
Personnel and Training .....	15
11. Monitoring for and Investigating Misconduct .....	16
Wash Trading .....	17
Position Parking .....	20
Front Running .....	22
Off Market Rates .....	24
Insider Dealing .....	26

## Part C: Internal Controls and Culture

12. Control Environment in Managing Conduct Risks .....	29
Governance and Reporting .....	30
Front-Middle-Back Office Controls .....	32
i. Entertainment and Gifts .....	33
ii. Broker / Counterparty Relationships .....	34
iii. Mandatory Leave .....	35
iv. Off-Premise and After-Hours Dealing .....	36
v. Business Norms .....	38
vi. Trade Capture, Cancellations and Amendments .....	38
vii. Access to Dealing Room and Systems .....	39
Handling of Inside Information .....	40
i. Chinese Wall .....	41
ii. Personal Account Dealing .....	42
Conflicts of Interest .....	44
Compliance Function .....	46
Internal Audit .....	48
13. The Role of Culture in Promoting Good Conduct .....	49
Remuneration and Key Performance Indicators .....	49
Consequence Management .....	50
Training .....	51

## Appendix & References

Appendix 1 .....	52
Appendix 2 .....	54
References .....	55

## Part A: Overview

### 1. Introduction

- 1.1 Integrity and professionalism by market participants in the conduct of their business, affairs and activities are key elements in maintaining efficiency and public confidence in Malaysia's wholesale financial markets. Financial institutions are responsible in their capacity as market participants to maintain adequate oversight of employees' conduct in the course of their market activities.
- 1.2 Market misconduct can be perpetrated through various methods and is commonly intended to create false impressions that mislead other market participants, allow market participants to profit from inside information, or circumvent internal controls, amongst others.
- 1.3 This document makes a general distinction between two categories of market misconduct:
  - a. Market abuse**
    - Actions or trading with the intent of manipulating market volumes, prices and order books in order to benefit from the resulting market reaction.
    - Attempts to influence benchmark rates, trade ahead of client orders, or take actions based on inside information.
  - b. Unauthorised trading**
    - Also commonly referred to as rogue trading. The financial institution's governance and controls may be deliberately circumvented to support risk-taking beyond authorised limits in search of greater profits.
    - Includes actions in trading which in effect violate the financial institution's internal policies (e.g. those pertaining to securities' aged inventory policy or allowable trading book holding period).
- 1.4 Financial institutions should have mechanisms in place to detect and deter market misconduct. In this regard, an effective surveillance programme is necessary to detect misconduct, while a strong internal control environment serves to deter or prevent misconduct.

### 2. Objective

- 2.1 The Bank takes a holistic view in its supervisory expectations and assessment of controls that financial institutions should have in place to manage conduct risks arising from their market activities across all financial products, and conducts supervisory reviews focused on this area.
- 2.2 Based on the Bank's supervisory findings and observations of banking institutions' practices in Malaysia, this document seeks to provide guidance on managing conduct risks arising from activities in wholesale financial markets, in particular on the following areas:
  - (a) setting up and operating effective trade and communications surveillance programmes over the activities of dealers, as well as typical examples of misconduct that should be in the scope of surveillance; and
  - (b) forming a strong conduct control environment, which includes elements such as conduct risk oversight and reporting, alignment of risk to rewards, segregation of controls and maintenance of information barriers, amongst others.
- 2.3 In the course of the Bank's supervisory reviews, this document will serve as a guide on the wholesale market conduct practices and controls which should be adopted by financial institutions where appropriate. Financial institutions should give consideration to the size and complexity of their operations in determining the design and scope of controls, where higher expectations are generally placed on financial institutions with larger and more complex operations. Practices or controls which deviate from the guidance in this document should demonstrate equal or higher effectiveness in addressing market misconduct risks.

### 3. Applicability

- 3.1 The guidance in this document is contextualised and applicable to the business and operations of licensed banks, licensed investment banks, licensed Islamic banks and prescribed development financial institutions. Other financial institutions such as licensed insurers, licensed Takaful operators and approved money-brokers as well as other market participants are also encouraged to consider adopting the guidance where relevant to their participation in wholesale financial markets.
- 3.2 In general, financial institutions that participate in, or offer services or products in the following financial markets are encouraged to adopt the guidance<sup>1</sup> in this document:
- (a) Foreign exchange market;
  - (b) Money market;
  - (c) Capital market (bond and equity markets);
  - (d) Derivatives market; and
  - (e) Commodities market.
- 3.3 Financial groups are encouraged to adopt the guidance herein and address wholesale market conduct risks holistically across their subsidiaries, and seek to implement group-wide standards of control, adopting the higher local regulatory standards where applicable.

### 4. Legal Provisions

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

### 5. Effective Date

- 5.1 This document comes into effect on 31 December 2021.

### 6. Related Legal Instruments, Policy Documents and Guidance

- 6.1 This document should be read together with other relevant legal instruments, policy documents and guidelines that have been issued by the Bank, in particular:
- (a) Code of Conduct for Malaysia Wholesale Financial Markets;
  - (b) Principles for a Fair and Effective Financial Market for the Malaysian Financial Market;
  - (c) KLIBOR Rate Setting;
  - (d) Corporate Governance;
  - (e) Risk Governance;
  - (f) Employee Screening; and
  - (g) Management of Customer Information and Permitted Disclosure.
- 6.2 This document should be read together with other locally issued guidance (e.g. by the Securities Commission Malaysia, Bursa Malaysia, etc.) as well as international best practices on wholesale market conduct.

### 7. Documents Superseded

- 7.1 This document supersedes the notification on Managing Unauthorised Trading and Market Manipulation issued on 20 November 2015.

---

<sup>1</sup> The guidance in this document is intended to address institutions' proprietary trading and facilitation of client deals to which the institution acts as principal. Discretion should be applied for parts of the document that are not applicable in specific contexts (e.g. equity trading, etc.)

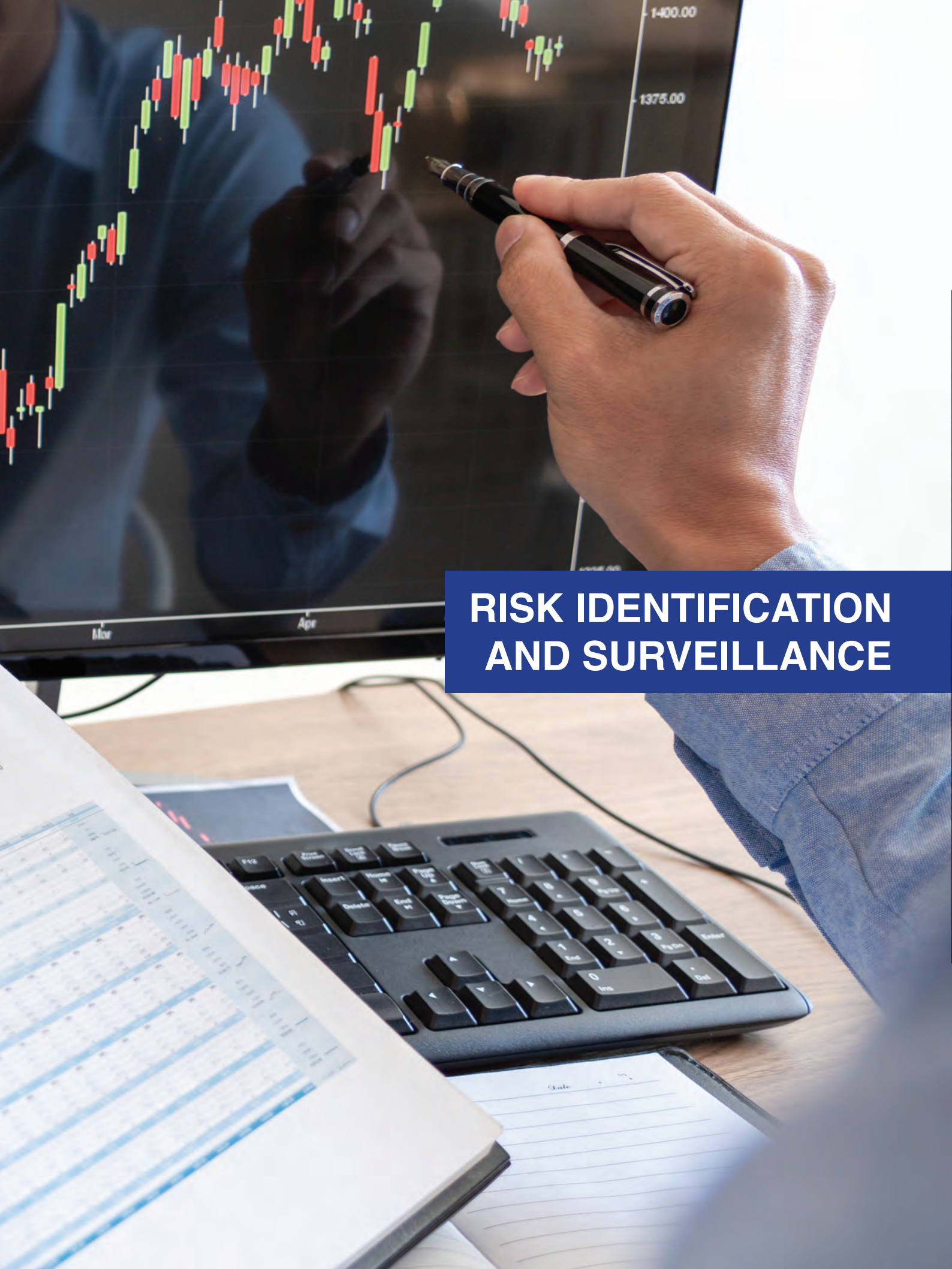
## 8. Interpretation

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

8.2 For the purpose of this document:

<b>“DOs”</b>	refer to good practices observed among banking institutions in the course of the Bank’s supervisory reviews as well as some recommendations for good practice;
<b>“DON’Ts”</b>	refer to poor practices observed among banking institutions in the course of the Bank’s supervisory reviews as well as some practices to avoid;
<b>“brokers”</b>	refer to employees of approved money-brokers who arrange deals between market participants in the wholesale financial markets;
<b>“clients”</b>	refer to market participants entering into transactions and activities with or through a financial institution;
<b>“Code of Conduct”</b>	refers to the Code of Conduct for Malaysia Wholesale Financial Markets;
<b>“deals” or “trades”</b>	refer to transactions in wholesale financial markets;
<b>“dealers”</b>	refer to employees of financial institutions dealing in the wholesale financial markets and may include traders and sales persons of the treasury division of the institution;
<b>“DFIA”</b>	refers to the Development Financial Institutions Act 2002;
<b>“financial product” or “product”</b>	refers to a financial instrument that is traded in the market or transacted with clients and counterparties, including structured products offered by institutions;
<b>“financial institutions”</b>	refer to licensed banks, licensed Islamic banks, licensed investment banks, prescribed development financial institutions, licensed insurers, licensed takaful operators and approved money-brokers;
<b>“FSA”</b>	refers to the Financial Services Act 2013;
<b>“IFSA”</b>	refers to the Islamic Financial Services Act 2013;
<b>“sales dealer”</b>	refers to sales persons of the treasury division of a financial institution; and
<b>“senior management”</b>	refers to the Chief Executive Officer and senior officers of market participants; and
<b>“wholesale financial markets”</b>	refer generally to markets involving transactions between institutions and do not involve retail transactions (e.g. transaction with an individual customer).





