廉政公署
ICAC

CPAS 防貪諮詢服務
Corruption Prevention Advisory Service

CORRUPTION PREVENTION GUIDE FOR BANKS

Addendum

Corruption Prevention Services for the Private Sector

Please note that with effect from 10 September 2026, the Corruption Prevention Advisory Service (CPAS) and the Hong Kong Business Ethics Development Centre (HKBEDC) of the Independent Commission Against Corruption (ICAC) have been restructured as the Private Sector Integrity Centre (PSIC).

Accordingly, any references to the CPAS and HKBEDC in this publication are to be read as referring to the PSIC from that date onwards.

As a one-stop service and knowledge hub, PSIC continues to provide free, confidential, and tailor-made corruption prevention and integrity services to private-sector organisations.

For enquires or services, please contact PSIC through the following channels:

- Hotline: 2526 6363
- Email: psic@cpd.icac.org.hk
- E-form: eform.cefs.gov.hk/form/ica004/en/
- Website: psic.icac.org.hk

Disclaimer

(In the event of any inconsistency or conflict between the following disclaimer and the disclaimer contained in other part of the publication, the following disclaimer shall prevail to the extent of the inconsistency or conflict.)

Descriptions and explanations of the legal and regulatory requirements under the Prevention of Bribery Ordinance (Chapter 201 of the Laws of Hong Kong) and any other ordinances, subsidiary legislation, orders, rules, regulations and case law (collectively, "Laws and Regulations") in this publication are intended to be general and abbreviated for ease of understanding. Users of this publication are advised to refer to the original text of the Laws and Regulations if considered necessary. Case scenarios are used in this publication to illustrate the legal and regulatory requirements and corruption risks. These case scenarios should be taken as hypothetical and not referring to any particular real case or any particular organisation or person. Moreover, the advice and recommendations given in this publication are by no means prescriptive or exhaustive, and are not intended to substitute any legal, regulatory or contractual requirements. Users should refer to the relevant instructions, codes and guidelines issued by the relevant authorities, and adopt the appropriate measures that best suit their operational needs and risk exposure.

The descriptions and explanations of the Laws and Regulations, case scenarios, advice and recommendations given in this publication are for general reference purposes only. The ICAC makes no warranties, express or implied, as to the accuracy, completeness, suitability and applicability of the aforesaid descriptions, explanations, case scenarios, advice and recommendations. The ICAC shall not have or accept any liability, obligation or responsibility whatsoever for any loss or damage incurred directly or indirectly by any person acting or refraining from acting in reliance upon the descriptions, explanations, case scenarios, advice, recommendations or any other information provided in this publication. Users of this publication are strongly advised to seek professional legal or other appropriate advice in relation to the information contained in this publication if considered necessary.

Private Sector Integrity Centre
Independent Commission Against Corruption
10 September 2026

廉政公署 ICAC

PSIC 私營機構誠信建設中心 Private Sector Integrity Centre

Table of Content

Foreword

Chapter 1 Legislation and Other Requirements/Guidelines

1.1 Introduction 8

1.2 Prevention of Bribery Ordinance (Cap. 201) 8

1.2.1 Sections 9(1) & 9(2) – Corrupt Transactions with Agents 8
Case Study 1 – Offering/Accepting Advantages in relation to Loan Extension 9

1.2.2 Section 9(3) – Use of Misleading/False/Defective Document to Deceive Principal 12
Case Study 2 – Using Falsified Receipts to Deceive Reimbursement 12

1.2.3 POBO Provisions Governing Public Servants and Persons Having Dealings with Public Servants 13
Case Study 3 – Offering Gifts to Public Servants while Having Business Dealings 14

1.3 Other Major Legal Concerns 15

1.3.1 Banking Ordinance (Cap. 155) 15

1.3.2 Securities and Futures Ordinance (Cap. 571) 15

1.3.3 Theft Ordinance (Cap. 210) 16

1.3.4 Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) 16

1.3.5 Organized and Serious Crimes Ordinance (Cap. 455) 16

1.3.6 Personal Data (Privacy) Ordinance (Cap. 486) 17

1.3.7 Extra-territorial Legal Obligations 17

1.4 Regulatory and Professional Guidelines/Requirements 18

1.4.1 Hong Kong Monetary Authority 18

1.4.2 The Hong Kong Association of Banks and The DTC Association 18

1.4.3 Securities and Futures Commission 19

1.4.4 Insurance Authority 19

1.4.5 Mandatory Provident Fund Schemes Authority 19

1.4.6 Office of the Privacy Commissioner for Personal Data 19

1.4.7 Hong Kong Exchanges and Clearing Limited 20

Chapter 2 Standards of Behaviour and Integrity Management

2.1 Introduction 24

2.2 Fostering a Clean Business Culture 24

2.3 Essential Probity Requirements in a Code of Conduct 26

2.3.1 Company Statement 26

2.3.2 Prohibition of Bribery 26

2.3.3 Acceptance and Offer of Advantages 28

2.3.4 Acceptance of Entertainment 30

2.3.5 Conflict of Interest 30

2.3.6 Misuse of Official Position 33
2.3.7 Safeguard of Customers' Funds and Interests 33
2.3.8 Handling of Records, Accounts and Other Restricted Information 33
2.3.9 Personal Investments 33
2.3.10 Outside Employment/Work 34
2.3.11 Reporting of Violations, Suspected Corruption and Other Criminal Offences 34
2.3.12 Compliance with Laws and Other Professional Standards and Regulatory Requirements 34
2.3.13 Compliance with Code of Conduct 35
2.4 Making Ethical Decision – ETHICS-PLUS Decision Making Model 35

Chapter 3 Governance and Anti-Corruption Control

3.1 Introduction 38
3.2 Respective Roles in Implementing Anti-Corruption Policy and Controls 39
3.2.1 The Board 39
3.2.2 Committees 39
3.2.3 Independent Non-executive Directors 39
3.2.4 Senior Management 40
3.2.5 Managers Undertaking Key Control Functions 40
3.2.6 Staff in General 40
3.3 Key Elements of Anti-Corruption Control 41
3.3.1 Clear Policies, Work Procedures and Guidelines 42
3.3.2 Corruption Risk Assessment and Management 42
3.3.3 Checks and Balances 43
3.3.4 Record Keeping and Information Security 43
3.3.5 Supervisory Monitoring and Accountability 44
3.3.6 Training 44
3.3.7 External Communication 45
3.3.8 Complaint and Reporting Channels 45
3.3.9 Reviews and Audits 46
3.3.10 Control through Digitalisation and Regtech Solutions 47
3.4 Controls Against Money Laundering 48

Chapter 4 Management of Bank Accounts

4.1 Introduction 52
4.2 Key Processes 53
4.3 Major Corruption Risks and Red Flags 53
4.3.1 Bank Account Opening 53
Case Study 1 – Soliciting Handling Fees for Opening Corporate Accounts from Customers 54
Case Study 2 – Conspiracy with Intermediaries to Submit False Information on Account Opening Applications 55
4.3.2 Management of Customers' Personal Data and Bank Account 57

Case Study 3 – Misuse of Customers' Personal Information 57
Case Study 4 – Bribe for Assistance in Money Laundering 59
4.3.3 Online Banking 60
4.4 Corruption Prevention Safeguards 62
4.4.1 Guidelines and Instructions 62
4.4.2 Account Opening 62
4.4.2.1 Application Process 62
4.4.2.2 Checking Process 63
4.4.2.3 Account Opening through Online Banking 63
4.4.3 Safeguarding of Customers' Personal Data 64
4.4.4 Management of Customers' Bank Accounts 66
4.4.5 Banking Services through Online Banking 66
4.4.6 Anti-money Laundering Measures 67
4.4.7 Staff Training 68

Chapter 5 Credit Facility and Loan Services

5.1 Introduction 72
5.2 Key Processes 73
5.3 Major Corruption Risks and Red Flags 73
5.3.1 Submission of Loan Applications by Applicants 73
Case Study 1 – Conspiracy with an Intermediary for Deceiving Commissions 74
Case Study 2 – Conspiracy with Customer to Conceal Material Facts in Loan Application 75
Case Study 3 – Acceptance of Bribe for Assistance in Application for Government-Guaranteed Financing Scheme 77
5.3.2 Customer Due Diligence and Completion of Application Documents 79
Case Study 4 – Using False Documents to Deceive Mortgage Referral Fees 79
Case Study 5 – Acceptance of Advantages during Site Inspection outside Hong Kong 81
5.3.3 Credit Assessment and Approval of Loan Applications 83
5.3.4 Compliance with Terms of Credit Facility and Repayment of Loan 83
5.4 Corruption Prevention Safeguards 84
5.4.1 Guidelines and Instructions 84
5.4.2 Submission of Application and Supporting Documents 85
5.4.3 Site Inspection and Work Outside Hong Kong 86
5.4.4 Safeguards for Government-Guaranteed Financing Scheme 87
5.4.5 Credit Assessment and Approval of Application 87
5.4.6 Notification of Results 89
5.4.7 Loan Repayment and Approval of Extension 89
5.4.8 Staff Training 89

Chapter 6 Sales Process and Wealth Management

6.1 Introduction 92

6.2 Key Processes 93

6.3 Major Corruption Risks and Red Flags 93

6.3.1 Selling of Investment/Insurance Products and Wealth Management Services and Products / Referral of Business 93
Case Study 1 – Conspiracy with Outsiders for Deceiving Customer into Taking Out Insurance Policy for Illegal Commissions 94

6.3.2 Handling of Purchase for Investment/Insurance Products 95
Case Study 2 – False Representation of Handling Staff on Application Forms to Deceive Commission 95

6.3.3 Wealth Management Services and Products 97
Case Study 3 – Soliciting Additional Commission from Customers 97

6.4 Corruption Prevention Safeguards 99

6.4.1 Guidelines and Instructions 99

6.4.2 Remuneration Structure and Incentive System 100

6.4.3 Selling of Investment/Insurance Products and Wealth Management Services and Products / Referral of Business 101

6.4.4 Handling of Application/Instruction for Investment/Insurance Products 102

6.4.5 Provision of Wealth Management Services and Products 102

6.4.6 Staff Training 103

Chapter 7 Procurement and Staff Administration

7.1 Introduction 106

7.2 Key Processes 107

7.2.1 Procurement 107

7.2.2 Staff Administration 107

7.3 Major Corruption Risks and Red Flags 108

7.3.1 Procurement 108
Case Study 1 – Acceptance of Advantages for Assistance in Service Contract Renewal 109
Case Study 2 – Connivance of Substandard Renovations Outside Hong Kong 111

7.3.2 Staff Administration 112
Case Study 3 – Provision of False Academic Proof for Bank Employment 113
Case Study 4 – Offer of Job Opportunity in Return for Business Opportunities to Boost up Sales Target 114

7.4 Corruption Prevention Safeguards 117

7.4.1 Procurement 117

7.4.1.1 Handling of Personal Data and Confidential Information 117

7.4.1.2 Performance Monitoring 117

7.4.1.3 Procurement Outside Hong Kong 118

7.4.1.4 Staff Training 118

7.4.1.5 Engagement of Service Providers 118

7.4.2 Staff Administration 119

7.4.2.1 Recruitment and Remuneration 119

7.4.2.2 General Controls and Staff Supervision 120

7.4.2.3 Reimbursement of Claims 121
7.4.2.4 Staff Performance Appraisal, Promotion and Disciplinary Action 121
7.4.2.5 Staff Outside Hong Kong 122
7.4.2.6 Staff Training 122

Chapter 8 ICAC Service and Assistance

8.1 Introduction 126
8.2 Corruption Prevention Advisory Services 126
8.3 Education Services 127
8.4 Reporting Corruption 128

Appendices

1 Sample Code of Conduct 130
2 Examples of Conflict of Interest 142
3 Mitigating Measures for Managing Declared Conflict of Interest 143
4 Ethics-Plus Decision Making Model 144

FOREWORD

A system of good corporate governance and robust internal controls is crucial to the success, effective operation and sustainable development of a bank[1]. It helps to ensure that the bank achieves its goals and objectives, complies with applicable laws and regulations as well as internal policies, and effectively mitigates risks of losses or reputational damage. Among the risks faced by a bank, one of the most damaging is corruption, which would not only lead to financial loss but also seriously damage the bank's reputation and erode the trust of its customers and stakeholders. Therefore, an effective anti-corruption and corruption risk management system is a key component of good corporate governance and internal control. It is imperative for banks to be vigilant in upholding high integrity standard and take a proactive stance against corruption through regular risk assessment and adoption of corruption prevention measures including appropriate technologies.

To assist banks in effective corruption prevention and risk management, the **Corruption Prevention Department (CPD)** of the **Independent Commission Against Corruption (ICAC)** has developed this **Corruption Prevention Guide for Banks (the Guide)** for reference by the directors, senior management and managerial staff of banks in Hong Kong with a view to –

(a) ensuring banks', their staff's and agents' compliance with the Prevention of Bribery Ordinance (POBO) (Cap. 201), and entrenching a clean business culture in the bank and in the industry;

(b) enhancing their awareness and knowledge of corruption risks and practices (with case studies, red flags, etc.) so that they may stay alert and vigilant against the risks; and

(c) providing them with practical guidance on anti-corruption policy, system, management and control measures, so as to establish and strengthen corruption prevention capabilities in their banking operations.

Apart from the core and essential corruption prevention measures, this Guide also includes measures that are advisable to be adopted by different institutions in the industry. Individual banks may adopt these measures to suit their operational needs while adhering to the principles. The **Corruption Prevention Advisory Service (CPAS)** of the CPD will provide tailor-made advice on request.