## **RISK IDENTIFICATION AND SURVEILLANCE**



IDENTIFY  
RISK

## Part B: Risk Identification and Surveillance

### 9. Risk Identification and Assessment

- 9.1 The first step for institutions in managing conduct risk is to prepare a market conduct risk assessment. This assessment represents a systematic method of identifying financial products traded by the institution and assessing their susceptibility to different types of misconduct, as well as documenting mitigating actions or controls.
- 9.2 The market conduct risk assessment is intended to assist the institution in:
- (a) understanding the market and operational environment for its wholesale market activities;
  - (b) identifying the types of market misconduct applicable to a particular product, and the corresponding level of risk;
  - (c) prioritising the rollout of surveillance of market misconduct where the potential exposure is assessed to be of higher risk;
  - (d) calibrating parameters and thresholds used in surveillance; and
  - (e) ensuring all its traded products have been considered in refining the coverage of surveillance.
- 9.3 The market conduct risk assessment is intended to serve as an input in managing market conduct risk through means of surveillance and other controls. It is not intended to provide an overall assessment of the institution's net market conduct risk exposure. As such, moderating down the assessed risk exposure because of surveillance and controls in place can provide a false sense of comfort.
- 9.4 Factors that institutions can consider in assessing the respective level of risk include, but are not limited to:
- (a) whether the product is traded on an exchange<sup>2</sup> or in over-the-counter (OTC) markets;
  - (b) overall traded volume and number of transactions;
  - (c) distribution of individual transaction sizes (e.g. percentile analysis);
  - (d) changes in (b) and (c) across time periods;
  - (e) market liquidity of the product;
  - (f) operational aspects (e.g. client order handling, mode of settlement) which increase or reduce the susceptibility of a product to certain types of market abuse; and
  - (g) how items (a) to (f) connect to the underlying motives for misconduct.
- 9.5 While business units can provide meaningful inputs on the facets of wholesale financial markets and its products, the market conduct risk assessment should be prepared typically by an internal control function (e.g. Surveillance function, Compliance or Risk Management) given the outcomes outlined in paragraph 9.2 and 9.3.
- 9.6 The market conduct risk assessment must be discussed at the relevant senior management and board committees for better appreciation of the institution's wholesale market conduct risks.
- 9.7 From the Bank's supervisory observations to date, banking institutions are generally lagging in having a properly documented risk assessment on their exposure to market conduct risks, despite already having some surveillance mechanisms in place.

---

<sup>2</sup> Exchange-traded products (e.g. Bursa stocks, futures) have greater market visibility of price, volume and order queue information that are common vectors for perpetrating market abuse.



## Q&A Segment



### What should a market conduct risk assessment look like?



A complete inventory of the institution's traded products would be mapped against the various known types of market misconduct<sup>3</sup>, which are then individually assessed for applicability and susceptibility. This is followed by identifying corresponding controls or surveillance mechanisms to detect and/or deter that type of misconduct. An example of a market conduct risk assessment is shown in **Appendix 1**.



### Is the market conduct risk assessment a static document?



No. The market conduct risk assessment must be periodically reviewed, at least annually, to ensure it remains current.



### The average transaction size for my institution's foreign exchange (FX) deals is small (e.g. RM1,000-RM3,000). Can I interpret that to mean the risk of misconduct is low?



- While relevant, average transaction size is generally of limited value as an indicator of conduct risk.
  - ➔ For FX in particular, low averages are the norm when the scope of analysis includes numerous small customer transactions that typically originate from the institution's branches and do not directly impact the market.
- The potential for specific market abuses, such as front running, may need to be measured using different indicators.
  - ➔ For front running, having a grasp of how big transactions can get and how frequently large transactions occur (i.e. via percentile analysis) is more meaningful.
  - ➔ Non-empirical inputs like operational norms also have a role, for example, requests for market quotes from the trading desk when handling large client orders inherently provides opportunities for front running.
- Institutions are recommended to consider a range of factors as listed in paragraph 9.4 in assessing their susceptibility to different types of market misconduct.

<sup>3</sup> Work published by the UK FICC Markets Standards Board (FMSB) such as 'Behavioural Cluster Analysis - Misconduct Patterns in Financial Markets' (July 2018) provide a source of reference.



**Instead of coming up with a separate risk assessment, will it suffice if conduct risk is already identified and documented in my institution's Risk Control Self Assessment (RCSA)?**



The Bank has observed that conduct risks documented in RCSAs are typically high level and lack the granularity required to inform and benefit the surveillance process. This is in view of RCSAs generally being oriented to serve the purpose of facilitating an aggregated view of the institution's operational risks and corresponding mitigating controls.



**Can institutions perform surveillance without a market conduct risk assessment?**



Having a market conduct risk assessment is necessary to inform an effective surveillance programme and support on-going oversight of a financial institution's management of misconduct risks, both of which are expected elements in the Bank's supervisory assessments. Such assessments should serve to prioritise surveillance scenarios for some types of market misconduct, as well as threshold and parameter setting.



**For global banking groups, would it suffice for the Malaysian entity to rely on a regional market conduct risk assessment?**



Regional assessments are predominantly based on combined data or profile of trading activities of multiple countries, which may not adequately capture the local environment perspective that is key to adapting surveillance thresholds to different locations. Such assessments are also not presented to the respective local senior management and board committees for their oversight.

## 10. Surveillance

- 10.1 Surveillance of dealers' activities is the core pillar supporting an institution's ability to detect market misconduct by its dealers. Such attempts at misconduct may occur despite having relevant policies and a dealers' code of conduct in place.
- 10.2 Each institution should assess its potential exposure to conduct risks arising from its activities in wholesale financial markets, and incorporate that assessment to design and implement an effective surveillance programme covering both dealers' trades and communications.
- 10.3 Surveillance should be performed independently from the business unit, with the function typically taken on by Compliance or Risk Management. A centralised or outsourcing model is common for banking groups, where a surveillance function or hub performs first-level conduct surveillance for entities within the group.
- 10.4 For institutions that choose to retain the setup of surveillance performed by a semi-independent party (e.g. business support unit which still reports to the treasurer), it is important to establish arrangements to preserve the independence of the function from the business unit. The following examples of governance and control practices can prevent undue business influence from hampering effective surveillance or skewing the findings and assessments of the surveillance team:
- (a) establishing a reporting line to an independent function such as Compliance, and reflecting this oversight and accountability through the setting and measurement of the surveillance function's key performance indicators;
  - (b) independent review of surveillance work; and
  - (c) involvement of an independent party when following up on suspected misconduct or approving changes to surveillance parameters and thresholds.

### Trade Surveillance

- 10.5 Trade surveillance refers to the monitoring of dealers' trading activities to detect patterns that are consistent with behaviours commonly associated with market misconduct, or otherwise sufficiently incongruent with past trading behaviour to warrant further scrutiny.



**System**

- The usage of surveillance systems or platforms in trade surveillance is generally encouraged, as such systems facilitate the following outcomes:
  - ➔ Setting of parameters and threshold to flag out instances (alerts) where a single or group of trades exhibit behaviours indicative of market misconduct.
  - ➔ Minimizing human or operational errors that may arise from processing large volumes of trade information.
  - ➔ Tracking of timelines as well as documentation and record retention of analyses performed on surveillance alerts assigned to analysts (i.e. as a case management function). This will also enable quality assurance to be performed on the analysts' work.
- Institutions with substantial trade volume or market participation should have a surveillance system in place.





### System

- Institutions without substantial trade volume may not necessarily need to implement surveillance through a system.
  - ➔ In lieu of purchasing a surveillance system, opting for other means to facilitate surveillance (e.g. Microsoft Excel, in-house platform) may be considered equally effective provided the outcomes outlined above are achieved to the same standard.
  - ➔ The need for a surveillance system should be re-evaluated annually based on the refreshed market conduct risk assessment.
- Systems also allow for dynamic approaches to surveillance, for example applying differentiated thresholds across individual dealers which adjust according to their respective historical trading patterns. This can potentially help to identify anomalies and direct surveillance efforts more effectively.
- Some systems feature ‘machine learning’ capabilities that may facilitate further efficiencies such as filtering surveillance alerts based on past surveillance experience (e.g. alerts which exhibit similar characteristics as those consistently found in past ‘false positive’ alerts may be filtered out from review).

## Threshold and Parameter Setting

- 10.6 Based on the assessed exposure to each type of market misconduct, a set of parameters<sup>4</sup> and thresholds<sup>5</sup> (i.e. surveillance scenario) should be implemented to detect trade patterns or behaviours associated with that misconduct.
- 10.7 In building surveillance capabilities, the number and breadth of surveillance scenarios implemented should be prioritised to address the institution’s core market conduct risk exposures (e.g. those deemed as higher risk).
- 10.8 Surveillance parameters may take on different dimensions (e.g. price, transaction size, time window) that correspond to behaviours indicative of market misconduct.
- 10.9 Arriving at the ‘right’ surveillance thresholds is acknowledged as a matter of some subjectivity, which nonetheless should be supported by documented assessments to reflect the decision-making process and reasonableness of thresholds used. These documented assessments could include but is not limited to consideration of the following:
- (a) the institution’s transaction profile in a particular product;
  - (b) transaction size which would have appreciable market impact;
  - (c) market liquidity of a particular product, stock or currency pair; and
  - (d) nuances associated with the particular type of misconduct under surveillance.
- 10.10 Surveillance thresholds should be reviewed at least annually to ensure they remain relevant and effective in picking up market misconduct. Empirical approaches to calibration should be applied where possible, with careful emphasis to draw the line between reducing the number of false positives and ‘managing the number of alerts’<sup>6</sup>. Examples of calibration techniques that institutions may consider employing are listed in **Appendix 2**.
- 10.11 Surveillance thresholds for specific types of market misconduct are discussed further in section 11 of this document.

<sup>4</sup> Filtering criteria used to isolate records of interest (e.g. minimum transaction size; maximum allowable deviation from market price).

<sup>5</sup> The value assigned to a parameter (e.g. RM5,000 minimum transaction size; 0.5% allowable deviation from market price).

<sup>6</sup> Changes to thresholds in this case are primarily motivated by resource and personnel constraints (i.e. reducing alerts to a manageable level) at the expense of having gaps or reduced effectiveness in surveillance.

## Industry Practices



### DOs

- ✓ Business personnel are not privy to the inner workings of surveillance. Thresholds and parameters are approved independently of the business unit under surveillance.
- ✓ Review or calibration of surveillance thresholds addresses instances of having few or no alerts, as this may indicate ineffectiveness at detecting misconduct.
- ✓ Ensuring surveillance thresholds remain able to detect patterns similar to past cases or experience of potential misconduct (these may not have been actionable cases, but still involved highly suspicious circumstances).
- ✓ Global or regionally set surveillance thresholds are assessed and recalibrated utilising trading profiles and data of the Malaysian entity to ensure appropriateness and suitability vis-à-vis the Malaysian trading environment.



### DON'Ts

- ✗ Adopting off-the-shelf vendor surveillance scenarios and parameters without first assessing whether they are adequate for the institution.
- ✗ For institutions that benefit from global surveillance programmes or centralised group surveillance, there is little involvement by the relevant local teams (e.g. Risk management and Compliance to fully understand key aspects of surveillance that form an essential control to mitigate market abuse and conduct risks).
- ✗ Solely relying on verbal engagements with business experts or personnel for input on surveillance thresholds. Thresholds are not substantiated with empirical studies.
- ✗ Changing thresholds to 'manage' or drive down the number of alerts without consideration of whether the new thresholds have become disconnected from the market abuse under surveillance.

#### Examples:

- ◆ Raising the minimum transaction size to RM50,000 even though sizes of RM40,000 would still be viable to perpetrate market abuse.
- ◆ New thresholds would no longer detect transactions with characteristics similar to those in past alerts where misconduct had been suspected.

- ✗ Setting overly rigid or an excessive number of parameters that must be met for an alert to be generated. This may reduce effectiveness at detecting potential misconduct, and will likely result in no alerts being generated at all.

## Communications Surveillance

- 10.12 Communications surveillance refers to the monitoring of dealers' written and verbal exchanges on channels used to conclude trades or communicate with other market participants. These channels typically comprise of voice calls, electronic messaging<sup>7</sup> and emails.
- 10.13 Surveillance of dealers' communications complements trade surveillance, particularly in monitoring for certain types of market misconduct where trading patterns would provide little insight. For example:
- (a) collusion to influence or move a benchmark rate;
  - (b) collusion to temporarily withhold market participation for prospective gain, based on possession of inside knowledge; or
  - (c) disclosure of confidential information on the institution or clients, such as proprietary positions, as well as trades which have been concluded or are pending market execution.
- 10.14 Institutions must have infrastructure to facilitate the conclusion of deals on recorded devices (e.g. company-issued mobile devices or softphones on computers when such dealing takes place from alternate or off-premise sites). Communications on these devices must also be subjected to communication surveillance.



**System**

- The usage of systems or tools is necessary for communications surveillance.
- A single platform that consolidates and processes information from all text-based communication channels has been observed to be the most effective at facilitating the following outcomes:
  - ➔ Setting of trigger keywords to flag out instances (alerts) where the language used may indicate potential attempt at misconduct.
  - ➔ Tracking of timelines as well as documentation and record retention of analyses performed on surveillance alerts assigned to analysts (i.e. case management function), subsequently enabling quality assurance to be performed.
- Usage of disparate platforms to monitor the respective communication channels can be a viable option for institutions with smaller trade volume and less complex products. However, given that such platforms typically lack case management functions, institutions should accord sufficient care to the recording and review of analysts' justifications.
- There should be a means of enabling quick retrieval and playback of voice-based communications. Correspondingly, there should be reasonable efforts to perform surveillance over voice-based communications (e.g. via adequate sampling of voice-based communications or using voice to text technology to perform surveillance over voice-based communications).