ELECTRONIC VERSION OF THE GUIDE

This Guide is available at

cpas.icac.hk/EN/Info/Lib_List?cate_id=3&id=2728

[1] *Under the Banking Ordinance (Cap. 155), Authorized Institutions covering licensed banks, restricted licence banks, and deposit-taking companies, are authorised to operate banking businesses and/or a business of taking deposits in Hong Kong, and are subject to supervision by the Hong Kong Monetary Authority. For the purpose of this Guide, Authorized Institutions are collectively referred as "banks".*

HOW TO USE THIS GUIDE

For quick and easy reference, users will find the following icons throughout this Guide which lead them to the following information –

Case Studies

hypothetical case scenarios in perspective

Corruption Prevention Safeguards

useful tips for corruption prevention

Corruption Prevention Safeguards (for Customers)

safeguards relating to customers

Corruption Risks

major corruption risks and malpractice

Frequently Asked Questions

frequently asked questions with corresponding guidance given

Good Practices

examples of good practices for Bank's reference

Pointers

cross references to other Chapters/Sections of the Guide

Red Flags

indicators of areas where management oversight is required to safeguard against possible corruption and fraud

Use of Technology

examples of measures where technology may be adopted to reduce corruption risk

FROM THE EDITORIAL BOARD

Descriptions and explanation of legal requirements under the POBO and other relevant ordinances/laws in this Guide are necessarily general and abbreviated for ease of understanding. Users of the Guide are advised to refer to the original text of the relevant ordinances/laws or seek legal advice on particular issues where necessary. The ICAC will not accept any responsibility, legal or otherwise, for any loss occasioned to any person acting or refraining from action as a result of any material in this Guide.

Case scenarios are used in this Guide to illustrate the legal requirements and corruption risks. These case scenarios should be taken as hypothetical and not referring to any particular real case or any particular organisation or person. The advice and recommendations given in the Guide are by no means prescriptive or exhaustive, and are not intended to substitute any legal, regulatory or contractual requirements. Users should refer to the relevant instructions, codes and guidelines issued by the relevant authorities, and adopt the appropriate measures that best suit the operational needs and risk exposure of their organisations. The information contained in this Guide is updated as at the last revision date shown.

Throughout this Guide, the male pronoun is used to cover references to both the male and female genders. No gender preference is intended.

The copyright of this Guide is owned by the ICAC. Interested parties are welcome to reproduce any part of this Guide for non-commercial use. Acknowledgment of this Guide is required.

January 2023

ACKNOWLEDGEMENT

The CPD has consulted the Hong Kong Monetary Authority, The Hong Kong Association of Banks, The Hong Kong Institute of Bankers and The DTC Association in the development of the Guide. Their input and efforts are gratefully acknowledged.

HONG KONG MONETARY AUTHORITY
香港金融管理局

THE HONG KONG ASSOCIATION OF BANKS
香港銀行公會

HKIB
The Hong Kong Institute of Bankers
香港銀行學會

存款公司公會
The DTC Association

[This Corruption Prevention Guide for Banks is for reference only.]

ABBREVIATIONS

AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
CPAS	Corruption Prevention Advisory Service
CPD	Corruption Prevention Department
DTCA	The DTC Association
FI	Financial Intermediary
HKAB	The Hong Kong Association of Banks
HKBEDC	Hong Kong Business Ethics Development Centre
HKEX	Hong Kong Exchanges and Clearing Limited
HKMA	Hong Kong Monetary Authority
HKMC	The Hong Kong Mortgage Corporation Limited
IA	Insurance Authority
ICAC	Independent Commission Against Corruption
INED	Independent Non-executive Director
IT	Information Technology
MPF	Mandatory Provident Fund
OPCPD	Office of the Privacy Commissioner for Personal Data
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
POBO	Prevention of Bribery Ordinance (Cap. 201)
PDPO	Personal Data (Privacy) Ordinance (Cap. 486)
SFC	Securities and Futures Commission
SPM	Supervisory Policy Manual

INTERPRETATION

The following defined terms shall bear their stated meaning in the Guide.

"Banks"	refer to authorized institutions under the Banking Ordinance, covering licensed banks, restricted licence banks, and deposit-taking companies.
"Customer"	include a customer for any bank services and a potential customer for such.
"Fintech"	refer to financial technology adopted in the banking sector.
"Regtech"	refer to the use of technologies that enhances efficiency and/or the effectiveness of risk management and regulatory compliance in the banking sector.

1 LEGISLATION AND OTHER REQUIREMENTS/ GUIDELINES

1.1 INTRODUCTION
1.2 PREVENTION OF BRIBERY ORDINANCE (CAP. 201)
1.3 OTHER MAJOR LEGAL CONCERNS
1.4 REGULATORY AND PROFESSIONAL GUIDELINES/REQUIREMENTS

1 LEGISLATION AND OTHER REQUIREMENTS/GUIDELINES

1.1 INTRODUCTION

To ensure compliance with law and adherence to a high standard of integrity and avoid pitfalls of corruption in carrying out the banks' business, bank directors, staff and industry practitioners should have a clear and adequate understanding of the relevant legal and professional requirements. This Chapter provides an overview of the anti-bribery law (i.e. the Prevention of Bribery Ordinance (POBO) (Cap. 201)) in Hong Kong, and highlights other major legislations and professional requirements governing banks' integrity management and prudent operation.

1.2 PREVENTION OF BRIBERY ORDINANCE (CAP. 201)

The POBO is enforced by the Independent Commission Against Corruption (ICAC) to combat bribery and corrupt transactions in both the private and public sectors. The following is a gist of the relevant sections of the POBO (An extract of the POBO is at ***Annex 1*** of ***Appendix 1***). Full text of the POBO can be found in the Hong Kong e-Legislation of the Department of Justice: *www.elegislation.gov.hk/hk/cap201*

1.2.1 SECTIONS 9(1) & (2) – CORRUPT TRANSACTIONS WITH AGENTS

- **Section 9(1)** – It is an offence for any agent (the text refers to agents under the POBO such as an employee (See definition at ***page 9***)) to, without the permission of his principal (e.g. employer) or reasonable excuse, solicit or accept any advantage as an inducement to or reward for his doing or forbearing to do any act in relation to his principal's affairs or business.
- **Section 9(2)** – Any person who offers an advantage to an agent under the above circumstances also commits an offence.
- The maximum penalty is a fine of $500,000 and seven years' imprisonment.

Case Study 1 – Offering/Accepting Advantages in relation to Loan Extension

1 A corporate customer holds a loan at a bank. He runs into cash flow problem and cannot service the loan repayment. The corporate customer offers expensive gifts such as watch and cigars, to a bank manager (i.e. an agent of the bank under the POBO) and asks for extension of the loan repayment due date for a couple of times.

2 Despite the fact that the bank has issued clear guidelines to all staff on the prohibition of acceptance of any advantage by its staff in performing the bank's duties, the bank manager accepts the gifts, and endorses the extensions of the loan repayment due date when it is within his approving authority or makes favourable recommendations to the bank when it is beyond his authority. The bank grants extensions as recommended.

3 The bank manager and the corporate customer may contravene Sections 9(1) and 9(2) of the POBO respectively.

Analysis and Points to Note –

- **Principal** – The principal of a company generally refers to the employer (i.e. the owner or the board of directors (the Board) of the company) or any person authorised to act on the employer's behalf. In general, the principal of a bank director / staff member usually refers to the bank which appoints/employs him.
- **Agent** – An agent is a person acting for, or employed by, the principal. If a company appoints a person to act for it in business dealings, that person becomes the company's agent irrespective of whether the appointment is full-time or part-time, and whether or not the agent receives a salary or a fee from the company. For example, an employee or a director of a bank is the bank's agent. As far as a bank's daily operations are concerned, its agents include mostly its directors and staff members.
- **Advantage** – An advantage refers to anything that is of value such as money, gift, discount, commission, loan, employment, service or favour (except entertainment).

Q1. Is there a value threshold (e.g. $500) for an "advantage" in the POBO?

A No. Some people misunderstand that the POBO sets out a limit on the value of the advantage below which acceptance is statutorily permissible. In fact, the POBO has **not** specified any threshold or ceiling of allowable advantages. The recipient/offeror may commit an offence if he accepts/offers an advantage of any value in relation to the bank's affairs or business without the permission of the bank (Reference at ***Section 1.2.1***). A private company may permit its staff to accept advantages from other persons related to the company's business up to a specified limit and under certain circumstances. This is the company's internal policy and must not be confused with the provisions of the POBO.

In this regard, banks should issue clear internal policy (e.g. Code of Conduct) on solicitation/acceptance of advantages, and specify the circumstances where acceptance of advantage/gift may be allowed, including the threshold and handling procedures (e.g. seek approval from the appropriate authority, require proper documentation/registration), and communicate the policy to their staff (Reference at ***Section 2.3.3*** of ***Chapter 2***).

- **Entertainment** – Entertainment, defined as the provision of food or drink (e.g. a meal) provided for consumption on the occasion and other entertainment connected with, or provided at the same time as such provision. For instance, a show provided at the venue where the meal is provided, is not an advantage under the POBO, while a ticket to a show/concert may constitute a gift or favour (i.e. an advantage) under the POBO.
- **Purpose of Bribery Being Not Carried Out** – The offeror and the recipient of a bribe will be guilty irrespective of whether or not the purpose of bribery has actually been carried out. It is not a defence for the recipient to claim that "the act requested to be done was not actually carried out" (Section 11 of the POBO). As in the above scenario, the offeror (i.e. the corporate customer) and the recipient (i.e. the bank manager) may commit an offence even if the latter does not actually have the power, right or opportunity to favour the former in the loan repayment extension process.
- **Principal's Permission** – It is lawful for an agent to accept an advantage in relation to his official duties with his principal's permission. The permission must be given by the recipient's principal, and **not** the recipient's supervisor or the offeror's principal. In case where an advantage has been accepted without prior permission, the agent must apply for his principal's approval as soon as possible afterwards.

Q2. In the course of handling credit facility application of a customer, who is a watch manufacturer, he offers an expensive watch as a gift to me for my assistance in favourably approving his application. According to the bank's policy, we cannot accept advantages from customers as an inducement to or reward for our doing or forbearing to do any act in relation to the bank's affairs or business. However, the customer claims that his offering is customary and a "normal" trade practice/culture. As it may also look impolite or even damage client relationship to decline the gift, should I accept it?

A Under the POBO, "advantage" includes "gift". Being an agent of the bank, you may contravene Section 9(1) of the POBO if you accept the gift **without the bank's permission** as a reward for doing an act in relation to the bank's affairs (e.g. handling credit facility applications). Your customer may also contravene Section 9(2) of the POBO under such circumstance. Besides, according to Section 19 of the POBO, it is **not** a defence to claim that an advantage accepted or offered is customary in any profession, trade, vocation or calling. As such, you should not accept the advantage offered, and politely explain to the customer the legal requirements and the bank's strict policy. Experience tells us that contrary to your worry, most customers would appreciate the professionalism of the staff and ethical culture of the bank.

For the actual provision of Section 19 of the POBO, please refer to the Hong Kong e-Legislation at *www.elegislation.gov.hk/hk/cap201*.

- If a bank allows its directors and staff to accept advantages (e.g. business gifts, "lai sees") from persons having business dealings with the bank under certain circumstances (e.g. during festive seasons), while such permission can be given on a case by case basis, it is advisable to also lay down the bank policy and rules/restrictions (e.g. subject to a limit of amount/value), such as in the bank's Code of Conduct (Reference at ***Section 2.3*** of ***Chapter 2***).

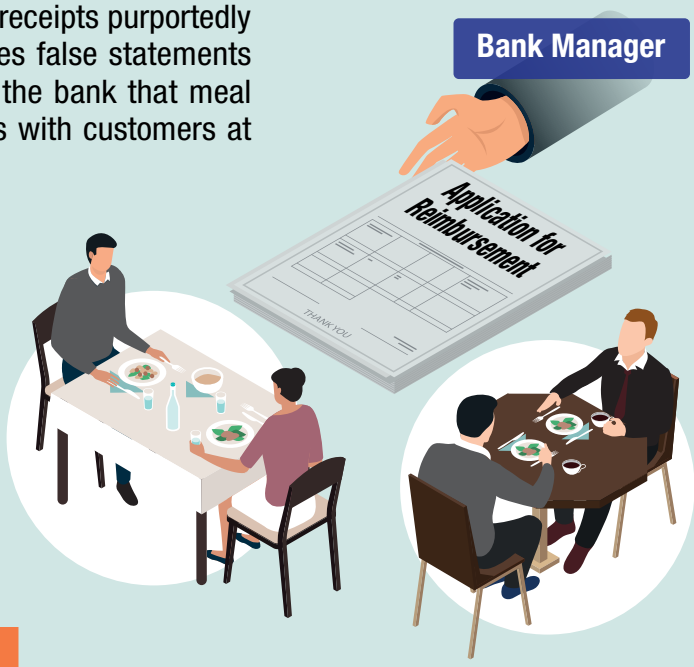
1.2.2 SECTION 9(3) – USE OF MISLEADING/FALSE/DEFECTIVE DOCUMENT TO DECEIVE PRINCIPAL

- **Section 9(3)** – It is an offence for any agent to, with an intent to deceive his principal, use any receipt, account or other document which contains any statement which is misleading, false or defective in any material particular in respect of which the principal is interested.
- The maximum penalty is a fine of $500,000 and seven years' imprisonment.

Case Study 2 – Using Falsified Receipts to Deceive Reimbursement

1 A bank manager working in a wealth management department is responsible for providing banking services to customers, and is entitled to apply for reimbursement of meal expenses incurred in meetings with customers. With intent to deceive the bank, the bank manager uses various receipts purportedly issued by different restaurants, and makes false statements on the expenses claim forms to mislead the bank that meal expenses have been incurred in meetings with customers at those restaurants.

2 The bank manager using documents with intent to deceive his principal, contravenes Section 9(3) of the POBO.



Analysis and Points to Note –

- **No Necessity for Offering and/or Acceptance of Advantage** – Section 9(3) of the POBO does not require the element of offering and/or acceptance of advantage. In general, if an agent under the POBO (e.g. a bank manager), with an intent to deceive his principal (i.e. the bank), uses any receipt, account or other document (e.g. expenses claim forms, attendance sheets) which contains any statement which is misleading, false or defective in any material particular in respect of which the principal is interested, an offence is committed under the section.

1.2.3 POBO PROVISIONS GOVERNING PUBLIC SERVANTS AND PERSONS HAVING DEALINGS WITH PUBLIC SERVANTS

- For persons employed by the Government or public bodies (e.g. Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC), Insurance Authority (IA), The Hong Kong Mortgage Corporation Limited (HKMC)) who are public servants, relevant provisions of the POBO, in particular Sections 4, 5 and 8, are relevant to them. The provisions prevent public servants from abusing official authority for private gain and safeguard the interests of public bodies and the wider community at large. In this regard, banks and their staff should be alert to avoid breaching these provisions in the course of undertaking any business dealings with the Government and public bodies (e.g. applying for banking licence issued by the HKMA).