<sup>7</sup> Includes messages on external platforms (e.g. Bloomberg, Reuters, etc) and internal company chat platforms.



## Industry Practices



### DOs

- ✓ Business personnel are not privy to the inner workings of surveillance. There is no business influence on the choice of trigger keywords.
- ✓ Keywords used to trigger scrutiny are attuned to the local environment by incorporating non-English languages (e.g. Malay, Mandarin, Cantonese), words, phrases, short forms and colloquial norms.
- ✓ Employing a structured approach in formulating a dictionary of keywords.
  - ➔ Identifying keywords that might be used in perpetrating each type of misconduct, and categorizing them accordingly for easier review.
- ✓ Periodic review (quarterly or annually) to support either maintaining or expanding the existing dictionary of keywords.
- ✓ Process improvements by exploring the use of technologies<sup>8</sup> and past observations from surveillance to reduce the number of false positives.
- ✓ Use of voice to text technology to perform surveillance over all voice-based communications.
- ✓ Reviewing dealers' communications with a particular focus. This is done in addition to reviewing communications with triggered keywords.

#### **Example:**

- ◆ *Reviewing the communications of benchmark rate submitters on a sampling basis to detect any collusion.*



### DON'Ts

- ✗ Solely using off-the-shelf vendor keywords without first assessing whether they are adequate for the institution.
- ✗ Focusing resources on communications surveillance at the expense of trade surveillance. This comes with inherent limitations such as:
  - ◆ Challenges in identifying every permutation of keywords that are indicative of misconduct.
  - ◆ Some types of misconduct do not involve collusion, as they require only a single perpetrator.
  - ◆ Arrangements for collusion or misconduct may be concluded on unrecorded channels.

<sup>8</sup> As an example, Natural Language Processing can potentially be used to provide context-filtering i.e. ignoring instances where the surrounding text for a triggered keyword does not indicate misconduct (e.g. standard footnote to an email, meeting invitation, etc). The industry is also exploring other machine learning capabilities that may facilitate further filtering of surveillance alerts based on past surveillance experience.

## Analysis / Investigation

- 10.15 Personnel responsible for attending to surveillance alerts (i.e. surveillance analysts) should exercise adequate scrutiny when searching for signs of misconduct.
- 10.16 Steps taken and information examined during analysis of alerts should be comprehensive and correspond to the nature of the misconduct. In this regard, a particular alert may require scrutinising both trade data and dealers' communications.
- 10.17 Standard procedures for analysing surveillance alerts should be documented to promote consistency across analysts and preserve the transfer of knowledge and expertise in the context of employee attrition or turnover.
- 10.18 Institutions should maintain sufficiently detailed documentation of analysts' rationales and conclusions pertaining to both closure of surveillance alerts (i.e. alerts considered false positives) and investigation of alerts.
- 10.19 Specific to communications surveillance, the standards for documentation should generally be in line with paragraph 10.18. However, documentation can make reference to communications which, taken in their entirety, are self-explanatory, clearly absent of misconduct and does not trigger further probing.
- 10.20 Surveillance alerts should be closed within a reasonable timeframe, and there should be clear procedures for escalation to senior management once reasonable grounds are established to present a case for misconduct. Institutions should ensure the following:
  - (a) no undue influence by business units to skew or otherwise ignore surveillance findings;
  - (b) confirmation of findings by Risk Management and/or Compliance if surveillance function is being undertaken by a semi-independent party as described in paragraph 10.4;
  - (c) involvement of one or more independent parties in the deliberation of consequence management actions to be taken against employees for misconduct; and
  - (d) reporting of the occurrence of misconduct to the relevant board and senior management committees.
- 10.21 Pertinent questions that might assist analysis for specific types of market misconduct are discussed in section 11 of this document.

## Industry Practices



### DOs

- ✓ A standard checklist or operations manual provides step-by-step guidance to analysts for each surveillance scenario.
- ✓ Surveillance function understands the business nature and individual behaviours of the dealers under surveillance, and applies that knowledge in analysing alerts.
- ✓ Proper record keeping of analysts' justifications and reasoning in closing alerts.
- ✓ Quality assurance (i.e. validation review) by the line manager or an independent party to ensure the adequacy of analysts' justifications and reasoning.



### DON'Ts

- ✗ Automatically dismissing alerts that have commonly been flagged in the past on a particular dealer without exercising reasonable scrutiny each time.

#### **Examples of ineffective approaches observed in analysing alerts for specific surveillance scenarios:**

##### **Front Running**

- ◆ *Mistakenly focusing scrutiny on the deal activity of the sales dealer who originated the large client order, instead of the activity of traders who are actually in the position to trade ahead or front run client orders in the market.*

##### **Position Parking**

- ◆ *Analysis solely relies on searching for indicative keywords like 'park' and 'place' in the communications of the dealer under scrutiny. Subsequently, concluding that no misconduct had occurred simply from the absence of those words.*
- ◆ *Collusive arrangements may have been made outside of monitored communication channels.*

## Personnel and Training

- 10.22 Surveillance analysts must receive adequate training to carry out their function effectively. This includes having working knowledge of common market practices, market conventions as well as market misconduct typologies, to assist in their analysis of alerts.
- 10.23 Former dealers or brokers can be a highly valuable resource within surveillance teams. This is owing to their knowledge of market norms and conventions ('tricks of the trade') and ability to provide a dealer's perspective on how market misconduct might be perpetrated.



## 11. Monitoring for and Investigating Misconduct

- 11.1 This section seeks to provide guidance on some types of misconduct that are commonly within the scope of banking institutions' surveillance of wholesale market activities. The contents of this section are not intended to be exhaustive, and institutions should still conduct their own research and self-assessment on exposure to market misconduct.
- 11.2 Market misconduct can be wide in scope and exist in many forms, but commonly have the following underlying motives, objectives and vectors for perpetration:

Motive / objective	Vector
Influencing market behaviour / benchmark rates	<ul style="list-style-type: none"><li>• Transacted or closing market prices</li><li>• Transacted market volume (circular trades)</li><li>• Market order queue (e.g. exchange-traded products)</li><li>• Benchmark rate submission</li></ul>
Taking advantage of inside information	<ul style="list-style-type: none"><li>• Trading ahead of client orders</li><li>• Acting on material non-public information (e.g. from sell-side activities)</li></ul>
Concealing positions / Hiding losses / Circumventing holding periods	<ul style="list-style-type: none"><li>• Circular trades</li><li>• Off-market trades</li></ul>

- 11.3 While industry terminologies have been established to provide classification to different types of misconduct, the landscape may continue to evolve based on changes in business models, processes and markets in general.
- 11.4 Institutions are encouraged to develop a holistic view in assessing how surveillance and other controls and checks come together to effectively address specific types of misconduct.

## Wash Trading

### Definition

- Buying and selling the same financial product for (usually but not necessarily) the same amount and price, involving one or more counterparties, effectively having no change in beneficial ownership<sup>9</sup>.
- Among the potential motives for this kind of misconduct are to:
  - ➔ Misrepresent market liquidity of a particular stock or product by giving a false impression of high market activity intended to trigger a market reaction.
  - ➔ Manipulate the market closing price of a stock or product.
  - ➔ Defraud client accounts by generating unnecessary transaction fees.
  - ➔ Ramp up the market price of a stock or product, when done at progressively increasing prices.
  - ➔ Generate commissions to reward brokers for favours received or collusion in other areas.



#### Applicable financial products

- In principle, the potential for this kind of misconduct is present in most financial products given the array of possible motives. Nonetheless, those with the following characteristics are considered to be at 'higher risk':
  - ➔ Traded in markets which provide market participants with intraday information on last done prices and executed market volumes. (e.g. products listed on an exchange).
  - ➔ Executed market volume within a narrow time frame is used in the calculation of market benchmarks.
  - ➔ Has a market price that is used for valuation purposes.



#### Factors to consider when setting up surveillance

- Wash trades are typically perpetrated by dealers whose role or actions can have a market impact.
- Surveillance parameters should be able to identify clusters of potential wash trades including where there is slight variation to the executed prices and aggregated trade amount (i.e. does not offset perfectly).
- Wash trades do not always occur in pairs.

#### Examples of variations:

- ◆ A single transaction that is followed by two or more smaller offsetting transactions. (e.g. buy 20 lots followed by sell 10, 5, 5 lots).
- ◆ A number of smaller transactions in one direction (buy/sell) followed by one or more larger offsetting transaction. (e.g. buy 5, 2, 5 lots followed by sell 6, 6 lots).

- The appropriate interval of time (or lookback period) used to identify potential wash trades should be based on factors such as the underlying motive (e.g. compensation trades may have a longer interval) and market liquidity of the product.
- Filtering out irrelevant trade records, particularly typical transfers from the sales desk to the trading desk may help provide focus to surveillance.
- One observed approach to parameter setting is to aggregate relevant trades within a specified time interval before and after each trade, and flag out instances where the aggregated trade amount within that time period is almost completely offsetting (i.e. nets close to zero).

<sup>9</sup> Definition referenced from Behavioural Cluster Analysis – Misconduct Patterns in Financial Markets (2018). FICC Markets Standards Board.

## Analysing Potential Cases

Trade patterns resembling wash trades may occur for reasons ranging from system-generated internal deals to genuine trading decisions. In establishing whether misconduct has actually occurred, analysis should focus on questions and indicators which support the motives behind wash trades.



### Price manipulation

- Was the wash pattern within a very short time frame?
  - ➔ This may warrant scrutiny on whether the motive was to influence the intraday market price, particularly if there were multiple repetitions and/or at increasing prices. Judgment should be exercised as the time frame may be longer for less liquid securities.
- Did the wash pattern occur near the time of market close?
  - ➔ This may indicate intent to manipulate the closing price for more favourable mark-to-market valuations.
- Was there any avenue for the dealer under scrutiny to benefit from price manipulation?
  - ➔ Having positions on book prior to the observed pattern of wash trades would establish a motive for manipulation that should be investigated further.
- The degree of scrutiny for price manipulation should be greater for wash patterns in products where market participants have access to intraday information on last done prices and executed market volumes (vectors for manipulation).



### Market / trade volume

- Does the dealer or institution's traded volume constitute a sizeable portion of the overall market volume for the day?
  - ➔ This would point towards an attempt to misrepresent market interest or the liquidity of a product, which is ultimately intended to have influence on market prices.
- Deviations in the volume of trades compared to past norms or what is typical in the dealer's trading behaviour deserve increased scrutiny.






### Market liquidity

- Market abuse may be easier to achieve for illiquid securities, but the scope of potential gain from capitalizing on market reaction is more limited. Consideration of other possible motives such as seeking a more favourable book valuation can be explored for wash patterns involving illiquid securities.



### Number of counterparties

- While a cluster of wash pattern trades with the same counterparty is a clearer indicator of potential misconduct, in instances where there are different counterparties, the same level of scrutiny should be placed if those counterparty names recur repeatedly.

 <p><b>Operational aspects</b></p>	<ul style="list-style-type: none"> <li>Does the product being scrutinised for wash trades have any unique settlement norms?             <ul style="list-style-type: none"> <li>➔ Wash trades with the intention of manipulating market prices or volumes may be less feasible for products settled on gross basis (instead of net) owing to some cost involved for the required scale. However, institutions should still assess whether these costs are insignificant relative to the potential gain before making conclusions</li> </ul> </li> </ul>
 <p><b>Compensation trades</b></p>	<ul style="list-style-type: none"> <li>Wash pattern trades executed through the same broker may indicate an intent to generate commissions for the broker without clear benefit and at the expense of the institution.</li> <li>Compensation can also be passed on through slightly different price or size between trades.</li> <li>Reconciliation against brokerage statements may help assist in analysis here.</li> </ul>
 <p><b>Dummy / client accounts</b></p>	<ul style="list-style-type: none"> <li>Scrutiny should be placed on wash patterns between internal dummy accounts.</li> <li>Client accounts can potentially be used by dealers or brokers to do wash trades (e.g. stockbroking client accounts).</li> </ul>



## Position Parking

### Definition

- Position parking occurs when two or more market participants agree to conclude a deal that will be reversed on a future date with a view towards concealing dealing positions or transferring profits and losses.
- Among the potential motives for this kind of misconduct are to:
  - ➔ Circumvent penalties or forced selling associated with the institution's aged inventory policy on securities. (e.g. trading book holding period).
  - ➔ Conceal or postpone recognition of losses, allowing time for markets to potentially recover and reduce or reverse the initial loss amount.
  - ➔ Conceal risk positions, possibly to temporarily take on additional risk without triggering internal risk limits.
  - ➔ Avoid capital charge requirements.
  - ➔ Conceal landed positions from securities underwriting.