- **Section 4(1)** – It is an offence for any person, in Hong Kong or elsewhere and without lawful authority or reasonable excuse, to offer any advantage to the public servant as an inducement to or reward for that public servant's performing or abstaining from performing any act in his capacity as a public servant.

- **Section 4(2)** – It is an offence for a public servant, in Hong Kong or elsewhere and without lawful authority or reasonable excuse, to solicit or accept any advantage as an inducement to or reward for his performing or abstaining from performing any act in his capacity as a public servant.

  The maximum penalty for the above offences is a fine of $500,000 and seven years' imprisonment.

- **Section 5(1)** – It is an offence for any person, without lawful authority or reasonable excuse, to offer any advantage to a public servant as an inducement to or reward for that public servant's giving assistance or using influence in regard to contracts with the public body concerned.

- **Section 5(2)** – It is an offence for any public servant, without lawful authority or reasonable excuse, to solicit or accept any advantage as an inducement to or reward for his giving assistance or using influence in regard to contracts with the public body concerned.

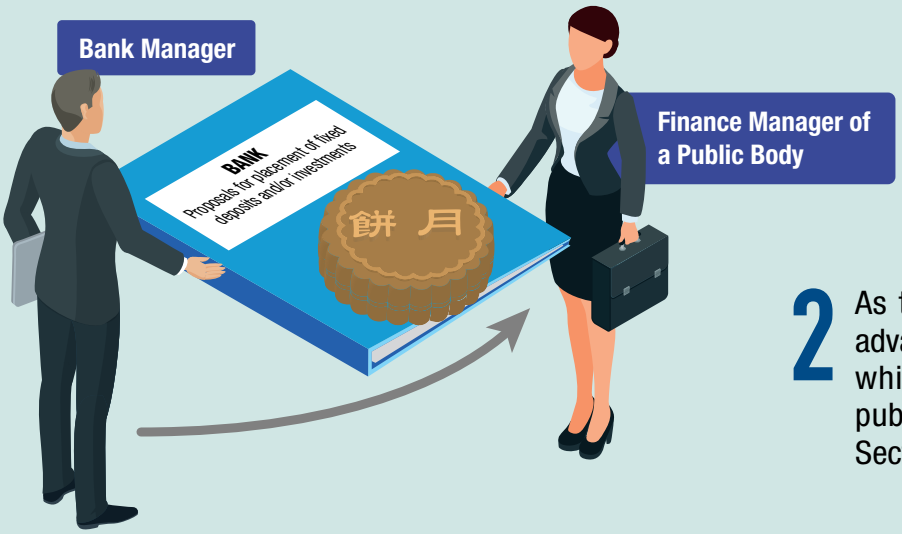
  The maximum penalty for the above offences is a fine of $500,000 and 10 years' imprisonment.

- **Section 8** – It is an offence for any person, without lawful authority or reasonable excuse, to offer any advantage to a public servant while having dealings of any kind with the government department or public body in which the public servant is employed.

  The maximum penalty for the above offence is a fine of $500,000 and seven years' imprisonment.

Case Study 3 – Offering Gifts to Public Servants while Having Business Dealings

1 A public body regularly places its surplus fund into bank deposits and/or investments. A finance manager of the public body (i.e. public servant) is responsible for inviting banks to submit quotations including proposals for placement of fixed deposits and/or investments. During a quotation exercise, a bank manager who has submitted proposals to the public body sends mooncake coupons to the finance manager as gifts during Mid-Autumn Festival.



2 As the bank manager offers the advantage to the finance manager while having dealings with the public body, he may contravene Section 8(2) of the POBO.

Analysis and Points to Note –

- **Need for Awareness** – Banks might have official dealings / business relationship with a government department/office or a public body. They should be aware that public servants are governed by relevant legal provisions or administrative rules on acceptance of advantages and entertainment. In particular, they should, as a general rule, without lawful authority or reasonable excuse, avoid offering gifts or other advantages to a public servant if they have any official dealings with the latter's government department or public body.

- **Committing Offence even without Bribery Intent** – As in the above case scenario, unlike bribery (e.g. Section 4 of the POBO as explained in ***Section 1.2.3*** above) which often involves a reciprocal performance of duties (or refrain from performance of duties) by a public servant being offered an advantage, Section 8 of the POBO does not require the proof that the advantage is offered in return for any favour. The offeror (i.e. the bank manager) under the above scenario still commits an offence even he has made no request for favourable treatment from the staff member (i.e. the finance manager) of the public body.

- **Relevant Corruption Prevention Guide** – To obtain a basic understanding of the relevant legal provisions and administrative rules / regulations governing the integrity of interaction between public servants and persons having business dealings with them, banks can make reference to the ***"Integrity and Corruption Prevention Guide on Managing Relationship with Public Servants"*** published by the ICAC which is available at the following webpage - *cpas.icac.hk/EN/Info/Lib_List?cate_id=3&id=226*.

1.3 OTHER MAJOR LEGAL CONCERNS

While the following ordinances/laws aim to govern the integrity and business practices of relevant operators including banks and their agents, offences under them are also often associated with corruption. Bank directors and staff should be aware of the risk exposure.

1.3.1 BANKING ORDINANCE (CAP. 155)

- This Ordinance, being the principal legislation to regulate the banking industry in Hong Kong, empowers the HKMA to, among other duties, supervise banks' compliance with the provisions of the Ordinance, covering promoting and encouraging proper standards of conduct amongst banks; suppressing illegal, dishonourable or improper practices in relation to banks' business practices; taking all reasonable steps to ensure that all banks are operated in a responsible, honest and business-like manner, and banking business undertaken by banks are carried on with integrity, prudence, professional competence, etc.
- It is an offence for any director or employee of a bank to ask for or accept advantages for his own personal benefit, or for that of his relatives, for showing favour to any person when approving loans or credit facilities from the bank. There is no defence of the bank having agreed to the acceptance of the advantages concerned (Section 124).
- It is an offence for any director or employee of a bank, with an intent to deceive, to wilfully make false entry of documentation in relation to the bank's business (Section 123).

1.3.2 SECURITIES AND FUTURES ORDINANCE (CAP. 571)

- Part XIII of the Ordinance prohibits insider dealing in relation to listed corporations and other market misconduct such as false trading, price rigging, market manipulation in securities or futures trading. As many banks provide wealth management services, the banks and their staff involved should be aware of the relevant provisions and restrictions when providing trading services to customers, and resist any corrupt offers or requests for information or undue favour that may breach these provisions.

1.3.3 THEFT ORDINANCE (CAP. 210)

- It is an offence for any person, by any deceit and with intent to defraud, to induce another person to commit an act or make an omission, which results in benefiting any person, or in prejudice or a substantial risk of prejudice to any person. For instance, any bank staff member, with intent to defraud the bank (e.g. submit false documents to deceive the bank for commissions) or a customer (e.g. defraud the customer to purchase additional services or pay extra handling fee), which results in benefit to him or prejudice to the bank/customer, may commit an offence under the Ordinance (Section 16A).

1.3.4 ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING ORDINANCE (CAP. 615) (AMLO)

- This Ordinance imposes requirements, among others, relating to customer due diligence and record-keeping on banks. It requires banks to take all reasonable measures to ensure that proper safeguards exist to prevent a contravention of any requirement under the Ordinance, and to mitigate money laundering and terrorist financing risks. The Ordinance also provides for the powers of the relevant authorities and regulatory bodies to supervise banks' compliance with those requirements. Besides, it is an offence for any person who is an employee of / employed to work for a bank with the intent to defraud the bank or any relevant authority, causes or permits the bank to contravene a specified provision in the AMLO. Given the more stringent customer due diligence requirements under the Ordinance, there are incentives for ineligible bank account applicants / corrupt parties to bribe bank staff for their assistance to circumvent the controls or requirements imposed by banks and regulators, the banks and their staff involved should be aware of the relevant corruption risks and turn down any corrupt offers or undue favour.

1.3.5 ORGANIZED AND SERIOUS CRIMES ORDINANCE (CAP. 455) (OSCO)

- It is an offence for any person who (i) deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of an indictable offence (Section 25), or (ii) fails to disclose such knowledge or suspicion to the authorised authority (Section 25A). As banks and their staff frequently assist customers to handle their funds (e.g. remittance), they should be aware of the relevant provisions, and resist any corrupt offers or undue requests (e.g. customer offers advantages to bank staff for their assistance to conceal the source of fund when using bank services and the bank staff do not disclose such knowledge or suspicion to the authorised authority).

1.3.6 PERSONAL DATA (PRIVACY) ORDINANCE (CAP. 486) (PDPO)

- This Ordinance protects privacy with respect to personal data. As banks collect and maintain large amount of personal data of customers which may have commercial value to other parties, bank staff may be tempted by corrupt parties to "sell" customer information to the latter for a bribe, breaching both this ordinance and the POBO at the same time. Banks should implement adequate safeguards on the personal data collected and raise staff's awareness on the restrictions in using personal data, which should help to reduce the risk of corruption in relation to abuse of customer data.

1.3.7 EXTRA-TERRITORIAL LEGAL OBLIGATIONS

- Banks having business operations outside Hong Kong should also observe the anti-corruption laws and regulations in the respective jurisdictions, in particular those anti-corruption legislations having extra-territorial effect and may be applicable to banks conducting business in Hong Kong and bribery committed in Hong Kong.
- For instance, the Criminal Law of the People's Republic of China prohibits the acceptance/offering of bribes by/to State functionaries[2] or State organs, State-owned companies, enterprises, institutions or people's organisations. Due to the increase in cross-boundary business activities, staff of banks in Hong Kong may need to travel to and carry out bank duties in the Mainland. They should therefore be aware of the anti-bribery provisions under the Criminal Law of the People's Republic of China[3,4].

[2] *State functionaries refer to persons who perform public service in State organs; persons who perform public service in State-owned companies, enterprises, institutions or people's organisations; persons who are assigned by State organs, -State-owned companies, enterprises or institutions to companies, enterprises or institutions that are not owned by the State or people's organisations to perform public service and the other persons who perform public service according to law.*

[3] *Regarding the Mainland legislation, please visit the following websites:*
Ministry of Commerce of the People's Republic of China: www.mofcom.gov.cn
Supreme People's Procuratorate of the People's Republic of China: www.spp.gov.cn

[4] *Readers may refer to "Business Success: Integrity & Legal Compliance Corruption Prevention Guide for SMEs in Guangdong, Hong Kong and Macao" published jointly by the ICAC and the Guangdong Provincial People's Procuratorate, the extract of which can be assessed on the following website: hkbedc.icac.hk/en/resources/practical_guides?page=1.*

1.4 REGULATORY AND PROFESSIONAL GUIDELINES/ REQUIREMENTS

Regulators and industry associations issue guidelines to banks from time to time to help ensure their prudent business practices. Banks, and their directors and staff should be aware of the relevant guidelines in carrying out the business. While banks should comply with the regulatory guidelines and requirements, they should also diligently remind their directors and staff to ensure their strict compliance.

1.4.1 HONG KONG MONETARY AUTHORITY

- The HKMA issues Supervisory Policy Manual (SPM)[5] setting out its latest supervisory policies and practices, the minimum standards banks are expected to attain in order to satisfy the requirements of the Banking Ordinance and recommendations on the best practices that banks should aim to achieve. The SPM covers various activities carried out by the banks in Hong Kong, including Code of Conduct (Reference at ***Section 2.3*** of ***Chapter 2***), Corporate Governance (Reference at ***Chapter 3***), and Guidelines on Anti-Money Laundering and Counter-Financing of Terrorism (Reference at ***Section 3.4*** of ***Chapter 3***).

1.4.2 THE HONG KONG ASSOCIATION OF BANKS (HKAB) AND THE DTC ASSOCIATION (DTCA)

- The HKAB and DTCA have also jointly issued the Code of Banking Practice[6] for their members in dealing with their daily operations with customers. It specifically covers banking services such as current accounts, savings and other deposit accounts, loans, overdrafts and card services. The HKAB has also developed a "Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism" to assist banks in understanding the relevant guidelines issued by the HKMA (Reference at ***Section 3.4*** of ***Chapter 3***).

[5] *Available on HKMA's website: www.hkma.gov.hk/eng/regulatory-resources/regulatory-guides/supervisory-policy-manual*

[6] *Available on HKAB's website: www.hkab.org.hk and DTCA's website: www.dtca.org.hk/cop.asp*

1.4.3 SECURITIES AND FUTURES COMMISSION

- The SFC has issued a Code of Conduct for Persons Licensed by or Registered with the SFC[7]. General principle "honesty and fairness" under this Code sets out the anti-bribery guidelines for a licensed or registered person and requires him to be familiar with the POBO. The SFC is also guided by this Code of Conduct when considering whether a licensed or registered person satisfies the requirement that he is fit and proper to remain licensed or registered.

1.4.4 INSURANCE AUTHORITY

- The Code of Conduct for Licensed Insurance Agents[8] issued by the IA sets out the fundamental principles of professional conduct which buyers of insurance are entitled to expect in their dealings with licensed insurance agents. The Code requires licensed insurance agent to be familiar with and not to contravene the POBO, and prohibit them from soliciting/accepting/offering an advantage without permission from the appointing insurer/agencies.

1.4.5 MANDATORY PROVIDENT FUND SCHEMES AUTHORITY

- The Conduct Guidelines[9] issued by the Mandatory Provident Fund (MPF) Schemes Authority provide guidance in respect of the minimum standards of conduct expected of regulated persons who engage in conducting sales and marketing activities and giving advice in relation to registered schemes. The Guidelines disallow MPF intermediaries from offering rebates, gifts, or advantage to any person when conducting regulated activities.

1.4.6 OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA (OPCPD)

- The Code of Practice on Consumer Credit Data[10] issued by the OPCPD provides guidance in respect of requirements under the PDPO imposed on data users in handling of consumer credit data (including banks). It deals with, among others, use and security issues relating to personal data of individuals who are or have been

[7] *Available on SFC's website: www.sfc.hk/en/Rules-and-standards/Codes-and-guidelines/Codes*

[8] *The "Code of Conduct for Licensed Insurance Agents" is available on IA's website: www.ia.org.hk/en/supervision/reg_ins_intermediaries/regulatory_instruments.html.*

[9] *It is named "Guidelines on Conduct Requirements for Registered Intermediaries" available on Mandatory Provident Fund Schemes Authority's website: www.mpfa.org.hk/en/info-centre/laws-and-regulations/guidelines#.*

[10] *Available on OPCPD's website: www.pcpd.org.hk/english/resources_centre/industry_specific/files/CCDCode_2013_e.pdf.*

applicants of consumer credit. It is applicable for credit providers (including banks) in their dealing with credit reference agencies and debt collection agencies. OPCPD has also issued the Guidance on the Proper Handling on Customers' Personal Data for the Banking Industry[11] which aims to assist banks in understanding and complying with the relevant requirements under the PDPO and promoting good practices in relation to customers' personal data.

1.4.7 HONG KONG EXCHANGES AND CLEARING LIMITED (HKEX)

- The Corporate Governance Code[12] of the HKEX's Listing Rules requires listed companies, on a comply or explain basis, to establish policies and systems that promote and support anti-corruption laws and regulations, and a whistleblowing policy and system for employees and those who deal with the companies to raise concerns. The Environmental, Social and Governance Reporting Guide[13] of the Listing Rules also requires listed companies to disclose on a comply or explain basis, anti-corruption information covering the companies' anti-corruption policies, compliance with relevant laws and regulations, concluded legal cases regarding corrupt practices, corruption prevention measures, whistleblowing procedures, and anti-corruption training provided to directors and staff, etc. Banks which are listed companies should comply with the relevant requirements.

[11] *Available on OPCPD's website: www.pcpd.org.hk/english/resources_centre/industry_specific/files/GN_banking_e.pdf*

[12] *Appendix 14 of Mainboard Listing Rules and Appendix 5 of the GEM Listing Rules.*

[13] *Appendix 27 of the Main Board Listing Rules and Appendix 20 of the GEM Listing Rules.*

2 STANDARDS OF BEHAVIOUR AND INTEGRITY MANAGEMENT

2.1 INTRODUCTION
2.2 FOSTERING A CLEAN BUSINESS CULTURE
2.3 ESSENTIAL PROBITY REQUIREMENTS IN A CODE OF CONDUCT
2.4 MAKING ETHICAL DECISION – ETHICS-PLUS DECISION MAKING MODEL

2 STANDARDS OF BEHAVIOUR AND INTEGRITY MANAGEMENT

2.1 INTRODUCTION

Apart from the compliance with law and regulatory/professional requirements, a clean business culture is essential in upholding the high integrity standard of bank personnel and building trust by customers in a bank. To foster a clean business culture, there should be a clear integrity commitment from the top, and the expected values, behaviour and integrity standards should be effectively communicated to its directors and staff, as well as other stakeholders. This Chapter highlights the steps to foster a clean business culture, and provides the essential probity elements in a Code of Conduct that are fundamental in building a clean business culture in the bank, and safeguarding directors and staff against pitfalls of corruption and other malpractice. An ethical decision-making model is also included for reference by bank directors and staff.

2.2 FOSTERING A CLEAN BUSINESS CULTURE

Culture defines values and desirable behaviour within an organisation. In March 2017, the HKMA initiated a Bank Culture Reform[14] through promoting the adoption of a holistic and effective framework for fostering a sound culture within banks through three pillars, namely governance, incentive systems, and assessment and feedback mechanism. The HKMA has also issued corporate governance guidelines set out in the SPM (Reference at ***Section 1.4.1*** of ***Chapter 1***) which requires the Board, among others, to ensure that a culture of competence and ethical behaviour is embedded within a bank at both the institution and individual staff levels[15]. To foster a clean business culture within a bank, the essential elements are highlighted as below –

[14] *Regarding the Bank Culture Reform, please visit HKMA's website: www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20170302e2.pdf.*

[15] *SPM module "Competence and Ethical Behaviour" (CG-6) provides guidance on measures banks are expected to adopt in monitoring and maintaining the competence levels and ethical behavior of their staff.*

- Develop ***ethical leadership***, i.e. top-level commitment to integrity, with leaders being role models in anti-corruption business practices.
  - The Board should play a leading role in establishing and fostering the bank's clean business culture, values and behavioural standards that promote integrity and anti-corruption. Senior management should put in place effective mechanisms for ensuring that the bank's clean business culture is understood and shared by all levels of staff.
- Promote ***clean business culture in the bank*** by –
  - issuing a ***Code of Conduct (the Code)*** (a sample is at ***Appendix 1***), endorsed by the Board to all directors and staff setting out the probity standards and requirements; updating the relevant probity guidelines periodically and circulating them (e.g. via intranet) regularly or before major festivals to remind directors and staff rules relating to acceptance of advantages (e.g. "lai sees") from persons having business dealings with the bank;
  - ensuring that directors and staff have adequate understanding and knowledge on the anti-bribery law, integrity management issues, corruption prevention controls, etc. (Reference at ***Section 3.3.6*** of ***Chapter 3***);
  - making ***transparent*** the Code (e.g. via intranet) to demonstrate commitment to directors, staff, business partners and customers; and
  - providing an ***ethics hotline*** for enquiries on and reporting of integrity issues (Reference at ***Section 3.3.8*** of ***Chapter 3***).
- Commit ***business partners to clean business practices*** – Business partners (e.g. fund managers, insurance companies, debt collection agencies, suppliers and contractors) may be exposed to risks of corruption committed by their staff, such as soliciting/accepting bribes from customers or others when acting on the bank's behalf or providing services to the bank, or offering advantages to the bank's personnel to secure business, etc. It is recommended that a bank commits its business partners to clean business practices by informing them of its anti-corruption policy. As far as practicable, for major contracts and partnering arrangements, the bank should include suitable anti-corruption and probity requirements in the agreements with the business partners, which should at least include the following –
  - prohibition against bribing the bank's directors and staff or offering advantages to them without the bank's permission;
  - prohibition against bribery of any form in carrying out business under the contract/ partnership or on behalf of the bank;
  - the need to ensure that all the relevant personnel of the contractor are made aware of the anti-corruption requirements, such as through a Code, probity guidelines and training; and

- the right for the bank to terminate the contract with the business partner if it or its director or staff member has breached the anti-corruption requirements.

- Enhance ***transparency of policies to external parties*** – Alert customers and engage business partners through making transparent (e.g. bank website, posters or signs in branches/offices, messages on printed letters or e-newsletters) the bank policies and procedures on conduct requirements, such as not to offer any advantages/gifts to bank staff.

- Designate an ***Integrity Officer*** or a ***department/division*** for coordinating the implementation of the above policies and practices, and conducting periodic monitoring and reviews to ensure effective sustainability and compliance.

2.3 ESSENTIAL PROBITY REQUIREMENTS IN A CODE OF CONDUCT

The expected standards of behaviour of banks, and their directors and staff are set out in the modules "Corporate Governance of Locally Incorporated Authorized Institutions" and "Code of Conduct" in the SPM issued by the HKMA (Reference at ***Section 1.4.1*** of ***Chapter 1***). The SPM has set out the minimum standards which the HKMA expects banks to adopt, covering the ethical and professional standards of the Board and requiring banks to develop its own Code of Conduct to set out the standards of behaviour expected of its staff. Apart from the standards of behaviour set by the HKMA, a bank may refer to the Sample Code at ***Appendix 1*** which contains a comprehensive list of probity provisions. The following are those necessary requirements which the Code should cover –

2.3.1 COMPANY STATEMENT

- To provide a clear direction to all stakeholders, the Code should spell out the bank's firm commitment to clean business practices and prohibition against any bribery and corrupt practices in carrying out the bank's business.

2.3.2 PROHIBITION OF BRIBERY

- The Code should clearly prohibit all forms of bribery or corruption and require compliance with the POBO (and anti-bribery laws applicable to the bank) in carrying out business for the bank. Directors and staff should be prohibited from –

  - soliciting or accepting any advantage from others as a reward for or inducement to doing any act in relation to the bank's business;

  - offering any advantage to an agent of another as a reward for or inducement to doing any act in relation to the latter's principal's business; and

- offering any advantage to any government officer or public servant as a reward for or inducement to performing any act in his official capacity, or while having business dealings with the government or public body he belongs to.

Q3. I am a Branch Manager. My team has received customer requests of providing special assistance in account opening, such as expediting the application due to urgent needs, waiving the submission of some documents, which is within the staff's authority and can be provided for good customer service. Those customers may offer the staff responsible a gift for the special assistance rendered. If we provide such "special assistance" as part of customer service without deviating from any bank policies, is the acceptance of the gifts still regarded as bribery?

A **Under the POBO, "advantage" includes "gift".** The bank staff may contravene Section 9(1) of the POBO if he, being an agent of the bank, accepts the gift as a reward for doing something **in relation to the bank's affairs** (which may include any service or assistance in the account opening process, whether that involves special favour or deviation or not), without the bank's permission. The customer may also contravene Section 9(2) of the POBO if he offers an advantage under the same circumstance. As a prudent approach, your staff should decline and discourage offers of advantage of any kind by customers regardless of intention, and immediately report to supervisors or the ICAC if there is any corrupt intent.

In this regard, the bank should issue clear policy (e.g. Code of Conduct) on acceptance and prohibition of solicitation of advantages from persons having business dealings with the bank; where acceptance (but not solicitation) of advantages/gifts under certain circumstances without risk of corrupt intent is considered allowable in view of general business practices, specify the circumstances where acceptance of advantage/gift may be allowed, including the restrictions (e.g. types and allowable limit of value of the gift, types of and relationship with the offeror, types of occasions), the allowable disposal methods, the approving authority for cases not covered by blanket approval (if any), and the procedures, and implement the policy effectively to ensure staff's compliance (Reference at ***Section 2.3.3***).

Q4. I am a Division Head. My division manages investment accounts for customers. A customer who has made a handsome profit would like to reward me with a "lai see" of $50,000 as he believes that it would continuously bring luck to him. Since I have not given any special favour to him during the course of handling his investment account, and to maintain good client relationship, is it proper for me to accept the "lai see"?

A You may refer to answer of Q3 above for reference.

2.3.3 ACCEPTANCE AND OFFER OF ADVANTAGES

- In addition to prohibiting the acceptance/offer of advantages for a corrupt purpose, to maintain a good standard of integrity among the bank's personnel and protect them and the bank from perception or allegation of impropriety, the Code should –

Acceptance and Solicitation of Advantages

- prohibit directors and staff from soliciting or accepting advantages from persons having business dealing/relationship with the bank (e.g. suppliers, customers), except accepting certain advantages within specified permissible natures, values and under specified circumstances or occasions with no improper influence is involved;
- where acceptance of gifts/advantages may be allowed, set out the circumstances/ occasions (e.g. during festive seasons where business gifts are traditionally exchanged) and restrictions for acceptance of advantages (e.g. allowable limit of value of the gift, cash not allowed, acceptance of gifts from suppliers/contractors prohibited), and the channel for special approval in exceptional cases;
- prohibit supervisors from soliciting advantages from subordinates, and only allow acceptance of advantages from subordinates under specified circumstances (e.g. wedding) or occasions with no improper influence involved;
- remind directors and staff to actively discourage personnel having business dealings/ relationship with the bank (e.g. business partners, suppliers, customers) from offering advantages of any kind;

Offer of Advantages

- remind directors and staff to offer gifts to the corporate instead of to individual staff;
- remind directors and staff to ascertain the intended recipient is permitted by his employer/principal to accept the advantage under the relevant circumstances before the advantage is offered; and

Referral of Business

- remind directors and staff on the policy for referral of customers to any other banks or companies.
    - In particular, directors and staff should be prohibited from soliciting or accepting advantages (e.g. referral fee) for referring a customer to any other banks or companies without the prior approval of the bank as this might constitute an offence under the POBO. Even the referral might not involve an advantage, they should be made aware that such referrals without proper declaration and prior approval of the bank as required might also constitute a conflict of interest or misuse of their official position.

Q5. I am a Department Head. During festive seasons, my staff would like to offer gifts (e.g. hamper/mooncake) to the staff or agents acting on behalf of our private sector business partners. What are the areas of concerns when making such offers?

A The bank should ensure that its staff understand and comply with Section 9 of the POBO (Reference at ***Section 1.2*** of ***Chapter 1***), and the bank's policy to avoid them from falling prey to corruption. When offering advantages (e.g. gifts) to staff or agents of a business partner in the private sector through your staff who deal with that business partner, the staff should reasonably ascertain with the intended recipients that they have the permission of the business partner (i.e. principal under the POBO of the recipients) to accept the advantages.

In this regard, the bank should issue clear policy (e.g. in the Code of Conduct) on offering of advantages to persons having business dealings with the bank, reminding them of the legal requirements, specifying the circumstances for offering advantages and the steps to be taken to ensure compliance.

Q6. A regulator which is a government department / public body has recently conducted an inspection on my bank's operations and provided useful recommendations to our bank for improvement. Following a business practice and courtesy for private sector business partners/customers, can I offer festive gifts (e.g. hamper/mooncake) to the inspection team of the regulator to appreciate their efforts?

A The answer is a strict "No". The laws governing the public sector are more stringent in this regard. Directors and staff should strictly be prohibited from offering any advantage to public servants (e.g. employees of regulators) having business dealings with the bank. According to Section 8 of the POBO (Reference at ***Section 1.2*** of ***Chapter 1***), it is an offence for any person to offer advantage to a public servant while having dealings of any kind with the government department or public body in which he is employed. Therefore, directors and staff of the bank should be prohibited from offering any advantage (e.g. gift) to public servants (e.g. inspection team of the regulator) who have business dealings with the bank. Banks should ensure that their directors and staff understand the POBO and comply with the bank's policy to avoid falling prey to corruption.

In this regard, the bank should issue clear policy (e.g. in the Code of Conduct) to prohibit staff from offering of advantages to public servants having business dealings with the bank including the relevant laws, and implement the policy effectively to ensure staff's compliance.