#### Applicable financial products

- In principle, the potential for this kind of misconduct is present in financial products which have a specific stock code. (e.g. bonds, equities).



#### Factors to consider when setting up surveillance

- Surveillance for position parking should be on dealers who carry out the role of taking on or warehousing risk for the institution.
- The modus operandi for position parking is similar to wash trading, albeit with a longer time interval potentially stretching up to a few weeks between the initial sale and subsequent buyback.
- Position parking can happen at any time and is not necessarily limited to the period around month end or at the cut-off between financial reporting periods. This is in view of the following:
  - ➔ Dealers' profit and risk positions are tracked daily.
  - ➔ Compliance with aged inventory policies on securities is typically tracked based on time lapsed from the date of initial acquisition.
- Position parking can be executed in a circular flow involving different counterparties.
- Surveillance parameters should flag out potential position parking in paired trades of matching size, although executed prices may differ slightly.
- The motives behind position parking are more pronounced for less liquid securities.
- Separate scrutiny or review of the institution's transaction history in less liquid securities may help identify instances where position parking is performed through multiple trades rather than a single pair of trades.

## Analysing Potential Cases

Pairs of trades of matching size and price are unusual but may well be the result of genuine trading decisions. In establishing whether misconduct has actually occurred, analysis should focus on questions and indicators which support the motives behind position parking.



### Circumvent inventory / holding period policies

- At the point of initial sale (i.e. first leg of position parking), were the securities nearing the end of the holding period specified in the institution's trading book policy?
  - ➔ This would strongly indicate a motive for using position parking to circumvent the holding period policy.



### Concealing positions

- Does the timing of the trades coincide with significant valuation markers? (e.g. month-end, cut-off for performance measurement, etc).
  - ➔ There may be a motive to temporarily conceal positions to improve performance measurement.
- Would any risk or stop-loss limits have been breached if the amount of securities initially sold are retrospectively included in the calculation of risk exposure?
  - ➔ If so, position parking may have been used to conceal positions and prevent breach of risk limits.
- Were any of the trades concluded at off-market rates?
  - ➔ This may indicate an attempt to conceal losses (e.g. transacting at a price more favourable than the market price in the first leg, followed by the same or slightly better price in the second leg).



### Market liquidity

- Scrutiny for position parking should be greater for less liquid products as there may be difficulty in finding willing buyers at a favourable price, and larger spread or cost is incurred from the act of selling and repurchasing in the market.



### Number of counterparties

- Patterns of position parking involving the same counterparty are a clearer indicator of potential misconduct.
- However, trades that involve different counterparties should still be examined to address the possibility of a circular flow involving more than one counterparty.

# Front Running

## Definition

- Taking a position in a financial product ahead of executing a large client order, and subsequently profiting by closing out the position once market prices have moved. The client may also potentially be disadvantaged by receiving a less favourable price as a result<sup>10</sup>.
- Front running can be perpetrated by individuals who are either transacting for the institution or dealing for a personal account, depending on market access.
- Collusion with other market participants to withhold bids or offers on the expectation of large incoming client flows during the day is also treated as a form of front running.



### Applicable financial products

- In principle, the potential for this kind of misconduct is present in financial products where the institution is in the business of accepting and executing client orders.
- For FX in particular, the spot leg of FX forwards transacted with clients may also be the target of front running. Institutions should consider including this perspective in the scope of surveillance.



### Factors to consider when setting up surveillance

- Front running is made possible or more lucrative by large client orders that are able to move market prices.
- Opportunities for front running are higher under the following business operating norms:
  - ➔ Sales dealers practise taking client orders where the price is not agreed upfront and left to market forces (e.g. fixing order, limit order, etc), and details of these yet to be filled orders are visible to traders for the purpose of planning and risk management.
  - ➔ Sales dealers regularly seek market quotes from traders when handling large client orders and the details on potential transaction size is communicated to traders.
- Surveillance parameters should flag out instances of large client deals (i.e. sales deals). Analysis should focus on the activity of trading desk dealers (i.e. traders) in the time window between the receipt or communication of the large client order and conclusion or recording of the deal.
- Setting an appropriate surveillance threshold that defines a 'large' order may incorporate the following steps:
  - (1) Estimating the potential market impact for a range of trade sizes.
  - (2) Examining the typical position-taking sizes for the trading desk.
  - (3) Using (1) and (2) to reason out a threshold where the amount of financial gain from front running makes the misconduct worthwhile.
- Collusion with other market participants to withhold market participation should be monitored via communications surveillance.
- Institutions may consider having separate books, still managed collectively, that capture exposures derived from client flows and proprietary trading respectively. This would serve the purpose of providing clearer records to facilitate surveillance analysis.

<sup>10</sup> Definition referenced from Behavioural Cluster Analysis – Misconduct Patterns in Financial Markets (2018). FICC Markets Standards Board.

## Analysing Potential Cases

Scrutiny should be placed on the activity of traders, not sales dealers who do not have market access and do not warehouse risk. Establishing whether front running has occurred can be challenging from a record-keeping perspective, as analysts may have difficulty distinguishing between proprietary trades and trades intended to hedge or de-risk exposures from client deals. In establishing whether misconduct has actually occurred, analysis should focus on questions and indicators which support the motives behind front running.



### Market price movement

- Was there a movement in market price after concluding or recording the client deal? (i.e. market price rose for a client buy, or declined for a client sell)
  - ➔ The case for front running might be supported if traders had undertaken proprietary trades that benefitted from the market movement.
  - ➔ In the case market movement was absent, or movement was in the opposite direction, this may indicate either absence of misconduct or a failed attempt. Other indicators need to be examined.



### Nature of trades within specified time window

- Between the time the large client order was received up to the point of deal conclusion, were there any proprietary trades in the same direction as the large client order?
  - ➔ Positions from such trades would likely result in financial gain when the client order enters the market, and is consistent with the motive for front running.
- Shortly after the client deal was concluded or recorded, was a proprietary trade executed in opposite direction but of similar size to another proprietary trade executed earlier?
  - ➔ May be an act of closing the earlier front running position.
- If there are issues with identifying proprietary trades, some insight may be gained by netting exposures from all the trader or desk deals executed during the window. This to determine whether a sizeable net exposure was maintained which subsequently benefitted from market movement.



### Counterparties of interest

- Brokered deals and direct deals with other market participants should be the focus of analysis.

## Off Market Rates

### Definition

- Off market rates refer to trades that are concluded at prices or rates that are away from where the market is trading at the time of execution. It can be a symptom of misconduct, as opposed to being a type of misconduct on its own.
- Among the potential motives for transacting at off market rates are to:
  - ➔ Conceal trading losses by transacting at above market price, or postpone gains by transacting at below market price (e.g. position parking arrangement may be used).
  - ➔ Pass an immediately profitable trade to a counterparty in return for favours received but at the expense of the institution.



#### Applicable financial products

- In principle, off market rates can be perpetrated for all financial products, including money market deposits.
- For clarity, off market rates do not refer to off market transactions in the context of equity instruments, where the exchange of shares does not involve the stock exchange.



#### Factors to consider when setting up surveillance

- Surveillance for off market rates typically involves selecting a reference price that is reflective of the market, setting a range around that reference price, and then scrutinising each trade which falls outside that range.
- Ideally, the reference price used should correspond to the exact time that trade was executed.
  - ➔ In the absence of data on intraday price points, institutions can consider alternatives such as daily market High-Lows, closing price, and other sources where valuations are derived.
- Attention should be paid to products that may not have an updated or available daily or intraday reference price (e.g. illiquid or OTC). Such products should be identified and assigned a proxy reference price where feasible.
- The surveillance threshold or range for deviations from the reference price should be reasonable and differentiated according to the market norms and characteristics of different products.

#### **Example:**

- ◆ *Applying a 2% threshold for products across asset classes or currencies is unlikely to be effective. If applied to the USD/MYR pair (Exchange rate: 4.00), a 2% threshold would translate to 800 pips, which is extremely far from usual market bid-ask spreads and typical daily market movement.*

- The approach to setting surveillance thresholds should differ according to the reference price used (e.g. daily closing price, intraday prices).
  - ➔ If closing prices are used as reference, an analysis of daily movements in closing prices helps determine an appropriate threshold.
  - ➔ If intraday prices are used as reference, a threshold based on historical bid-ask spreads around the mid-rate plus some allowance may be considered.



- Setting a high threshold that is intended to account for or prevent false positives from client deals is generally ineffective at identifying off market rates in the interbank trading markets.
  - ➔ Due to sales spreads, client prices are typically much higher compared to prices that would be considered off market in interbank trading markets.
- Surveillance thresholds for client deals may be differentiated from those applied to traders' trades, and focus on compliance with the institution's client spread or pricing policy.

## Analysing Potential Cases

In scrutinising off-market rates, common practice is to request for an explanation from the dealer responsible. This is acceptable and unavoidable as dealers are closer to market developments and the reasons given may be genuine. However, steps should be taken to validate or independently confirm the reasons given by dealers where possible, and analysts' documentation of conclusions should provide sufficient clarity where dealers' explanations do not.

As off-market rates are just a symptom of potential misconduct, institutions should consider potential motives. Forming linkages with other types of misconduct may be helpful. Communications surveillance may be helpful in uncovering misconduct should dealers give reasons which prove to be implausible.



# Insider Dealing

## Definition

- Taking part in or carrying out a transaction based on non-public information that would, or would tend to, have a material effect on the price or value of financial instruments.
- Insider dealing can be perpetrated by individuals who are either transacting for the institution or dealing for a personal account, depending on market access.
- The motive of such misconduct is to profit by buying a security when in possession of positive news, or avoid losses by selling the security or profit by short-selling when in possession of unfavourable news, prior to the information becoming public.
- Inside information typically originates from business units involved in capital market activities or corporate banking (business team servicing a client that the information concerns). Additionally, other persons that are brought over information barriers to provide inputs like market insights (e.g. dealers) may also have access to inside information.



### Applicable financial products

- In principle, insider dealing can be perpetrated for all financial products where the market price is linked to the performance and actions of a specific company (e.g. equity, bonds, derivatives).



### Factors to consider when setting up surveillance

- Apart from surveillance, preventive controls such as Chinese Wall policies (discussed in section 12 of this document) play a crucial role.
- In the context of institutions' own trading, surveillance for insider dealing revolves around identifying instances where dealers were in possession of inside information and examining whether said information was acted upon.
  - ➔ Identifying wall-crossed employees and companies that were the subject of wall-crossing.
  - ➔ Scrutinising the trading activities of wall-crossed employees that involve securities of the companies in concern.
  - ➔ Surveillance should cover the period from the date of wall-crossing up to the time when the information shared ceases to be inside information.
- In general, abnormal profits coming from trading in securities issued by companies should be scrutinised when not attributed to broad market movements.
- For equities in particular, licensed investment banks typically have parameters to flag out accounts which undertake significant and out of the norm trades just prior to a market announcement.
- Mechanisms to prevent and detect insider dealing in an individual capacity are discussed in section 12 on Personal Account Dealing.

## Analysing Potential Cases

Establishing whether insider dealing has occurred requires time and diligence. Once there are reasonable grounds for suspicion, an explanation from the dealer should be sought. In establishing whether misconduct has actually occurred, analysis should focus on questions and indicators which support the motives behind insider dealing.



### Market price movement

- Was there movement in the market price of the securities?
  - ➔ Firstly, there does not need to be an immediate observable benefit to establish the occurrence of insider dealing. While the element of benefit would help support the case for misconduct, any action taken based on inside information is considered insider dealing.
  - ➔ If positions in the security are taken just prior to a market announcement, and subsequently disposed of at a profit shortly after the announcement, this would be strong grounds to suspect insider dealing.



### Past trading behaviour

- Are the trades under scrutiny typical of the dealer's past trading profile or strategies?
  - ➔ Further questions should be asked if the trades being scrutinised deviate in size (i.e. larger volumes traded compared to historical average volumes) and frequency from the dealer's past trading behaviours.