2.3.4 ACCEPTANCE OF ENTERTAINMENT

- Entertainment (Reference at ***Section 1.2*** of ***Chapter 1***) is an acceptable social activity, but extravagant or frequent entertainment offered to the directors or staff from companies having business dealings may have or be seen to have a sweetening effect which may lead to corrupt behaviour in future. The Code should include guidelines on entertainment, advising them to avoid accepting/offering entertainment that may be regarded as –

  - ***excessive*** – taking into account its value, substance, frequency and nature;
  - ***inappropriate*** – taking into account the relationship between the director/staff and the offeror; or
  - ***undesirable*** – taking into account the character or reputation of the host or other attendees,

  and may require them to report or seek approval for acceptance of such entertainment.

2.3.5 CONFLICT OF INTEREST

Definition of Conflict of Interest

- A conflict of interest situation arises when the "private interests" of a director or staff member compete or conflict with the interests of the bank or the director's or staff's official duties. Private interests include financial and other interests of the director / staff member himself, and those of his connections including family and other relations, personal friends, the clubs and societies to which he belongs, any other groups of people with whom he has personal or social ties, and any person to whom he owes a favour or to whom he may be obligated in any way. Some common examples of conflict of interest are provided at ***Appendix 2***.

Mechanism to Manage Conflict of Interest

- To help directors and staff properly manage possible conflict of interest, the Code should set out ***guidelines on managing conflict of interest***. The following "three-step mechanism" should be adopted –

  - ***Avoid*** – All directors and staff should remain alert to and avoid any actual, potential or perceived conflict of interest situation.
  - ***Declare*** – If the conflict is unavoidable, the directors and staff should report it to the designated approving authority once he becomes aware of the conflict.

- ***Mitigate*** – The designated approving authority, after assessing the impact of the conflict and the risk of impropriety, should take appropriate mitigating measure as early as possible.

- The mitigating measure to be taken would depend on the circumstances of individual cases and the level of mitigation should be commensurate with the severity of the conflict, the interest involved and other's perception. Related mitigating measures are provided at ***Appendix 3***.

- Proper documentation of the declaration, the rationale for the decisions made and the course of mitigating measure taken should be maintained. A ***sample form*** for making the declaration, recording the decision made and the mitigating measure taken is at ***Annex 3*** of ***Appendix 1*** for reference.

- It would be helpful to designate an office / a staff member of appropriate rank to keep the precedent cases in managing declared conflict of interest so as to enhance consistency and facilitate sound decisions in managing declared conflict of interest in future.

- Require staff members newly joining the bank / taking up new roles / upon encountering a conflict of interest situation to make a declaration on whether there are any conflicts of interest between their personal interests and their job duties.

Positive Declaration

- Depending on the operational needs and circumstances, the bank may require a director or staff member who participates in projects/exercises involving sensitive issues/ information, or with great public concerns to declare if they have or do not have any conflict of interest (i.e. positive declaration) on the matter in order to protect the public interest and the interest of the bank.

Q7. I am a Vice President of the private banking department of a bank. Throughout the years, I have developed close relationship with my customers owing to my good services and professional investment advice provided to the customers. In view of our close relationship, one of my customers, a property investor, invites me to invest in his project in the property market. Would I breach the POBO or what are the areas of concern?

A First of all, having financial dealings (e.g. joint investment) with customers may constitute a conflict of interest with the staff's duty at the bank, which should be avoided. If it is unavoidable, the bank staff must duly declare such relationship and dealings to the bank of which the management should duly examine the circumstance of the case, seriousness of conflict and public perception, etc. and take appropriate measures to mitigate the risks. As a general rule, banks should normally prohibit their staff from entering into financial dealings with the customers under their charge to avoid any actual, potential or perceived conflict of interest. You should follow the bank's requirements in this regard if available and seek the appropriate authority's (e.g. the bank's ethics hotline or bank's integrity officer) advice as appropriate.

Secondly, the staff should be reminded that any investment profits and/or income arising from the joint investment may constitute an advantage as prescribed under the POBO if he colludes with the customer who offers an advantage, to be concealed in the form of investment profits and/or income, to him as a reward for assisting or favouring in banking matters. The staff and customer may respectively contravene an offence under Sections 9(1) and 9(2) of the POBO.

In this regard, the bank should issue clear policy (e.g. in the Code of Conduct) on avoidance and declaration of conflict of interest arisen at work scenarios covering the common examples such as staff's private dealings with customers, and implement the policy effectively to ensure staff's compliance.

Q8. I work at the credit department and it has come to my knowledge that my spouse's company has submitted a corporate loan application to the bank that I work for. What are the areas of concern?

A The spouse relationship together with the corporate loan application constitutes a conflict of interest with your duties at the bank, which you should avoid. If it is unavoidable, you must duly declare such relationship to the bank of which the management should duly look into the circumstance of the case, seriousness of conflict and public perception, etc. and take appropriate measures (e.g. refrain you from getting involved in approving such loan application) to mitigate the risks. You should follow the bank's requirements in this regard if available and seek the appropriate authority's (e.g. the bank's ethics hotline) advice as appropriate.

In this regard, the bank should issue clear policy (e.g. in the Code of Conduct) on management of conflict of interest declared by staff, and implement the policy effectively to ensure staff's compliance.

2.3.6 MISUSE OF OFFICIAL POSITION

- The Code should prohibit directors and staff from misusing their official position to pursue their own private interests, which include both financial and personal interests and those of their family members, relatives or close personal friends, etc.

2.3.7 SAFEGUARD OF CUSTOMERS' FUNDS AND INTERESTS

- In the course of their duties, directors and staff are entrusted by customers to handle huge amount of funds. To safeguard customers' interests and prevent corrupt practices connected with the mishandling of customers' funds, the Code should require those having access to customers' funds to make sure customers' funds are handled in a trustworthy and honest manner.

2.3.8 HANDLING OF RECORDS, ACCOUNTS AND OTHER RESTRICTED INFORMATION

- The Code should remind directors and staff to ensure that all records, receipts, accounts, etc. they submit to the bank give a true representation of the facts, events or business transactions as shown in the documents.
- The Code should remind directors and staff to safeguard, and not to disclose to others without proper authority, any restricted information (e.g. information about the bank, markets, details of business/transaction of customers, and personal data of customers), in particular prohibit unauthorised disclosure of information that might be of use to other banks, business operators or companies in competition with the bank's business.

2.3.9 PERSONAL INVESTMENTS

- The Code should prohibit directors and staff to deal in the shares or other securities of any listed companies when possessing privileged or price-sensitive information that is not generally known to other investors and to the public. Directors and staff should not disclose such information to any third party.
- The Code should require directors and staff to notify/declare to the bank immediately in writing of the details of any dealings in which they may have been inadvertently concerned in the shares or other securities of any listed companies of which they possess privileged or price-sensitive information. The bank should designate an appropriate authority to consider and manage such notification/declaration, and manage potential/actual conflict of interest identified or take action as appropriate (Reference at ***Section 2.3.5***).

2.3.10 OUTSIDE EMPLOYMENT/WORK

- The Code should remind bank directors and staff to avoid engaging in outside or part-time jobs/work which may give rise to conflict of interest (e.g. undertaking part-time employment with a supplier engaged by the bank, providing private services to customers under their own portfolio beyond the bank's assigned duty), and –
  - require all directors and staff to seek prior approval of the designated authority before taking up any outside employment/work;
  - remind the approving authority to consider whether the outside employment/work would give rise to a conflict with the staff member's duties in the bank or the interest of the bank, and where approved, specify any conditions and reminder to avoid conflict of interest in performing such outside employment/work; and
  - remind directors and staff to avoid conflict of interest in carrying out approved outside employment/work and update and seek further direction from the approving authority should he/she encounters actual conflict of interest.

2.3.11 REPORTING OF VIOLATIONS, SUSPECTED CORRUPTION AND OTHER CRIMINAL OFFENCES

- The Code should clearly state the bank's policy on handling reports of breach of the Code, misconduct and criminal offences including corruption.
- The Code should encourage directors and staff to report instances of crime or suspected crime including corruption discovered in the course of their work to the appropriate authority of the bank or regulators / law enforcement agencies at the first practicable opportunity. In this regard, the bank may consider issuing a separate whistleblowing policy (Reference at ***Section 3.3.8*** of ***Chapter 3***) to give clear guidance on handling of reporting of violations.

2.3.12 COMPLIANCE WITH LAWS AND OTHER PROFESSIONAL STANDARDS AND REGULATORY REQUIREMENTS

- The Code should require directors and staff to comply with all local laws and regulations when conducting the bank's business, and also those in other jurisdictions when conducting business there or where applicable.

- There are a number of professional requirements and standards on conducting banking business issued by the Government and relevant regulators (e.g. HKMA, SFC) (Reference at ***Section 1.4*** of ***Chapter 1***). To ensure compliance with regulatory requirements and professionalism, the Code should require directors and staff to observe the professional and regulatory requirements as imposed on them, as appropriate.
- The Code should encourage directors and staff, save for certain regulatory exceptions, to co-operate with government, regulatory or internal investigation including provision of materials requested by those conducting the investigation in a timely manner.

2.3.13 COMPLIANCE WITH CODE OF CONDUCT

- The bank should remind directors and staff, whether performing their duties of the bank in or outside Hong Kong, to comply with the Code. In particular, managers and supervisors should be reminded to ensure that the staff under their supervision understand well and comply with the Code.
- The Code should state the consequence of breaching the Code, which may include disciplinary actions including termination of appointment and that in cases of criminal acts, the bank will also promptly make a report to the relevant regulators and/or law enforcement agencies.

2.4 MAKING ETHICAL DECISION – ETHICS-PLUS DECISION MAKING MODEL

The rapid growth of technologies, proliferation of financial products and convergence of markets have brought new legal and ethical challenges to the banking industry. Banking staff, in particular those with management responsibilities, have to exercise caution and sound judgement when handling ethical challenges at work.

The ethics plus Decision Making Model at ***Appendix 4*** provides a step-by-step guidance to help bank management staff stranded in ethical crossroads to resolve ethical dilemmas at work.

3 GOVERNANCE AND ANTI-CORRUPTION CONTROL

3.1 INTRODUCTION

3.2 RESPECTIVE ROLES IN IMPLEMENTING ANTI-CORRUPTION POLICY AND CONTROLS

3.3 KEY ELEMENTS OF ANTI-CORRUPTION CONTROL

3.4 CONTROLS AGAINST MONEY LAUNDERING

3 GOVERNANCE AND ANTI-CORRUPTION CONTROL

3.1 INTRODUCTION

Establishment of a strong corporate governance with robust internal control mechanism is recognised as an effective anti-corruption tool and a key internal measure to address corruption, fraud, money laundering and other malpractices. While corporate governance sets a bank's values and standards and requirements, internal controls are the policies and procedures adopted to ensure compliance with them. The HKMA has issued the SPM (Reference at ***Section 1.4.1*** of ***Chapter 1***) which sets out the minimum standard of corporate governance expected of banks incorporated in Hong Kong[16], and the key elements of a bank's internal control system which the HKMA expects the banks to have in place[17]. It is imperative for the Board and senior management to demonstrate strong and visible commitment to anti-corruption business practices. All personnel in a bank should have their respective roles to play in helping the bank to adopt anti-corruption policy and controls. This Chapter covers –

(a) the roles and responsibilities of respective personnel within the governance structure of a bank in enhancing/implementing the bank's anti-corruption policy/controls;

(b) the key elements of anti-corruption control; and

(c) the specific corruption risks in connection with money laundering and corresponding controls required, in addition to the above.

[16] *SPM module "Corporate Governance of Locally Incorporated Authorized Institutions" (CG-1), among others, is a statutory guideline issued by the HKMA under the Banking Ordinance. Failure to adhere to the standards set out in this module may call into question whether a bank continues to satisfy the minimum criteria for authorization under the Banking Ordinance and may cast doubt on the fitness and propriety of individual directors and shareholder controllers of the bank.*

[17] *SPM module "Risk Management Framework" (IC-1), among others, specifies key elements of a sound internal control system, covering clear delegation of authority, written policies and procedures, separation of critical functions, internal audit function, etc.*

3.2 RESPECTIVE ROLES IN IMPLEMENTING ANTI-CORRUPTION POLICY AND CONTROLS

The responsibilities of respective parties within the governance structure of a bank and their roles in enhancing/implementing the bank's anti-corruption policy/controls as recommended by the Corruption Prevention Department (CPD) are set out below. Please note that the recommended practices below are by no means exhaustive and that individual banks may consider adopting them, among others, taking into account their governance structure, operational scale and needs, etc. while adhering to the principles of the recommended measures.

3.2.1 THE BOARD

- The Board and its directors should lead to demonstrate its visible and strong commitment to anti-corruption business objectives and strategies, and oversee to ensure that an effective anti-corruption policy is established, maintained, consistently followed and regularly reviewed.

3.2.2 COMMITTEES

- To enhance effective implementation of the anti-corruption policy/controls, the Board could delegate/designate a relevant committee such as audit committee, risk committee covering anti-money laundering issues with suitable knowledge and expertise to ensure accountability and effective oversight of the implementation of the anti-corruption policy/controls, taking into account the organisational structure of individual banks.

3.2.3 INDEPENDENT NON-EXECUTIVE DIRECTORS (INEDS)

- In view of the important role of INEDs in advising the Board on, among others, clean business practices and measures including compliance with anti-corruption laws and best practices, the Board should explicitly require INEDs as independent third parties to actively assist it in monitoring the effective implementation of the bank's anti-corruption policy/controls and in reporting promptly any discrepancies or irregularities detected.

3.2.4 SENIOR MANAGEMENT

- Senior management carries out the day-to-day operations and implements systems and controls in accordance with the business strategies, risk appetite and policies approved by the Board. They are responsible for designing, formulating and reviewing the anti-corruption controls/measures in the bank and ensuring that adequate resources and expertise are in place for the effective implementation.

3.2.5 MANAGERS UNDERTAKING KEY CONTROL FUNCTIONS

- With regard to the appointment of persons undertaking key control functions (e.g. internal audit, compliance) who fall within the definition of "manager" in the Banking Ordinance[18], the SPM[19] stipulates the systems of control (e.g. clearly defined the responsibilities, level of authority) on appointing them. Given the unique nature of control functions and their inherent oversight duties in support of the Board, bank managers of such key control functions should undertake specific internal control measures under their respective work mandates, with a view to preventing and detecting corruption, fraud and other malpractices.

3.2.6 STAFF IN GENERAL

- Resisting corruption and helping the bank uphold anti-corruption business practices are the responsibilities of staff at all levels. They are crucial to the effective implementation of corporate governance in the bank. They should familiarise themselves with the requirements of the anti-bribery laws (i.e. the POBO) in Hong Kong (Reference at ***Section 1.2*** of ***Chapter 1***), have a good understanding of the corruption risks in their working environment and the proper controls/measures they should adopt. They should also be alert of the requirement to promptly bring to the attention of the management or appropriate reporting channels of any corruption or practices conducive to corruption.

[18] *Under Section 2 of the Banking Ordinance, a "manager" of a bank means any individual appointed by a bank, to be principally responsible for the conduct of any affairs or business specified in the Fourteenth Schedule to the Ordinance, which includes carrying on of retail banking business, maintenance of systems of control of a bank, conduct of internal audits, compliance function, among others.*

[19] *SPM module "Systems of Control for the Appointment of Managers" (CG-2) specifies the system of control that a bank should have for ensuring the fitness and propriety of individuals appointed as managers.*

Q9. Are anti-corruption controls/programmes important to a bank?

A Corruption, fraud and other malpractice erode profits, damage the bank's reputation and jeopardise the business in the long run. For listed companies, the HKEX requires them to disclose, on a "comply or explain" basis, their anti-corruption policies and preventive measures against corruption (Reference at ***Section 1.4.7*** of ***Chapter 1***). Irrespective of whether a bank is a listed company, large or small, it should nevertheless instigate anti-corruption programme as early as possible in order to detect and deter corruption, taking into account the requirements of all applicable laws, in particular the POBO. An effective anti-corruption programme should include the following essential elements –

- an anti-corruption policy;
- probity standard and anti-corruption guidance for all bank personnel, including directors and staff, through a Code of Conduct;
- a mechanism for the identification and assessment of corruption risk;
- anti-corruption controls; and
- training and communication.

The Corruption Prevention Advisory Service (CPAS) of the ICAC (Reference at ***Chapter 8***) has developed a separate Corruption Prevention Guide which aims at helping listed companies effectively implement corporate anti-corruption programmes, covering anti-corruption policy, corruption risk identification and assessment, anti-corruption control, etc. For further reference of this guide, please visit *cpas.icac.hk/EN/Info/Lib_List?cate_id=3&id=2330*.

3.3 KEY ELEMENTS OF ANTI-CORRUPTION CONTROL

Effective anti-corruption control is imperative for an organisation as it provides the framework for plugging the corruption loopholes from the outset. Below highlights the key elements of such control including guidance on corruption risk assessment and management for the purpose of corruption prevention. The good safeguards as recommended in the Chapters hereafter specifically to address the risks for respective core banking operations have been made reference to the below key elements.

3.3.1 CLEAR POLICIES, WORK PROCEDURES AND GUIDELINES

- Lay down clear policies and guidelines for the bank's various business processes such as handling of customers and their accounts and information, credit approval, and anti-money laundering measures for staff compliance and implementation. Appropriate control measures including segregation of duties, approving authorities, documentation, supervisory checks and monitoring, and computerised processes should be built into the policies, procedures and guidelines.
- Stipulate procedures and guidelines for internal operations including financial control and reporting, compliance, risk management, procurement as well as human resources functions (e.g. remuneration[20] and performance measurement/monitoring).
- Where committees are established, clearly define their mandates and authority, and ensure that there are appropriate independence and objectivity in carrying out their functions.
- Stipulate the roles and responsibilities of each level of staff or post and the authorities for making decisions in various functions, with clear lines of reporting with requirements of accountability.

3.3.2 CORRUPTION RISK ASSESSMENT AND MANAGEMENT

- Include corruption risks as an integral part of the bank's risk management system and be accorded an equally high priority as other business/operational risks, and establish mechanisms to prevent and control the corruption risks with continuous monitoring/review.
- Recognise the serious damage of corruption to the bank when devising the risk management policy, and hence adopt the lowest level of acceptance for corruption risks that the bank is willing and able to take.
- There should be a designated team of suitable staff (which could be within the internal audit function or dedicated anti-corruption/anti-financial crime unit) to perform the corruption risk management function. The team should have direct reporting line to the Board and/or the risk committee to ensure its independent assessment and their role should be distinct from other executive functions to avoid conflict of interest in carrying out the functions.
- Ensure that the risk assessment and management framework is able to help identify business operations, processes and practices that are conducive to corruption or weakness that give rise to corruption risks, and put in place anti-corruption measures to prevent and control the risks identified with continuous monitoring/review.

[20] *SPM module "Guideline on a Sound Remuneration System" (CG-5) provides guidance to ensure that banks' remuneration systems are consistent with and promote effective risk management, and contribute toward acceptable staff behaviour.*

3.3.3 CHECKS AND BALANCES

- Implement segregation of duties in critical functions such as customer handling / relationship management, credit approval/verification and compliance with statutory law, rules and regulations. For example, in order to safeguard independence, staff responsible for the audit function should not involve in the daily operations. Staff who are holding credit approval authorities should not perform client-facing roles.
- Institute policies and procedures such as cross-checking of documents, dual control of assets, and conduct of random risk-based and independent checks (e.g. check the CCTV/audio recording) to deter and detect possible malpractice.
- Conduct random/surprise checks with customers to detect any irregularities, for instance, making post-application / post-sales calls to customers on a risk basis (e.g. vulnerable group) to verify some essential information of the banking process (e.g. source of business, terms and conditions of the service applied, fees, whether purchase of investment/insurance product is a pre-requisite for opening a bank account) by an independent team/staff and taking appropriate follow-up action(s) for suspicious case(s).
- Put in place staff administration measures such as reference checks[21] on prospective employees in particular the senior staff, job/duty rotation (e.g. allocate credit assessment cases to staff by rotation), compulsory uninterrupted annual leave arrangements and assignment of a second/backup officer where practicable for functions with risks of corruption or malpractice.

3.3.4 RECORD KEEPING AND INFORMATION SECURITY

- Put in place a record keeping system and require staff to keep proper record of business transactions such as customers' instructions, and staff members involved in processing, validating, and authorising, in written and/or digital/electronic form for future audits and deterrence of malpractice. Document decisions/actions for important or exceptional cases with justifications to ensure that all personnel involved are accountable for their decision/actions.
- Lay down the policies and rules on classification and handling of information (e.g. limit access to restricted/commercially sensitive information to authorised staff only on a need-to-know basis and require them to protect the information from leakage).

[21] *To address the "rolling bad apples" phenomenon in the banking sector in Hong Kong i.e. situations where individuals who engage in misconduct during their employment in one institution are able to obtain subsequent employment in another institution without disclosing their misconduct to the new employer, the HKMA endorses the Mandatory Reference Checking Scheme which requires authorized institutions to obtain reference information during their recruitment process for certain positions and provide the same upon request of another institution. The first stage of the Scheme will cover senior staff such as directors, chief executives and managers as defined under the Banking Ordinance, as well as executive officers and responsible officers for securities, insurance and MPF regulated activities.*

- Implement security safeguards to protect both hardcopy and record/data in the computer system from tampering or destruction (e.g. audit trail function with generation of management reports for identification of and following up on abnormalities).
- Remind staff that unauthorised disclosure of or tampering with records could constitute a breach of the bank's rules or even a criminal offence, and disclosure in return for advantages may amount to bribery.

3.3.5 SUPERVISORY MONITORING AND ACCOUNTABILITY

- Require supervisors to remain vigilant at all times to potential risk of corruption or other malpractice.
- Provide relevant information (e.g. financial statements, budgets, market statistics and legislation) to enable supervisors to fulfil their responsibilities effectively.
- Require supervisors to implement measures to deter or detect malpractice (e.g. conduct routine and/or risk-based spot checks on operations and transactions, use an information management system which can generate management reports to facilitate monitoring of important operations), and make thorough enquiries into suspected irregularities and/or report to appropriate authorities.

3.3.6 TRAINING

- Ensure that bank's guidelines including the Code are transparent and well understood by directors, staff at all levels and business partners through circulars, briefings or training sessions.
- Include anti-bribery knowledge (e.g. the POBO, key corruption risk indicators, common corruption risks and safeguards as well as integrity challenges the bank needs to handle) in the training.
- Apart from operational training, provide directors and staff with training on anti-bribery laws, corruption risks and related measures for specific business function(s), pitfalls relating to integrity issues (e.g. conflict of interest) they may face in their business operations, and guidance on how to properly deal with them.
- Ensure effectiveness of the training by adopting different formats (e.g. e-training, quiz) with content regularly updated, conducting periodic reviews and providing information on available training and resources.
- Issue periodic reminders of the bank's anti-corruption policy, such as before festivals when business partners and customers are expected to offer gifts.

3.3.7 EXTERNAL COMMUNICATION

- Apart from the disclosures required from regulators and industry associations, make known to customers, suppliers and service providers, and business associates the bank's anti-bribery provision (e.g. prohibition of solicitation and acceptance of advantages by bank staff in relation to the bank's business) (Reference at ***Section 2.2*** of ***Chapter 2***) and warn them against the offering of any advantages to staff of the bank in relation to their banking services (e.g. by including/publicising such information in the form of "important notice", reminder, leaflet, application forms, bank's websites, service contracts, etc.).

- Impose the necessary probity requirements on these external parties, e.g. draw their attention to a warning on possible consequences (i.e. criminal liabilities) of providing false information and submitting bogus documents, and require them to declare on relevant documents that all the information and supporting documents provided are true and accurate.

- Make known to these external parties the due diligence process to be conducted by the bank (e.g. inform customers of the bank's right and action to verify the information provided by the applicants) and the bank's policy to report corrupt/fraudulent practice to the law enforcement agencies.

- Draw these external parties' attention to important notes such as, without limitation, the need for them to –

  - check the terms and other essential information carefully, and avoid signing blank or unclear documents;

  - be alert to any suspicions (e.g. unauthorised change of information or transactions in bank account, failure to receive any notification of result after submitting applications for a long period of time, being solicited of advantages by bank staff in relation to the bank's business / service engagement), and contact the bank promptly and directly through a designated enquiry hotline, etc.; and/or

  - avoid collusion with intermediary companies in applying for any bank service / bidding for service contract and keep them known of the serious consequences of the breaches via the application forms, corporate website, etc.

3.3.8 COMPLAINT AND REPORTING CHANNELS

- Conduct survey or set up hotline to collect customers' feedback on the services provided by staff and encourage customers to reflect their opinions frankly.

- Develop procedures and guidelines for the proper handling of enquiries/complaints/reports, the procedures should include accessibility of confidential information, escalation process, record keeping, time frame and monitoring, etc. to ensure that all enquiries/complaints/reports are properly handled with reporting mechanism to appropriate authorities (e.g. the Board and senior management).
- Establish a whistleblowing policy and system[22] , in particular for reporting of corruption and violations, which covers the following –
  - state the bank's anti-corruption policy and provide suitable channel(s) for reporting corruption and violation of the policy;
  - require all personnel of the bank to report promptly any corruption to the ICAC or through the reporting channels provided as appropriate;
  - encourage business partners (e.g. suppliers, contractors) to report corruption or corruption attempts by any of the bank's personnel;
  - provide assurance of confidentiality, prompt handling by sufficiently senior authority and non-retaliation to the staff/persons who make a report in good faith;
  - avoid any acts that may jeopardise or affect future investigation by a law enforcement agency;
  - reiterate the zero-tolerance policy towards any corrupt behaviour detected, which will result in reporting to the relevant law enforcement agency and disciplinary action such as termination of employment (in the case of staff) or termination of contract and exclusion from future bidding (in the case of suppliers/contractors); and
  - inform the Board regularly on the report received (e.g. number, type, handling of complaints).

3.3.9 REVIEWS AND AUDITS

- Put in place an internal audit function to independently evaluate the effectiveness of risk management, control and governance processes.
- Ensure that the internal audit function –
  - is independent from operation under audit, sufficiently staffed by staff of appropriate qualification and training, has unfettered access to all records, assets, personnel and premises, and to obtain such information and explanations as and when considered necessary;

[22] *The CPAS of the ICAC has developed a framework of the core elements/provisions of a corporate whistleblowing policy which aims at helping organisations to enhance their corporate whistleblowing policy and corruption prevention capability. For further information, please contact the CPAS through the established channels (Reference at Chapter 8).*

- develops an audit programme setting out the auditing assignments to be performed and conducts regular review to the programme taking into account the risk of key business processes; and
- reports directly to the Audit Committee, if established, or the senior management and draws their immediate attention to any significant irregularities detected in the course of audit review.

- Conduct periodic compliance / audit checks to ensure bank staff's compliance with the established policies and procedures.
- Conduct regular/random independent audits on operations/processes/transactions that are exposed to risks of corruption or malpractice (e.g. based on the audit team's knowledge or past corruption cases) to deter and detect irregularities. Deploy management/exception reports and computer-aided audit tools to facilitate the audit. Regularly monitor and review the risks and controls, and update/improve the controls where necessary.
- Make the parties concerned (e.g. bank staff) aware of the random/independent check policy for deterrence purpose.
- Require the Board to give due consideration to the opinions and findings of both the internal and external auditors, and take timely actions in response to the recommendations/findings, as well as monitoring the progress in redressing any problems/loopholes raised by the auditors.

3.3.10 CONTROL THROUGH DIGITALISATION AND REGTECH SOLUTIONS[23]

- Identify and computerise/automate the work processes and workflow management where necessary and practicable, and resources permit, to reduce corruption and malpractices arising from manual errors and human manipulation.
- Upon considering adoption of technologies / Regtech solutions, seek expert advice, keep in view the technological development in the industry, and make reference to the regulator's recommendations where necessary and practicable, among others.
- Build in the necessary functionalities (e.g. the function of generating management and exception reports for management's review and analysis, the function to facilitate electronic declaration of conflict of interest by directors/staff and management of such declarations, monitoring on real time functions, case allocation and monitoring functions, adoption of artificial intelligence to automate business process, detect patterns and general insights) from the system / Regtech development stage to facilitate corruption and fraud prevention or in more holistic terms, overall governance and internal control.