The background is a dark blue abstract composition. It features a faint world map, a line graph with multiple colored lines (yellow, red, orange), and a bar chart at the bottom. A semi-transparent blue rectangle is positioned on the right side, containing the title text.

# INTERNAL CONTROLS AND CULTURE

## Part C: Internal Controls and Culture

### 12. Control Environment in Managing Conduct Risks

- 12.1 Pre-emptive and structural measures such as detective and preventive controls and institutional culture to address conduct complement the surveillance programme in mitigating exposure to conduct risks. These measures typically seek to address business and operational practices that may increase susceptibility to market misconduct.
- 12.2 A strong internal control environment, in the context of wholesale market conduct, should exhibit the following characteristics:
- (a) clear governance structure which facilitates the reporting and escalation of conduct-related matters, which include breaches of conduct and those outlined in paragraph 12.8;
  - (b) emplaced policies and procedures that can help deter misconduct, as well as reviews to provide assurance that those measures are working effectively; and
  - (c) additional detective tools to complement trade and communications surveillance, which can take the form of back office reconciliations, review of brokerage charges, etc.
- 12.3 The internal control environment involves the three lines of defence, with roles played by the business unit, Risk Management, Compliance, and Internal Audit respectively.
- 12.4 This section seeks to provide guidance on areas which fall within the scope of the guidance outlined in paragraphs 12.1 and 12.2.

### Q&A Segment



**I believe my institution has sufficient policies, processes and checks to prevent misconduct in general. Does that lessen the importance of trade and communications surveillance?**



A strong control environment does not eliminate or reduce the need for surveillance.



**How does the control environment link to surveillance?**



- i. To provide assurance that processes and controls are working effectively, institutions should have surveillance in place over established forms of market misconduct.
- ii. Based on this assessment, institutions may decide on the scope and intensity of surveillance performed for that type of misconduct. Institutions may also decide to strengthen processes and controls.
- iii. Institutions should assess how existing business processes and controls affect their susceptibility to the various types of misconduct.



## Governance and Reporting

- 12.5 Breaches of conduct can have a serious impact from financial, reputational and regulatory perspectives. The board and senior management are responsible to keep themselves regularly apprised of their institution's conduct risks, and accord sufficient attention to the management of those risks.
- 12.6 Each institution must have designated persons and/or committees responsible for overseeing its conduct in wholesale markets.
- 12.7 Institutions must provide a holistic view of conduct risk via the reporting of key indicators and updates to their relevant board and management committees<sup>11</sup>, to a degree that is commensurate with the institution's business transactions profile, significance of income contribution, as well as level of market participation and influence.
- 12.8 Areas that should be covered in the reporting include but are not limited to the following:

Areas	Examples
Outcomes of trade and communications surveillance	<ul style="list-style-type: none"><li>Numbers and trends in surveillance alerts by scenario type, as well as reasons generally contributing to those numbers (e.g. trading strategies, internal record-keeping, etc).</li><li>Analysis summary of surveillance alerts which warranted deeper review of the underlying trades or communication.</li><li>Results of quality assurance performed on the work of the surveillance team.</li></ul>
Indicators commonly associated with conduct	<ul style="list-style-type: none"><li>Numbers and trends in trade cancellations and amendments, supplemented with root causes.</li><li>Incidences of trading at off-market rates and whether these were justified reasonably.</li><li>Number of after-hours or off-premise trades, and reasons given to justify such instances.</li></ul>
Others	<ul style="list-style-type: none"><li>Dealers' compliance with mandatory or block leave requirements.</li><li>Instances of wall-crossing for the period under review,</li><li>Outcome of review on personal or proprietary dealing activity of wall-crossed employees.</li></ul>

- 12.9 The reporting in paragraph 12.7 must be on a periodic basis (at least quarterly) to provide assurance on the effectiveness of existing measures to manage conduct risk and enable decision-making.
- 12.10 Practices in the industry generally show fragmented reporting by the respective functions that dilute the importance and effectiveness of the controls performed. A single and consolidated reporting of outcomes from the various controls in place is recommended to provide senior management and the board with a holistic view of the institution's management of conduct risks.

<sup>11</sup> Management committees refer to senior management committees, with representation by senior leaders within the institution, particularly from the Risk and Compliance functions.

## Industry Practices



### DOs

- ☒ Establishment of a working level management committee to specifically oversee matters concerning dealers' conduct. This offers a consolidated view of how conduct-related controls come together:
  - ➔ The committee has representatives from all functions that are involved in administering controls related to dealers' conduct (e.g. treasury front-back office, Risk Management, Compliance, etc), and typically chaired by persons like the Chief Risk Officer or Chief Compliance Officer.
- ☒ Frequency and depth of reporting to the board and senior management are proportionate with the level of risk as identified in the institution's market conduct risk assessment (detailed in section 9).

### DON'Ts

- ☒ Business and/or control processes result in fragmented reporting on the outcome of conduct monitoring and controls.

#### Example:

- ◆ Risk Management would report the outcomes of monitoring under its jurisdiction to the Risk Management Committee, while Compliance reports to the board via its monthly compliance packs.

- ☒ Practices in escalating and reporting information does not foster holistic oversight of conduct risk in the institution's leadership.

#### Examples:

- ◆ Reporting to senior management committees like the Operational Risk Management Committee, as well as board committees, only highlights significant issues or indicators and lacks important insights from surveillance activities.
- ◆ Conduct indicators and outcomes of surveillance are largely absent from reporting as they may be viewed as insufficiently material for escalation when viewed on a standalone basis, often only escalated up to the heads of the respective control functions.
- ◆ Centralised global or regional surveillance functions do not sufficiently produce or escalate country-level surveillance indicators to the Malaysian entity leadership for oversight and decision making.
- ◆ Perspectives given in reporting are quite process-driven, losing context of the importance of those monitoring processes over time.



## Q&A Segment



**What are some indications relevant to reflect the business transactions profile, significance of income contribution, and level of market participation and influence mentioned in paragraph 12.7?**



- i. Business transactions profile: trade volume and number of transactions, client flows, and frequency of large single client deals.
- ii. Income contribution: percentage of the institution's income attributed to wholesale market activities; and contribution to treasury income from the trading desk relative to the sales desk.
- iii. Market participation and influence: trade volume relative to the industry; and capability to move markets that is enabled through large risk limits or management of intraday client flows.



**What are examples of institutions that are expected to have minimal focus on wholesale market conduct risk reporting?**



Institutions which have minimal participation in markets. An example would be an institution that has money market placements as the primary treasury activity, with almost negligible client flows and no proprietary trading in bonds, FX and equities.

## Front-Middle-Back Office Controls

- 12.11 In the context of trading in financial markets, institutions typically have a number of controls across their front, middle and back offices which contribute to deterring or detecting misconduct.
- 12.12 This segment will discuss common controls observed in the industry (not exhaustive). Institutions are encouraged to think about and consider other controls as appropriate to their operations.
- 12.13 To address unauthorised trading, institutions are expected to establish critical controls in treasury operations, particularly in the effective implementation of segregation of duties between the risk-taking activities, risk management and control functions, as well as the trade capture and confirmation functions.
- 12.14 Each institution must have a well-documented policy governing all trading activities. The policy must include, among others, the appointment of dealers, authorisation process, risk limits, conduct of dealers and rate-setting activities. More importantly, the policy must define the nature of trading practices deemed as unauthorised trading or manipulation of market volumes, process and benchmark rates.
- 12.15 Valuation of positions based on market prices and internal models must be performed independently of the front office (risk-taking function). Where this process involves obtaining inputs from the front office, continuous efforts should be taken to validate their accuracy.
- 12.16 The middle office function (Risk Management) must periodically inspect trading book and banking book positions to identify deviations from approved strategies, trading book policy or trading norms. Any deviations must be investigated immediately and escalated to senior management.

- 12.17 Institutions must establish specific key risk indicators for treasury activities and appropriate risk tools to promptly alert and identify potential control failures. The monitoring of risk limits must be conducted on a daily basis and any breaches should be immediately escalated to senior management, outlining the root causes and actions taken to address such breaches.
- 12.18 The back office function should be responsible for the reconciliation of trades against the profit and loss (P&L) account as well as valuation of collateral linked to the institution's trades. A granular P&L attribution analysis should be conducted to determine the nature of individual dealers' P&L, with follow up on sudden swings or irregularities.
- 12.19 In approving new products, institutions must document their assessment of all risks associated with the offering or trading of new products, including updates to the institution's market conduct risk assessment.
- 12.20 Each institution must update its Authorised Dealers List on a timely basis and such updated list should be notified to dealing counterparties and relevant parties within the institution.

#### **i. Entertainment and Gifts**

- 12.21 Entertainment and gifts (E&G) associated with clients and counterparties should be subject to internal policies and guidelines.
- 12.22 Institutions should be vigilant of frequent or unwarranted amounts of E&G that are received or given by their employees, as these could be used to secure cooperation for potential misconduct or affect impartiality in decision-making.
- 12.23 Controls over E&G activity must give consideration to the following:
  - (a) policy which specifies the forms and circumstances under which E&G can be given or received, including thresholds on monetary value;
  - (b) procedures for dealers to declare E&G that are given or received in a central register; and
  - (c) periodic review of the records under (a) and (b) to detect signs of irregularity.

## Industry Practices



### DOs

- ✓ Maintenance and review of the E&G register is centralised across business units, facilitated by a system, and under the purview of an independent function.
- ✓ For activities involving dealing in financial markets, review of E&G records is done with the following perspectives:
  - ➔ Reconciliation against concentration of trades with a particular counterparty or broker.
  - ➔ Significant increase or decrease in E&G disclosures for the period compared to the previous similar period.
  - ➔ Lack of E&G disclosures (i.e. non-reporting).
  - ➔ Reasonableness of declared monetary value and justifiability of individual items.
- ✓ E&G policies are designed to provide greater oversight with increasing levels of activity (e.g. dual approval by business head and independent functions (Risk Management or Compliance) for E&G above a certain amount and/or number of occurrence).
- ✓ Annual review of E&G policy, particularly to re-evaluate specified monetary value thresholds.
- ✓ For banking groups with multiple entities or branches, overall oversight on E&G is performed by a group governance committee to ensure consistency in implementation and monitoring.



### DON'Ts

- ✗ Stopping at obtaining declarations of E&G, with no further actions taken to scrutinise those records.
- ✗ Having insufficient details recorded on the nature of E&G received or given, which would otherwise assist in the review of those records.
- ✗ Setting a high threshold on the monetary value of E&G for which a declaration is required to be made.

## ii. Broker / Counterparty Relationships

- 12.24 Institutions must be cognizant of potential conflict situations arising from broker relationships, particularly if this affects their dealers' decision-making and results in less optimal outcomes for the institution. Possible scenarios include:
- (a) dealers favouring a particular broker to reciprocate receiving E&G or even kickbacks, despite better fees and research offered by another broker; or
  - (b) wash trades undertaken by dealers with the motive of generating brokerage fees as a favour.
- 12.25 Many institutions perform periodic reviews to examine concentration and trends in brokerage fees as well as E&G provided by brokers with regard to the institution's dealers.
- 12.26 Similarly, institutions should be vigilant of counterparty concentrations as these may be potential indications of collusion.



- 12.27 Institutions may also consider reconciling the analysis performed during their review against the E&G register to help explain any irregularities or shifts in dealers' trading patterns or behaviour that favour a particular broker or counterparty.

## Industry Practices



### DOs

- ✓ Broker used is recorded in front end systems at a transactional level, which facilitates identification of concentration to a particular broker as well as wash trades intended to generate brokerage fees.



### DON'Ts

- ✗ High-level examination of trends in brokerage fees paid by the institution, typically on aggregate amounts. This is unlikely to detect instances of misconduct that do not cause significant change to the total brokerage fees paid.
  - ➔ Itemised statements furnished by brokers can be used to facilitate more in-depth review.

## iii. Mandatory Leave

- 12.28 Enforcing a continuous period of leave on employees is a means to detect potential misconduct, which may surface in their absence. In the context of financial market activities, this can uncover unauthorised trading by dealers, particularly attempts to conceal positions.
- 12.29 Institutions should have a policy that specifies the length of mandatory leave that applies to different job functions and this should be commensurate with the size and complexity of the institution. A mandatory leave of 5-10 business days for dealers is widely practised.
- 12.30 During this period, dealers must be barred from dealing and having access to the institution's premises and systems. Work-related communications with and by these dealers must cease apart from under exceptional circumstances, which should be documented and subjected to appropriate governance.

## Industry Practices



### DOs

- ✓ Monitoring on dealers' compliance with the mandatory leave policy is performed by both the business unit and Compliance.
- ✓ Monitoring of the dealer's trades for suspicious and/or unauthorised activity while on Mandatory Leave.



### DON'Ts

- ✗ Physical access to the dealing room and access to dealing systems are not blocked for dealers during their mandatory leave. In lieu of blocking, there are also no subsequent checks for any booking of trades under the respective dealers' ID or trading book during the period.

#### iv. Off-Premise and After-Hours Dealing

- 12.31 Trades concluded outside of the dealing room or after normal working hours can give rise to heightened risks in the following forms:
- (a) inability to resolve dispute over trade details when deals are concluded on unrecorded channels (e.g. personal phones);
  - (b) complication in identifying potential breach of risk limits due to delayed capture of new exposures in the institution's front end systems. This can be exacerbated by genuine oversight or purposeful intent by dealers; or
  - (c) greater flexibility for dealers to collude while outside of the dealing room without prompting query in usual surroundings.
- 12.32 Institutions must put in place internal policies for authorised persons to deal after-hours or engage in off-premise dealings, which should cover prompt recording and reporting of dealings for timely risk capture and trade settlement.
- 12.33 Such trades should be treated as exceptions rather than the norm, tracked for frequency, and scrutinised for purpose.

#### Industry Practices

##### DOs



- ☒ Policy restricts off-premise or after-hours dealing to a few authorised persons, and in some cases the purpose of such deals is confined to the intent of lowering risk exposure.
- ☒ Enquiry is made into the purpose and nature of such deals, and supplemented by processes to detect and manage instances when such deals might go unrecorded in the institution's systems.
- ☒ Off-premise and after-hours deals are tracked in a register and scrutinised for unusual patterns and frequency.
- ☒ Utilizing technology to facilitate oversight by supervisors (e.g. desk heads) on off-premise or after-hours dealing, for example via system prompts or alerts.
- ☒ Incorporating exposures from off-premise or after-hours deals in the previous day's risk measurement to determine if any risk limits would otherwise have been breached.

##### DON'Ts



- ☒ Overly lax policy criteria for off-premise and after-hours dealing.
- ☒ Addressing off-premise and after-hours deals from the solely operational standpoint of ensuring timely settlement, without further scrutiny on any unusual behaviours.



### Dealing under work from home / BCP arrangements

- In light of Covid-19, institutions have allowed some dealers to work from home or implemented split operations between dealing room and Business Continuity Planning (BCP) sites.
- Institutions should ensure that dealing from home or alternate sites is supported by infrastructure that enable the following:
  - ➔ Timely input of deals into front end systems. Solutions such as Virtual Private Network (VPN) capabilities enable access to systems available at a dealing room workstation.
  - ➔ Record retention of dealers' work-related communications. This includes communications with clients and other market participants via company-issued phones or alternate communication platforms (e.g. softphones on computers).
- To the extent that deals concluded from home are supported by the above infrastructure, institutions should determine whether the heightened risks associated with off-premise trades are sufficiently mitigated.
- Institutions should avoid from allowing dealing to be conducted on personal phones. As a temporary measure, the practice of requiring subsequent confirmation in writing from the client or counterparty (e.g. via email) in such instances is inadequate to facilitate monitoring of dealers' conduct, as the context of dealers' conversations cannot be captured.
- The risk of market misconduct is arguably greater as being away from the dealing room allows dealers to engage in collusive conversations (via personal phone calls or messages) without triggering scrutiny from their surroundings.
- Institutions should revisit their market conduct risk assessment and operational risk assessment frameworks (e.g. RCSA to reflect the changes in risk under these operating arrangements).
- Additional controls, reviews and oversight should be accorded over flexible working arrangements to detect irregularities in the trading activity or communications of dealers. These include, but not limited to:
  - ➔ Enhancement to dealing room and conduct policies to provide greater guidance on execution of deals which uphold principles of good conduct when dealing in the financial markets.
  - ➔ Establishment of work from home daily report checklists for front, middle and back-office staff to report operational incidences and share challenges, especially in cases where there are significant changes to processes.
  - ➔ Reporting of key statistics to supervisors and management that can prompt improvement to processes to increase security, efficiency or to reduce risk levels (e.g. number of deals concluded as part of flexible working arrangement, details on minor and major operational incidences such as network disruptions and system downtimes).
  - ➔ Increased communication and engagement with staff to instil organisational values.
  - ➔ Trainings on lessons learnt from misconduct cases and highlight consequences to deter staff from misconduct.
  - ➔ Encourage 'over-reporting' of incidences or 'speak up' culture.
- Where institutions continue to implement flexible working arrangements on a permanent basis, institutions should also ensure their BCP plans are expanded to include disruptions when dealers are working from home/working remotely.

## **v. Business Norms**

- 12.34 Business norms refer to practices that exist outside of formal controls that are typical in the course of day-to-day business dealings, which can have an effect on the propensity for certain types of misconduct to occur.
- 12.35 For example, opportunities for front running may increase depending on how the institution handles client orders. Institutions should consider how their current business norms might have an effect on conduct risk.



### **Client order handling and front running**

- Front running is predicated on the availability of advance knowledge of a client seeking to buy or sell large amounts in the market. Traders may have access to such information through the following ways:
  - ➔ Practice by sales dealers to seek quotes from traders when handling clients looking to transact significant amounts. Regardless of whether the counterparty ultimately transacts with another institution, the trader is now aware of a trade that may potentially move the market.
  - ➔ The details of yet to be filled client orders placed with the institution are visible to traders for the purpose of planning and risk management. Here the practice of pre-hedging is argued to deliver better outcomes for clients, but depending on the type of client order, also presents an avenue for front running. This includes undertaking trades to trigger conditions specified by the client for the order to be filled.
- Institutions may consider measures to minimise the flow of information to traders on client orders that can be used to front run, and have surveillance in place to tackle residual risks.

## **vi. Trade Capture, Cancellations and Amendments**

- 12.36 Dealers should ideally be required to input or book their trades into front end systems as soon as each deal is concluded. In practice however, some institutions have been observed to tolerate some amount of delay where active traders are concerned, which can potentially derail surveillance efforts that are reliant on accurate time stamping to detect misconduct (e.g. wash trades, front running).
- 12.37 For the purpose of surveillance, where timely trade capture becomes an issue, institutions should consider maintaining a separate field that captures the time each deal is concluded instead of continuing to rely on the time of system booking.
- 12.38 On trade cancellations and amendments, frequent occurrences that are attributed to a particular dealer may signal an attempt at rogue trading.
- 12.39 Trade cancellations and amendments should be recorded in a central register and sufficient details should be documented on the reason for occurrence. The number and nature of cancellations and amendments should be analysed for trends that warrant further scrutiny.

## Industry Practices



### DOs

- ✓ Policies that require dealers to input deals into front end systems within a specified short time frame (e.g. 5-10 minutes to enable more accurate surveillance).
- ✓ Identifying irregularities and concentrations (e.g. to a particular dealer, product or reason) in the trend of cancellations and amendments.
- ✓ Validation of reasons given for cancellations and amendments where warranted.
- ✓ Utilizing technology to facilitate real-time supervision and efficient review.
  - ➔ Underlying reasons (e.g. client-driven, product-driven) are used to generate risk scores that prompt desk heads or supervisors on risky behaviours (e.g. high frequency, no replacement of cancelled deal).



### DON'Ts

- ✗ Tracking cancellations and amendments for operational risk or regulatory reporting without understanding why it is a concern. This results in superficial analysis that would fail to detect misconduct.

## vii. Access to Dealing Room and Systems

- 12.40 Physical access to the dealing room must be limited to authorised persons. Dealers should not have access to the back office.
- 12.41 Access to systems should be functionally segregated. Dealers must not have administrative user rights to make changes to any combination of front, middle and back office systems.
- 12.42 Physical and system access logs should be retrievable for the purpose of audit trail. The list of authorised persons or users should be immediately updated to reflect any changes in personnel.
- 12.43 Dealers should not be given discretion to create new books, folders or accounts in the front-end system for the purpose of booking trades. Any such requests should be notified to Compliance, Risk Management and back office.

## Industry Practices



### DOs

- ✓ Physical and system accesses are blocked during dealer's mandatory leave; or.
- ✓ Use of technology to enable real-time notification to supervisors on behaviours such as dealers accessing front end systems while on mandatory block leave or booking trades that are not part of their mandate.



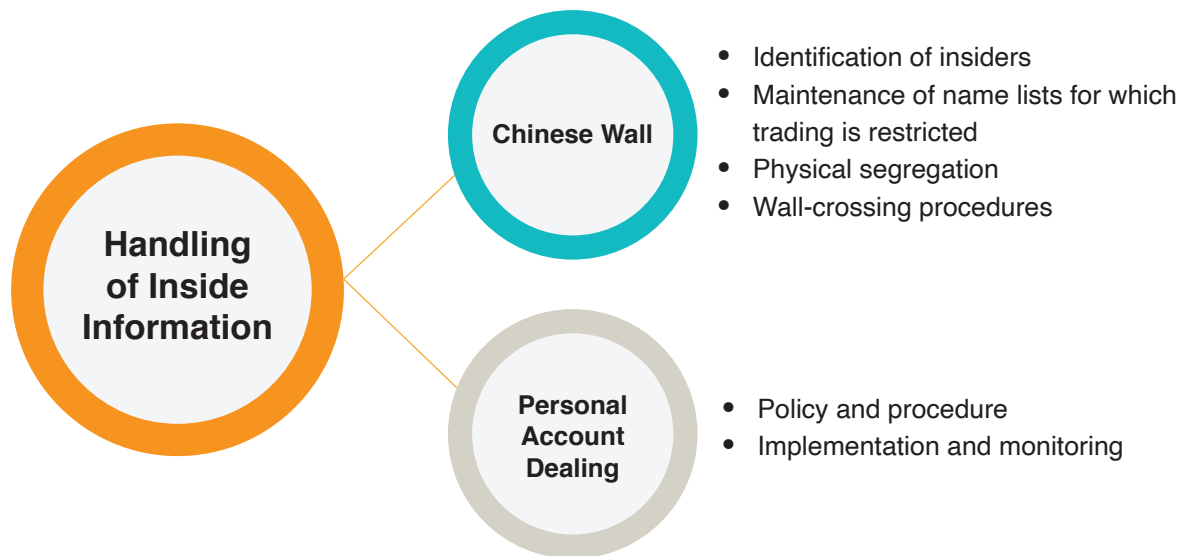
### DON'Ts

- ✗ Absence of periodic review to ensure the physical and system access matrices are up to date. A common audit finding is that some former employees still remain as authorised users in the relevant systems.



## Handling of Inside Information

- 12.44 Inside information in the context of wholesale markets refers to material non-public information that can be acted upon to derive financial gain. Examples include knowledge of an impending market exercise or announcement as well as unreleased financial results. For banking institutions, such information typically originates from capital market advisory and corporate lending businesses, as well as research departments.
- 12.45 The risk of insider dealing, as discussed in section 11, can arise when dealers are consulted pursuant to the above activities. These dealers are deemed to have crossed the information barrier (i.e. Chinese Wall) intended to limit the number of persons in possession of inside information, and become 'insiders' themselves.
- 12.46 Institutions should have measures in place to prevent and detect insider dealing by employees trading in a personal capacity and/or on behalf of the institution (i.e. proprietary trading).
- 12.47 The steps necessary to properly handle inside information can be summarised into the following:
- (1) keeping track of insiders via Chinese Wall policies and procedures;
  - (2) detecting insider dealing in the institution's proprietary trading; and
  - (3) monitoring the personal trades (i.e. personal account dealing) of insiders.
- 12.48 As detection of insider dealing in the context of institutions' own trading has been discussed in section 11, Chinese Wall and personal account dealing policies, procedures and controls will be the focus here.



## i. Chinese Wall

- 12.49 Each institution, where applicable, should have a Chinese Wall policy which addresses the following:
- (a) identification of insiders;
  - (b) wall-crossing procedures and treatment of new insiders;
  - (c) identification and maintenance of a list of client names where the organisation may be in possession of non-public market-sensitive information (e.g. watch list, restricted list, etc); and
  - (d) physical separation of work areas between insider departments and other departments.
- 12.50 Institutions should maintain complete records of employees' wall-crossing, including those where the inside information originated from an affiliated institution. For example, a commercial bank should record instances where its employees were wall-crossed to provide consultation to its investment banking subsidiary.