[23] *The HKMA promotes Regtech adoption in Hong Kong in recent years. Banks may refer to relevant webpage of HKMA for details (www.hkma.gov.hk/eng/key-functions/banking/regtech-knowledge-hub/). The term "Regtech" refers to use of technologies (e.g. artificial intelligence, machine learning, natural language processing, optical character recognition) that enhances efficiency and/or the effectiveness of risk management and regulatory compliance.*

- Where a workflow is digitised/automated, install adequate and essential security safeguards (e.g. encryption, data classification) and controls to enhance the effectiveness of digitalisation / Regtech solutions and efficacy of corruption/fraud prevention.
- Ensure effective implementation and usage of information technology (IT) systems / Regtech solutions by staff, covering issuance of clear policies, the requirement for generation of periodic reports for management's review and prudent follow-up, safekeeping of such reports for a specified period, provision of adequate training to staff on the proper usage, etc.
- Conduct periodic monitoring and assessment on systems / Regtech solutions adopted on areas including effectiveness of risk management and security controls regularly after the launch of the systems / Regtech solutions by staff members / external advisors with the necessary competencies and expertise in performing the assessment, who are also independent from the design, implementation and operation of the systems / Regtech solutions.

3.4 CONTROLS AGAINST MONEY LAUNDERING

Corruption and money laundering are very often intertwined. On one hand, money laundering allows the concealment of the unlawful source of funds and assets including proceeds of a corruption offence. Such corrupt proceeds may be placed, layered or integrated into one's legitimate accounts without being detected and confiscated. On the other hand, corruption may also facilitate the commission of a money laundering offence and hinder its detection. In terms of the channels for laundering proceeds for illicit activities, threat analysis reveals that banking sector continues to be exposed to relatively higher risks given that money laundering syndicates often attempt to misuse bank accounts for money laundering, trying to make use of Hong Kong's efficient financial and banking systems[24]. Besides, with technological advancement, the global payment landscape has been developing rapidly. Stored value payment products, internet and mobile payment services have gained popularity, with increased linkages to bank accounts. While bank accounts are the most common vehicle exploited for money laundering (Reference at ***Chapter 4***), money launderers may also attempt to launder their proceeds of illegal acts including corruption through other operations of banks (e.g. wealth management services) to create complex layers of transactions to increase difficulties in tracing the origins of funds (Reference at ***Chapters 5*** and ***6***). To safeguard the integrity of the banking industry and the bank itself against money laundering threat and the related corruption/fraud, banks should implement the following

[24] *The "Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report" published in July 2022 examines the money laundering and terrorist financing threats and vulnerabilities facing various sectors in Hong Kong and the city as a whole. The report is available at www.fstb.gov.hk/fsb/aml/en/doc/2nd%20HK%20ML%20TF%20Risk%20Assessment%20Report_e.pdf.*

holistic controls, making reference to the above internal control principles (Reference at ***Section 3.3***), and to be supplemented by the operation-specific ones at the relevant Chapters.

- Keep abreast of the legislative and regulatory requirements[25], as well as guidelines from industry associations[26] on anti-money laundering, and ensure that relevant operational guidelines of the bank are promptly updated with reference to the latest requirements.
- Internally, set up a management-led platform / task force to better identify, understand, and mitigate existing and emerging money laundering and financial crime risks so as to facilitate detection of suspicious activities in relation to such risks.
- Externally, step up communication within the banking network to discuss cases, trends and typologies and share intelligence with a view to strengthening banks' capability in the identification/inquiry of corruption-related money laundering activities.
- Undertake continuous awareness-raising efforts to educate operational staff preferably at all levels adequately on AMLO including the offences, the customer due diligence and record keeping requirements, through periodic capacity building sessions.
- Ensure that the relevant anti-money laundering safeguards are adopted in new procedures / provision of new services (e.g. digital payment channels, remote customer on-boarding).
- Make a best attempt to ensure that candidates applying for a banking job in particular for the persons who will hold a significant management functions are duly vetted or screened in the recruitment process (e.g. conduct reference checks with former and current employers, require disclosure of criminal records especially in relation to corruption and fraud) to reduce the chance that individuals who engage in misconduct / illegal activities in the past are able to obtain a job in another bank.
- Ensure that staff involving in compliance risk management and controls are equipped with necessary knowledge and experience, and engage external experts as appropriate (Reference at ***Section 7.4.1*** of ***Chapter 7***).

[25] *SPM module "Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions)" (AML-2) provides practical guidance to assist banks and their senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances, so as to meet the relevant AMLO requirements, and is available on HKMA's website: www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g33.pdf.*

[26] *The HKAB has developed the "Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism" to assist banks in understanding AML-2 and the relevant requirements (Available at www.hkab.org.hk/download.jsp?isTemp=N&section_id=5&file_name=AML+FAQ+20220630+%28clean%29.pdf). To provide banks with trade business for reference in the implementation / review of effective measures against related money laundering and terrorist financing risks, HKAB has also developed the "Guidance Paper on Combating Trade-based Money Laundering" which is available at the HKAB's website: www.hkab.org.hk/download.jsp?isTemp=N&section_id=5&file_name=Guidance+Paper+on+Combating+Trade-based+Money+Laundering+%28final%29.pdf.*

4 MANAGEMENT OF BANK ACCOUNTS

4.1 INTRODUCTION
4.2 KEY PROCESSES
4.3 MAJOR CORRUPTION RISKS AND RED FLAGS
4.4 CORRUPTION PREVENTION SAFEGUARDS

4 MANAGEMENT OF BANK ACCOUNTS

4.1 INTRODUCTION

The increased efforts in combating illegal activities (e.g. money laundering) in recent years have prompted banks to enhance their anti-money laundering and counter-terrorist financing controls, including a stringent due diligence process for customers. Given the more elaborated account opening process and stringent requirements, there are incentives for ineligible applicants / corrupt parties to bribe bank staff for their assistance to circumvent the controls or due diligence requirements imposed by banks and regulators. In addition, customers' personal information maintained by banks are of great marketing value and dishonest bank staff may sell the same to outsiders for illegal reward.

With the advancement of financial technology, banks have been providing and advocating online banking services. This facilitates customers to preserve privacy and conduct real time bank transactions / account enquiries. Among other benefits, the online banking services also make it easier for banks to monitor corruption/fraud before it causes further harm. Yet on the other hand, there are some corruption and security concerns with online banking (e.g. leakage of password). Meanwhile, in response to this technological development and increasing public demand, among others, virtual banks[27] have emerged to serve the community which primarily deliver retail banking services through the internet or other forms of electronic channels instead of physical branches. The pros and cons of online banking are similarly applicable to these virtual banks which may also be subject to other unique risks. The adoption of appropriate corruption prevention measures could help safeguard the integrity of the above processes, and protect the bank, its staff and customers.

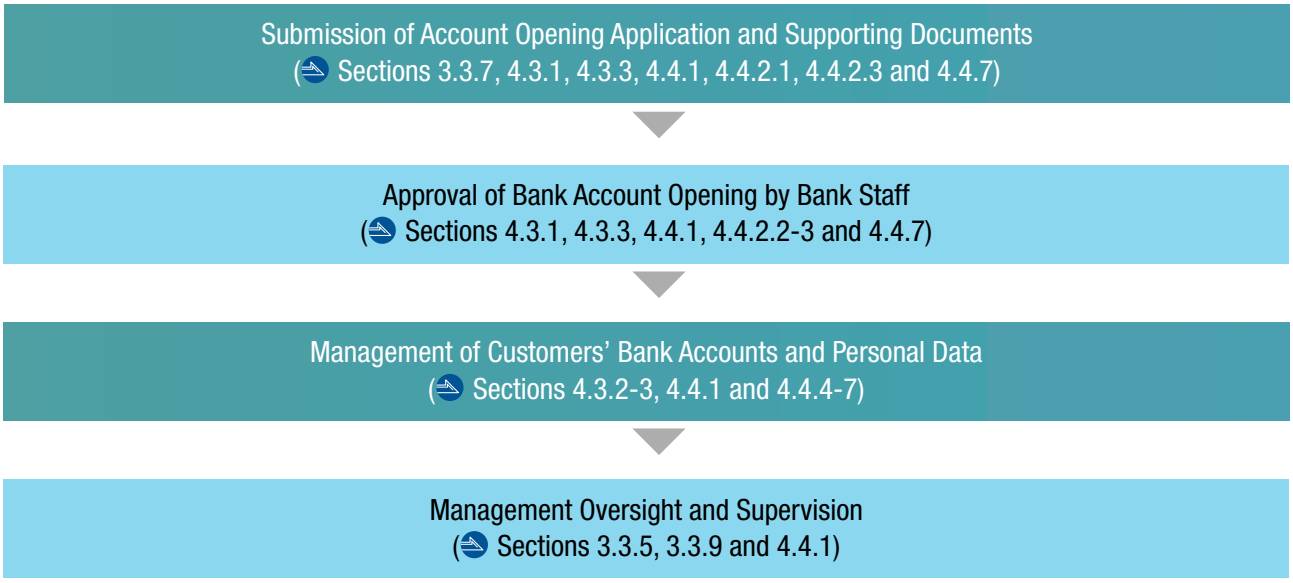
This Chapter highlights the major risks and provides the corresponding recommended measures in the related process covering bank account opening procedures and handling of customers' bank accounts and personal data, operation of online banking, and anti-money laundering requirements[28]. Given the increasing trend to use technologies for internal control, streamlining and efficiency (Reference at ***Section 3.3.10*** of ***Chapter 3***), the corruption prevention safeguards as recommended in this Chapter also cover adoption of technologies where appropriate.

[27] *As at 31 August 2022, there were eight virtual banks incorporated in Hong Kong and authorised by the HKMA.*

[28] *While some processes described in this Chapter such as handling of personal data, online banking and anti-money laundering requirements are also applicable/involved to/in other banking processes under the Chapters hereafter, they are highlighted in this Chapter given the level of relevancy and for simplicity.*

4.2 KEY PROCESSES

The following flow chart illustrates the key procedures adopted by a bank in handling bank account opening and provision of banking services –



4.3 MAJOR CORRUPTION RISKS AND RED FLAGS

MAJOR CORRUPTION RISKS

4.3.1 BANK ACCOUNT OPENING

- Corrupt bank staff soliciting/accepting advantages from applicants for facilitating account opening application process (e.g. skipping certain checks in vetting procedures, expediting the process).
- Colluded bank staff soliciting/accepting advantages from outsiders (e.g. intermediary companies) as a reward for assisting their customers in the account opening application process (e.g. accepting false information / bogus documentary proof, making false representation that the customers have arrived at the bank for the account opening process).
- Dishonest bank staff soliciting/accepting advantages from illicit parties for conniving at or even assisting in their scam for recruiting "stooges" (e.g. students, non-locals) to open bank accounts for illegal purpose (e.g. receiving proceeds of fraud or other criminal offences).

- Compromised bank staff soliciting/accepting advantages from customers using shell companies for opening a bank account for money laundering or other illegal purpose so as to hide the actual beneficial owners.

Case Study 1 – Soliciting Handling Fees for Opening Corporate Accounts from Customers

1 A relationship manager of a bank (Bank A) is responsible for opening bank accounts for customers.

2 The relationship manager solicits from some customers a handling fee, ranging from $5,000 to $12,000 for opening a corporate account, to which Bank A actually has no such requirement. Moreover, the relationship manager informs the customers that he can exert influence to expedite the account opening process upon receipt of the fee. Some customers accede to the relationship manager's request and agree to the payment. Those customers pay the fees to the relationship manager's personal bank account accordingly.

3 The relationship manager and the customers may respectively commit an offence under Sections 9(1) and 9(2) of the POBO.

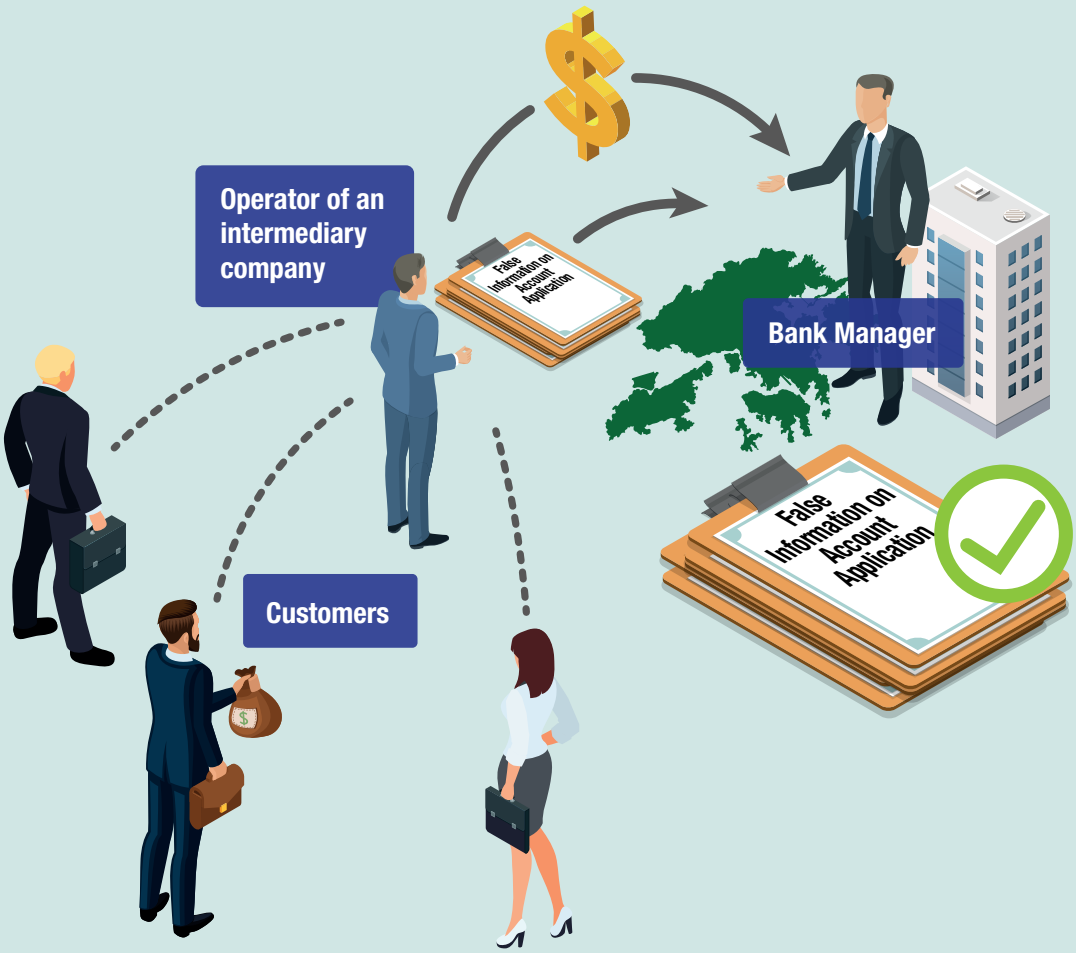
Analysis and Points to Note –

- Some anxious customers may offer or agree to the solicitation of dishonest bank staff to give money for the latter's assistance in opening a corporate bank account. Some compromised bank staff may exploit those customers with inadequate knowledge and deceive them into paying disguised fees in opening a bank account.
- Such contravention of the POBO and commission of other related offences by the parties concerned will adversely affect the reputation of the bank and injure the interests of customers. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 4.4.1-2*** and ***4.4.7***.