### Industry Practices

#### DOs

- ✓ Dual sign-off from Compliance and business heads is required when requesting for an employee to be wall crossed, with justification given on the duration and necessity.
- ✓ Wall-crossed employees are required to sign a declaration or letter of undertaking that they acknowledge and will abide by the requirements, responsibilities and restrictions when brought over the wall.
- ✓ Wall-crossed employees are subjected to surveillance whereby trades executed by the said employees in a professional (on behalf of the institution) or personal capacity are scrutinized against watch, grey or restricted lists for irregular activity.
- ✓ Employees who are deal team members or wall-crossed for a capital market deal are tagged as insiders with regard to the client.
- ✓ Individuals who are consistently privy to material non-public information are identified as 'Permanent Insiders', and the list is updated as required.

#### Example:

- ◆ *Members of the Corporate Banking division, Group Credit Committee and Group Investment Underwriting Committee are designated as 'Permanent Insiders'.*

- ✓ Maintenance of the respective insider and restricted name lists, as well as wall-crossing requests are facilitated via system and centrally managed by an independent Control Room function within Compliance.

#### DON'Ts

- ✗ Insufficient physical segregation between public and private side employees.

#### Example:


- ◆ *Situated in close proximity, unsecured telephone lines, frequent sharing of unsecured common areas for discussion and meetings.*

## ii. Personal Account Dealing

- 12.51 Each institution should have measures to deter and prevent its employees from acting on inside information in their possession. Particular focus should be given to trading in equity, which is the most accessible product to individuals.
- 12.52 Many institutions with capital market business activities choose to institute pre-emptive controls over the personal trading of their employees at the pre-transaction stage, rather than adopt the more passive approach of conducting post-reviews of their employees' trading.
- 12.53 Common elements pertaining to the pre-emptive controls include:
- (a) requirement for employees to request and obtain approval prior to executing any personal equity trades;
  - (b) cross referencing against the designated lists (e.g. Watch List, Restricted List), and factoring in employees' classification as an insider, prior to approving requests to conduct personal trades; and
  - (c) having a platform or system to automate the approval process with regard to (a) and (b).
- 12.54 There should be clear procedures for escalation in the event employees are suspected of insider dealing for their own account. Institutions should consider factors like the direction of the trades involved relative to the nature of the inside information in making their assessment.

### Industry Practices

#### DOs

- 
- ✓ Approval of personal trades is centrally managed by an independent Control Room function typically residing within Compliance.
  - ✓ Additional sign-off by immediate supervisor is incorporated into the approval process to address issues such as potential time lag between receipt of inside information and inclusion of the relevant counter in the institution's designated lists.
  - ✓ A 'validity' period is specified for employees to execute their trades once approval is granted. A reasonable benchmark is 48 hours.
  - ✓ For institutions with an equity-brokerage arm, the following practices strengthen pre-emptive controls by addressing the issue of non-disclosure.
    - ➔ Employees are required to close trading accounts at other institutions (i.e. only one trading account is maintained with the employer).
    - ➔ All employee trades are executed by a designated dealer within the institution, who must sight evidence of approval beforehand. Employees do not have access to online trading.
  - ✓ Obtaining Bursa CDS statements from employees to reconcile employees' trading against disclosures made, to ensure compliance with the personal account dealing policy.
  - ✓ Policy on personal account dealing may stipulate:
    - ➔ A minimum holding period for equities purchased by employees. Some institutions also specify a daily limit on employees' personal trading.
    - ➔ Requirement for employees to disclose the trading activity of connected persons such as household members, those financially dependent on said employee or parties on behalf of whom the employee executes trades and/or makes key investment decisions.

## Industry Practices



### DOs

- ✓ Post-reviews on the trading activities of insiders to determine if pre-emptive controls continue to operate effectively.
- ✓ Scrutiny over the volume of personal account dealing requests and reporting can help to detect abnormalities. Low volumes may indicate employees are not consistently or fully making disclosures.
- ✓ Personal account dealing policy also addresses treatment for directors of the institution who were exposed to inside information.
- ✓ Owners of inside information (i.e. investment banks) take accountability and provide oversight on handling of inside information within their banking group.

#### **Example:**

- ◆ *Employees that are wall crossed from the commercial or Islamic bank are subjected to similar personal account dealing controls.*



### DON'Ts

- ✗ Having no oversight on the personal account dealing of employees that are wall-crossed from other institutions within the banking group.
- ✗ Prematurely concluding a particular incident as free of insider dealing based on a relatively low transaction size. Institutions should remember that any action to trade based on inside information constitutes insider dealing.
- ✗ Lack of consequence management for breaches of personal account dealing policy (e.g. non-disclosure).

## Conflicts of Interest

- 12.55 A conflict of interest arises when an institution is placed in a situation of prioritising between competing interests and/or duties involving two or more parties, where choosing one may lead to detrimental outcomes for the other. If left unmanaged, conflicts of interest can become a precursor to misconduct.
- 12.56 Institutions will invariably find themselves inherently exposed to conflicts of interest in the normal course of business, and should seek to manage these situations by taking appropriate steps to identify and mitigate conflicts.
- 12.57 The following perspectives provide context to the different types of conflicts of interest that institutions should be aware of:

Category / Type	Examples
Client vs client (in relation to services provided by the institution)	<ul style="list-style-type: none"><li>• Prioritising between competing client orders for an asset, which can be in the context of brokerage, sales activities or book-building pursuant to a capital market issuance.</li></ul>
Institution vs client	<ul style="list-style-type: none"><li>• Holding a proprietary position in an asset while concurrently advising clients on the asset.</li></ul>
Employee vs institution/client (personal conflicts)	<ul style="list-style-type: none"><li>• Receiving E&amp;G that could affect decision-making in pursuing the employer's best interests.</li><li>• Personal relationships (e.g. relative or spouse acting as counterparty at another institution or holding a high position in a company) that could impair the ability to make decisions or give advice objectively to the employer or clients.</li><li>• Personal account dealing could similarly affect decision-making or incentivise taking advantage of knowledge of proprietary positions or client orders.</li></ul>
Others	<ul style="list-style-type: none"><li>• In pursuing the group agenda, safeguarding the interests of two entities within a banking group transacting with each other, where different stakeholders may have conflicting interests (i.e. depositors or shareholders).</li><li>• Submission of benchmark rates by the institution while having significant holdings of financial products that derive their value from those rates.</li></ul>

- 12.58 This segment is intended to provide guidance on managing structural conflicts that are present in an institution's business activities and processes.
- 12.59 A framework and a 'conflicts register' are useful tools for an institution to systematically identify and manage potential conflicts of interest from its wholesale market activities.

### Conflicts of Interest Framework

- Addresses the identification, documentation, management, and escalation of conflicts of interest in the course of carrying out financial and capital market activities.
- Provides guidance to business units on assessing the materiality and impact from identified conflicts, and deciding on mitigating actions.
- Gives clear examples of conflict scenarios as a guide in making assessments.
- Specifies actions that should be taken in the case of conflicts that cannot be satisfactorily mitigated via existing policies, procedures and controls (e.g. disclosure to clients, internal escalation, etc).

### Conflicts of Interest Register

- Facilitates identification of potential conflicts by business units at specified intervals (e.g. annually or semi-annually, upon launching a new product or business activity, etc).
- A central register should be maintained by the institution based on the consolidated inputs of respective business units.
- Key fields in the register include a description of each conflict, the likelihood and potential impact to which parties, mitigating controls in place, materiality after taking into account the residual level of risk, as well as next action steps with accompanying justifications.



## Industry Practices



### DOs

- ✓ Conflict of interest is recognised as a critical aspect to manage, with relevant policies and procedures in place.
- ✓ Examples given on conflicts of interest scenarios are as comprehensive as possible, based on the scope of the institution's business activities and nuances associated with each business line.
- ✓ Providing regular training and refreshers to employees to facilitate the identification of conflicts.
- ✓ Conflicts of interest receive sufficient senior management oversight by becoming a discussion agenda at specialised working group committees.
- ✓ Periodic engagement between the central controller of the institution's conflicts register and respective business units, to ensure the completeness of conflicts identified as well as mitigating actions.



### DON'Ts

- ✗ Identification and management of conflicts is confined to personal conflicts. Management of conflicts is limited to submission of an annual declaration of potential conflicts of interest, or disclosures at the pre-deal or transactional level. There is no further action to follow up on and manage personal conflicts other than for record-keeping.
- ✗ Conflict of interest is solely documented and only broadly identified as a risk in business units' RCSA tool. This is ineffective because:
  - ➔ Conflicts can differ greatly in nature across scenarios and require mitigating actions specific to each, thus requiring separate documentation and scrutiny in order to be managed effectively.
  - ➔ Risks identified via RCSA also tend to be filtered at the consolidated level, in favour of more common risks, potentially dropping from the institution's radar.

## Compliance Function

- 12.60 The compliance function (referred to as "Compliance") within an institution plays a significant role in administering checks and controls which contribute to managing wholesale market conduct. The following tasks are commonly under their purview:
- (a) trade and/or communications surveillance;
  - (b) issuing policies on Chinese Wall and personal account dealing by employees and directors, as well as coordinating and overseeing processes stipulated in these policies; and
  - (c) conducting periodic reviews on compliance with regulatory requirements and internal policy and procedures, or performing continuous monitoring where appropriate, such as for benchmark rate submissions or specific policy requirements.
- 12.61 Compliance may also take on responsibility as the coordinator in providing the board and senior management with a holistic view on wholesale market conduct, as outlined in paragraph 12.10.

## Industry Practices



### DOs

- ✓ Performing frequent and comprehensive reviews to establish that controls continue to work effectively in ensuring compliance with internal policies and regulatory requirements.

#### **Example:**

- ◆ *Compliance conducts periodic control testing with regard to internal conduct related policies as well as the Code of Conduct.*
- ◆ *In some institutions, a rigorous approach is taken when conducting reviews which include interviewing employees, sampling and validation of relevant documentation. This approach allows Compliance to assess the design of controls in place to conclude on their effectiveness.*

- ✓ Control Room function acts as a central and independent point of reference for areas relating to handling of inside information.
- ✓ Conducting quality assurance (i.e. validation reviews) on the work performed by the trade and communications surveillance team.
- ✓ Holding training sessions for employees within the institution on regulatory requirements and internal policy and procedures.



### DON'Ts

- ✗ Local Compliance does not take on an active role in understanding the review approach and outcomes of conduct-related compliance reviews performed by group or regional functions. Thus, local Compliance is unable to assess whether further review procedures or institutional controls are necessary.
- ✗ Local Compliance predominantly acts as a point of contact for escalation or follow up on queries from global or regional hub without further assessing the adequacy of the surveillance programme vis-à-vis local trading profiles.
- ✗ Surface-level understanding of financial market mechanics (e.g. how financial products are traded) and how market misconduct works. This undermines the quality of assessments on exposure to market conduct-related risks and analysis of surveillance alerts, where applicable.

#### **Example:**

- ◆ *In some institutions, Compliance does not escalate outcome from reviews conducted at a regional or global level to the institution's Board and Senior Management. In instances where these are escalated, there is no assessment of its adequacy.*
- ◆ *This may indicate a lack of ownership in managing local market abuse and misconduct risks.*

## Internal Audit

- 12.62 In the context of wholesale market conduct, the internal audit function (referred to as “Internal Audit”) must validate the adequacy and implementation of policies and procedures established by business units and second line control functions to address conduct risks.
- 12.63 Internal Audit must incorporate market conduct risk in formulating its audit plan. The decision on frequency of review over auditable units should factor in indicators such as the size and complexity of the institution’s market activities.
- 12.64 Assessment of the institution’s effectiveness in managing conduct risks in wholesale markets must be incorporated in audit procedures and may involve cross-department thematic reviews where appropriate. Areas that should be covered include but are not limited to:
- (a) market conduct risk assessment;
  - (b) trade and communications surveillance programme;
  - (c) dealing room conduct control practices (e.g. compliance with mandatory block leave policy, maintenance of E&G registers, etc.); and
  - (d) controls pertaining to handling of inside information and personal account dealing.
- 12.65 The market conduct risk assessment (section 9) can be a useful tool to assist audit planning and an audit assessment of the effectiveness of the institution’s surveillance programme and controls.

### Industry Practices



#### DOs

- ☒ Checking for compliance with regulatory requirements stipulated in conduct-related policies (e.g. Code of Conduct).
- ☒ Audit coverage of trade surveillance includes governance and methodologies used to determine surveillance parameters and thresholds, as well as quality and consistency of analysis in reviewing surveillance alerts.



#### DON'Ts

- ☒ Surface-level assessment of conduct controls (i.e. box-ticking) without assessing the effectiveness of implementation or whether there are any gaps that can be addressed by improving the design of existing policies and controls.

## 13. The Role of Culture in Promoting Good Conduct


- 13.1 Organisational or business culture plays a significant role in shaping employees' behaviours, and is often cited as the root cause of misconduct within the financial services industry. Misaligned performance measures and remuneration practices are typical examples of factors which lead to excessive risk taking by wholesale market participants.
- 13.2 This section seeks to provide guidance on practices that can reduce the propensity for misconduct in the context of wholesale financial markets.

### Remuneration and Key Performance Indicators

- 13.3 Overly aggressive financial performance targets in Key Performance Indicators (KPI) can encourage excessive risk-taking or misconduct. This may be further exacerbated by remuneration structures that grant immediate and outsized rewards for exceeding performance targets.
- 13.4 Most institutions incorporate both financial and non-financial indicators (e.g. risk, compliance, conduct, etc) in employees' KPIs, which promotes a more balanced measure of performance.
- 13.5 The following observed remuneration practices generally promote good conduct and accountability:
- (a) avoiding excessive variable compensation structures that reward meeting aggressive business targets;
  - (b) staggered or deferred payout structures for variable compensation<sup>12</sup>; and
  - (c) malus and clawback provisions.

#### Industry Practices

##### DOs

- 
- ✓ Conscious effort to manage the amount of fixed vs. variable compensation paid to employees, with some institutions setting an appetite or policy on a ratio between the two.
  - ✓ Reasonable structure for deferred payment of variable compensation. For example, equal instalments paid over a 3-year period.
  - ✓ Bonus pools for dealers are allocated jointly between the Treasury Head and representatives from the Human Resource department, which enables better transparency and consistency in awarding variable compensation.
  - ✓ All aspects of compliance (e.g. mandatory block leave, training, personal account dealing) and conduct are considered in determining performance and compensation. For some institutions, this process is facilitated by a system.
  - ✓ Malus and clawback provisions apply to all employees, and not just certain individuals in material risk-taking positions.

<sup>12</sup> For many institutions, this only applies to individuals in material risk-taking positions, who are identified based on an internal standard definition applied across business units. Based on this definition, most dealers are excluded from deferred compensation as they typically do not meet the threshold on variable compensation to be considered a 'material risk taker'. In this regard, institutions may wish to consider and evaluate wider application of deferred compensation for their dealers given the comparatively greater financial impact their activities can have on the institution.

## Industry Practices



### DON'Ts

- ☒ Low weightages (typically less than 10%) assigned to non-financial KPIs, with poor descriptions of non-financial KPI deliverables. This gives the impression that a good performance rating can still be achieved by solely focusing on profit-making at the expense of other areas.
- ☒ Sole discretion of Treasury Head to allocate bonus pools. Consequently, misconduct by some dealers may be overlooked in decision-making, inadvertently or otherwise.
- ☒ Deferred compensation structures feature short deferral periods. In some cases, most of the deferred sum is paid out within the following 6 months, which does not serve to hold employees accountable for their risk-taking as outcomes may materialise over a longer period.

## Consequence Management

- 13.6 Consequence management concerns how the institution should handle breaches of conduct by its employees.
- 13.7 Institutions are typically guided by an internal framework which stipulates possible disciplinary actions that can be taken. This ranges from letters of advice to outright dismissal.

## Industry Practices



### DOs

- ☒ Disciplinary actions taken are considered in the pay out of variable compensation. Some institutions have established a matrix which specifies varying levels of cuts to compensation (e.g. ranging from 5% up to 100%) depending on the frequency and severity of the misconduct.
- ☒ A stand-alone consequence management framework caters to specific types of breaches and misconduct in treasury business. This typically supplements a bank-wide consequence management framework.

### DON'Ts

- ☒ Loosely defined consequence management framework with wide discretion in decision-making for breaches and misconduct.
  - ➔ No guidance on how to treat relatively minor but repeated policy breaches in the context of treasury and trading activities.

#### Example:

- ◆ Minor breaches are not tracked. (e.g. high count of trade cancellations and amendments due to dealers' error; executing personal trades after the corresponding post-approval validity period has expired).
- ◆ These breaches are not considered when conducting performance appraisals, leading to minimal or no consequence for the employee.

## Training

- 13.8 Training has become increasingly important to reinforce good conduct amongst dealers.
- 13.9 Banking institutions have commonly been observed to provide limited training on wholesale market conduct for dealers as well as personnel in the second and third lines of defence (i.e. Compliance, Risk Management and Internal Audit). Training typically covers conduct topics such as anti-money laundering and anti-bribery and corruption, with little or no focus on market conduct.
- 13.10 Institutions must provide periodic training and refreshers on key conduct topics including, but not limited to:
- (a) understanding market abuse risks;
  - (b) good dealing practices for various financial products and markets;
  - (c) handling inside information (i.e. Chinese Wall and personal account dealing policy and procedures); and
  - (d) identifying and managing conflicts of interest in daily functions.
- 13.11 Institutions must also provide dealers with training and awareness programmes in the area of compliance and risk management practices. These should be designed to instil awareness on treasury related risks, regulatory requirements, and the control environment that should be observed.
- 13.12 Surveillance analysts are typically trained on-the-job. However, institutions must improve the skillset and capabilities of surveillance analysts by providing frequent and targeted training on reviewing and investigating misconduct.
- 13.13 Training must also be extended to back office personnel to enable them to identify misconduct in the course of performing trade operations.





## Appendix 1

### Example of Market Conduct Risk Assessment

Financial Product Traded	Trading Profile	Exposure to Potential Market Misconduct					
		E.g. Wash Trading	Front Running	Position Parking	Spoofing	Ramping	Etc.
FX Spot	[Key trading profile indicators such as but not limited to Transaction Count, Percentile analysis of transactions, Transaction Volume, Transaction Size, Revenue Contribution etc.]	(Insert risk level) e.g. Low-medium risk. – High trading volume / market share. (provide statistics) – Market benchmarks for the institution's commonly traded currencies are not calculated based on market volumes within a short window. – Motive to mislead the market is unlikely as information on market volume is not available real-time or intraday. – Possible wash trades with the motive of generating brokerage fees.	(Insert risk level) e.g. High risk. – In practice, FX dealers are consulted on the pricing for large client orders. – Only 1% of deals with clients are considered large, however there are a few hundred such deals in a year.	(Insert risk level) e.g. Low risk – What is the possibility and motivation of FX traders colluding to conceal net open positions or forex losses to evade detection by middle office?	(Insert risk level) – As this type of misconduct involves creating a false impression of market orders, are order queues visible to market participants for them to be misled? – Trading volume / market share?	(Insert risk level) – As this type of misconduct involves creating a false impression of market price direction, is real-time data/charts on market prices visible to market participants for them to be misled? – Trading volume / market share?	...
		<b>Surveillance Decision</b> <ul style="list-style-type: none"> <li>Should there be surveillance over this abuse scenario given the trading profile and susceptibility to market misconduct?</li> <li>What parameters would best suit the type of market misconduct under surveillance and what thresholds would best suit the trading profile?</li> <li>What is the result of back-testing and recalibration exercises that should result in changes to parameters or thresholds?</li> </ul>					
		✓ Implement surveillance to address the possibility of compensation trades  ✓ Parameters :  ✓ Thresholds : price variation, size variation, lookback periods etc.  ✓ Recalibration Input:	✓ Implement surveillance to detect front running.  ✓ Parameters : Min. client order size, lookback periods etc.  ✓ Threshold : Min. client order threshold is set at RM50m as xx% of client trades are <RM50m.		...	...	

Financial Product Traded	Trading Profile	Exposure to Potential Market Misconduct					
		E.g. Wash Trading	Front Running	Position Parking	Spoofing	Ramping	Etc.
FX Forward	...	...	...	...	...	...	...
		<b>Surveillance Decision</b> <ul style="list-style-type: none"> <li>Should there be surveillance over this abuse scenario given the trading profile and susceptibility to market misconduct?</li> <li>What parameters would best suit the type of market misconduct under surveillance and what thresholds would best suit the trading profile?</li> <li>What is the result of back-testing and recalibration exercises that should result in changes to parameters or thresholds?</li> </ul>					
etc.	...	...	...	...	...	...	...
Government Securities		(Insert risk level) – Can this method be used to influence benchmark/closing prices for less liquid bonds?  – Is there available real-time data on market volumes?	(Insert risk level) – Statistical distribution of client deals? – Ease/viability of front running?	(Insert risk level) – What is the level of trading book activity? (provide statistics) – How prevalent is trading in less liquid bonds?	...	...	...
		<b>Surveillance Decision</b> <ul style="list-style-type: none"> <li>Should there be surveillance over this abuse scenario given the trading profile and susceptibility to market misconduct?</li> <li>What parameters would best suit the type of market misconduct under surveillance and what thresholds would best suit the trading profile?</li> <li>What is the result of back-testing and recalibration exercises that should result in changes to parameters or thresholds?</li> </ul>					
		√ ... √ ...	√ ... √ ...	√ ... √ ...			
Private Debt Securities							
Listed Equities		...	...	...	...	...	...
Equity Derivatives		...	...	...	...	...	...
etc.		...	...	...	...	...	...

## Appendix 2

### Examples of Calibration Techniques for Setting/Reviewing Trade Surveillance Thresholds

The following are examples of calibration techniques that have been observed being practised in the industry. Institutions should exercise judgment in applying these techniques to their own surveillance scenarios.

Type of threshold	Techniques
Transaction value / quantity	<p>Typically concerns thresholds on the units/amount/value of a product that needs to be transacted for a surveillance alert to be triggered (e.g. an alert is generated if the minimum transaction size of RMx or x share units is met).</p> <ul style="list-style-type: none"> <li>Percentile analysis of the institution's past trades or contribution to market volume (e.g. arranging a counter's trade quantity or trade value per trade/account sequentially for a given period, and sensitizing thresholds based on the trade quantity or value corresponding to the levels at 95%, 90% of that sequence).</li> <li>Statistical distribution (e.g. mean, mode median) of a particular counter's trades/cancellations can also be useful to determine an appetite of what would be considered irregular.</li> </ul>
Number of price layers	<p>Typically concerns thresholds on the number of price levels that must be present in a set of trades/orders before being flagged as a surveillance alert (e.g. an alert is generated if a set of order cancellations involved x or more price levels).</p> <ul style="list-style-type: none"> <li>Reconciling historical order book partial fills/cancellations against the corresponding number of price levels involved to determine what would be considered irregular (e.g. if 90% of orders that resulted in partial fills/cancellations involved 2 price levels, a more effective threshold may be higher than 2).</li> </ul>
Time interval / lookback period	<p>Typically concerns thresholds on the length of time within which a surveillance scenario will examine for specific misconduct behaviours (e.g. an alert is generated if a set of trades within a x minutes displays wash trade behaviours).</p> <ul style="list-style-type: none"> <li>Volume analysis, which computes the average number of trades per day, per minute for a particular product. An appropriate time interval threshold can be inferred from the amount of time needed for a sizeable number of trades to conclude (e.g. if there are 10 trades per minute on average for one product vs 0.5 trades for another, differentiated thresholds such as 3 minutes for the former and 10 minutes for the latter may be considered).</li> <li>Institutions may also work backwards by using time as a starting point and examining the distribution to determine what is irregular (e.g. if 90% of order cancellations occurred more than 10 minutes after the order was placed, the time to cancellation corresponding to the remaining 10% may be of greater interest).</li> </ul>

## References

- Behavioural Cluster Analysis – Misconduct Patterns in Financial Markets (2018). *FICC Markets Standards Board*.
- MAS-SGX Trade Surveillance Practice Guide (2019). *Monetary Authority of Singapore, Singapore Exchange Regulation*.
- Wholesale Market Conduct Risk – Dear CEO Letter (2019). *Central Bank of Ireland*.
- FX Global Code (2021). *Foreign Exchange Working Group*.
- Conflicts of Interest Statement of Good Practice (2019). *FICC Markets Standards Board*.
- Strengthening Governance Frameworks to Mitigate Misconduct Risk: A Toolkit for Firms and Supervisors (2018). *Financial Stability Board*.
- Risk management and operational resilience in a remote working environment (2021). *Monetary Authority of Singapore and the Association of Banks in Singapore*.
- Spotlight Review: Hybrid Working in FICC Markets – Future Risk Management Frameworks (2021). *FICC Markets Standards Board*.