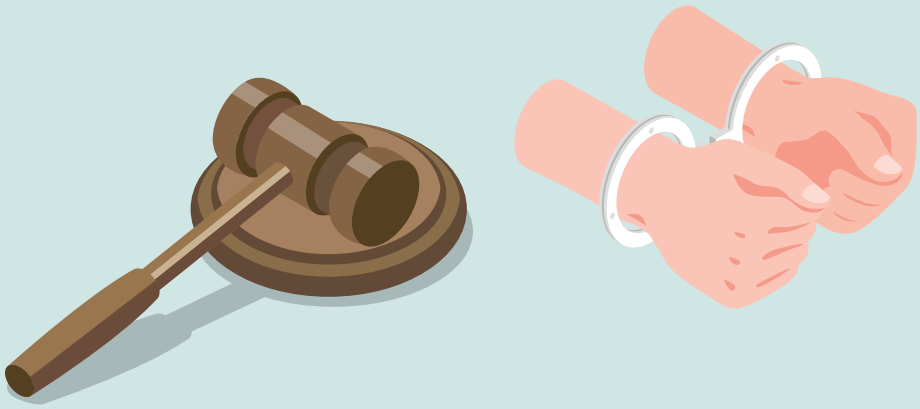
Case Study 2 – Conspiracy with Intermediaries to Submit False Information on Account Opening Applications

1 A bank (Bank B) requires customers, who wish to open a corporate account, to attend its branches in person for due diligence purpose.

2 As some of its customers consider inconvenient to come to Hong Kong or the branches in person, the operator of an intermediary company, which assists its customers to open bank accounts in Hong Kong, offers advantages to a bank manager of Bank B for his assistance in opening accounts for the customers who cannot visit the branches personally. As its general practices, Bank B relies on its bank managers to witness the attendance of customers and check the originals of the customers' supporting documents and sign to certify true copies of the documents. It does not require another staff member / the supervisor for counter check on the original documents or applications submitted. Knowing Bank B's practices, the bank manager falsely indicates on the application forms that those customers have visited the branch in person for the account opening process, and signs to certify copies of the customers' identity documents without checking the originals. The bank manager then submits the application forms together with the certified true copies of documents in support of the applications.



3 The manager of Bank B and operator of the intermediary company may respectively commit an offence under Sections 9(1) and 9(2) of the POBO, the manager may also contravene Section 9(3) of the POBO.



Analysis and Points to Note –

- Some dishonest bank staff might, for their own personal gain, conspire with customers or their representatives (e.g. intermediaries) to deliberately conceal or provide false information on the application forms, or submit false supporting documents so as to circumvent the controls on customer due diligence requirements. Customers who authorise the intermediaries to perform any corrupt act (e.g. colluding with the intermediaries to bribe the bank manager to facilitate the checking process) or any person who is involved in the scam may also contravene the POBO and commit other related offences.
- Such contravention of the POBO and commission of other related offences by the parties concerned will adversely affect the reputation of the bank. This may also reflect the incapability of the bank to comply with the regulatory requirements (e.g. anti-money laundering), resulting in possible sanction against the bank by regulators. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 4.4.1-2,*** and ***4.4.6-7***.

4.3.2 MANAGEMENT OF CUSTOMERS' PERSONAL DATA AND BANK ACCOUNT

- Compromised bank staff soliciting/accepting advantages as a reward for leaking customers' personal data (e.g. sharing customers' data to persons in other banks or companies for marketing purposes).
- Dishonest bank staff misappropriating customers' funds (e.g. using pre-signed instruction forms by customers, forging the signatures of customers on instruction forms with a view to swindling customers' money to themselves).
- Compromised staff soliciting/accepting advantages for facilitating money laundering activities (e.g. concealing/not reporting suspicious transactions to the banks).
- Dishonest bank staff facilitating the application for / conniving at the operation of "stooge account" (i.e. account used by criminals for receiving/laundering fraudulent payments or other crime proceeds).

Case Study 3 – Misuse of Customers' Personal Information

1 A manager of a bank (Bank C) possesses with access to a computer system storing customers' confidential information. He solicits commissions from some loan sales executives of Bank C, who have no access to the system, for providing Bank C's customer information. The loan sales executives agree.

2 Bank C does not have adequate safeguards in the computer system (e.g. no restrictions/ records on printing/sending of confidential information from the computer system). The manager retrieves personal data of a number of Bank C's customers and sends the retrieved data to the loan sales executives. Based on the customer information provided by the manager, the loan sales executives contact those customers to tout for personal loan business. For each successful loan procured, the loan sales executives pay the manager a certain percentage of the loan amount as commission.

3 The manager and loan sales executives may respectively commit an offence under Sections 9(1) and 9(2) of the POBO.

Analysis and Points to Note –

- There are cases where dishonest bank staff "selling" confidential/customer information to colleagues and/or outsiders who may use the information (e.g. marketing of their products). With the growing use of computer system in recording customer's information and handling of customer's requests, it is important for banks to adopt sufficient safeguards against misuse of customer information held in physical and electronic forms.

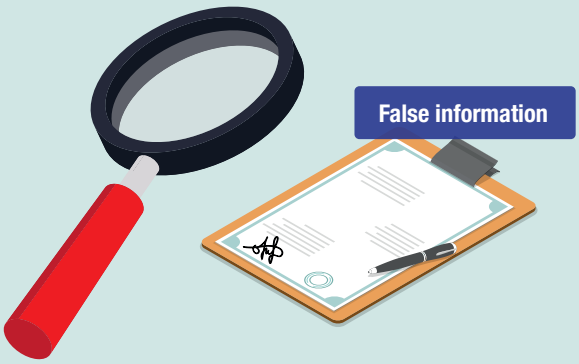
- Such contravention of the POBO and commission of other related offences by the parties concerned will adversely injure the interest of customers and cast doubt on the capability of the bank in protecting confidential information. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.9, 4.4.1, 4.4.3*** and ***4.4.7***.

Case Study 4 – Bribe for Assistance in Money Laundering

1 A relationship manager of a bank (Bank D) is responsible for looking after the bank accounts of an overseas corporate customer.

2 The compliance department of Bank D detects some suspicious transactions in the said bank account and requests the relationship manager to perform a customer due diligence check by completing a checklist, or else the relevant accounts may be frozen. During inquiries to the customers about those suspicious transactions, the relationship manager is aware that those suspicious transactions may involve crime proceeds. To cover up the money laundering activities, the customer offers bribe to the relationship manager. The relationship manager accepts the bribe and assists in concealing the issue when completing the customer due diligence checklist.

3 As its general practices, Bank D mainly relies on the information provided by the relationship manager upon investigating suspicious transactions. Knowing Bank D's practices and with the aim to assist the customer in retaining the account, the relationship manager provides false information on the checklist. Without further verification and investigation by the compliance department on the information provided by the relationship manager, Bank D retains the account of the customer.



4 The relationship manager and customer may respectively commit an offence under Sections 9(1) and 9(2) of the POBO. In submitting false information on the checklist, the relationship manager may also contravene Section 9(3) of the POBO.

Analysis and Points to Note –

- Some compromised bank staff might, for their own interests (e.g. soliciting/accepting advantages from customers), conspire with customers to deliberately conceal or provide false information to the bank during compliance checks. There are also cases where compromised bank staff assist criminals in money laundering or not report such suspicious transactions to the bank.
- Such contravention of the POBO and commission of other related offences by the parties concerned will adversely affect the reputation of the bank and its ability to detect suspicious transactions. The bank may also be penalised under AMLO by the relevant regulator(s). If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.9, 4.4.1*** and ***4.4.6-7***.

4.3.3 ONLINE BANKING

- Dishonest bank staff abusing the trust of customers having long established business relationship with them, or exploiting those customers with inadequate knowledge and experience in using online banking, soliciting customers' personal sensitive information such as user names and passwords to conduct unauthorised transactions (e.g. fund transfer) with the customers' bank accounts.
- Corrupt bank staff providing assistance to colluded customers in facilitating them to arrange rapid fund transfer to other accounts through online for money laundering purpose.
- Compromised bank staff facilitating ineligible customers / corrupt parties to open bank accounts through online banking given that verification of documentary proof could be more difficult to perform without the counter / face-to-face services.
- Bank accounts of vulnerable customers (e.g. the elderly) being exposed to higher risk of manipulation (e.g. abused by bank staff and colluded parties to open a bank account / perform a transaction without their authorisation) given that they do not need to be present at the branch in person for account opening applications and transactions.
- With the financial technology becoming more popular, banks possibly recruiting more staff with technology background rather than finance/banking background. With these staff who are relatively green in terms of banking experience, they may be more vulnerable to corrupt approaches and falling prey to corruption given their inadequate awareness/training regarding the importance of regulatory compliance.

Red Flags

1. **Malpractices in Account Opening**

   (a) **Exceptional increase of number of account opening cases** – Unexpected increase in account opening cases handled by a particular bank staff member, which is exceptional or without apparent reasons in a short period of time.

   (b) **Suspicious supporting documents** – Submission of suspicious supporting documents for application of bank account (e.g. blurred/unclear records, same address for different unrelated corporate/individual customers).

2. **Misuse of Customers' Personal Data**

   (a) **Abnormal patterns in log-in / access to information** – Abnormal patterns identified in bank staff's log-ins (e.g. frequent log-ins after office hours, access to accounts/ database that are outside the scope of their job or with volume far exceeding the job's needs).

3. **Mishandling of Customers' Bank Accounts**

   (a) **Irregularities identified in customers' requests** – Irregularities identified in customers' requests submitted through bank staff (e.g. questionable signatures on customer request form for transfer of funds).

   (b) **Abnormal patterns in customers' transactions** – Abnormal patterns identified in customers' transactions handled by the same bank staff member (e.g. frequent, large or unexplained deposits and withdrawals of funds between certain accounts in particular immediately after account opening, transaction amount/pattern that does not align with the profile of the customers).

4.4 CORRUPTION PREVENTION SAFEGUARDS

4.4.1 GUIDELINES AND INSTRUCTIONS

- Lay down comprehensive policies and procedures for handling of account opening applications, bank accounts and confidential information, including, amongst others, the following –
  - handling of different types of customers in particular those who pose higher risk to banks upon the banks' risk assessment (e.g. intermediaries, shell companies, customers with higher risk of money laundering / manipulation), and the relevant review and escalation procedures;
  - requirement for information and supporting documents for customer due diligence purposes;
  - vetting process including performance of verifications/checks (e.g. verification of customers' identity documents);
  - protection of customers' personal data (e.g. classification, access right controls, and proper storage of information);
  - handling of customers' bank accounts including dormant/inactive accounts (e.g. definition of dormant/inactive account, conditions under which such an account may be reactivated, due diligence check and approval authority for its reactivation); and
  - requirement of maintenance of proper record for subsequent audits.
- Ensure that the above rules are transparent to the parties concerned (e.g. via company intranet, circulars, training).

4.4.2 ACCOUNT OPENING

4.4.2.1 Application Process

- Segregate the duties of submission, checking and approval of applications in the account opening process.
- Enhance control and surveillance measures at counters / bank staff's office (e.g. install CCTV to record the application process).

- Require frontline staff to verify the authenticity of supporting documents submitted by applicant (e.g. certify against the genuine records) (*Use of Technology*) and require endorsement by another staff member and/or branch supervisor on a risk based approach.

- Publicise the different types of bank accounts' opening requirements/eligibility for customers' reference.

- Require customers to declare on the application form the source of referral and related fee/charge (e.g. whether they are referred by other bank staff or intermediaries such as a company secretary firm, whether a fee/charge is requested by such bank staff or intermediaries) for opening a bank account, and details of their previous application rejected by the bank (if any).

4.4.2.2 Checking Process

- Allocate application cases on a rotation basis to the checking staff for processing, with justifications properly documented for any out-of-turn cases.

- Adopt adequate internal controls in the checking process including the customer due diligence process (e.g. computer system to monitor the process, checklist of required documents, approval/rejection with detailed justifications recorded).

- Use computer system or provide checklists for bank staff to perform various checks when conducting customer due diligence process for different types of customers.

- Verify the customer's information against reliable and independent databases/ source (e.g. records of the Company Registry) (*Use of Technology*) or engage independent party (e.g. engage vendor to conduct company search) in the checking process on a risk basis.

- For any suspected fraudulent application/supporting document, remind staff to report to appropriate authorities in the bank (e.g. compliance department) and refer to law enforcement agency as appropriate.

4.4.2.3 Account Opening through Online Banking

- Exercise the same vigilance and independence when handling the account opening applications through online banking as that of other in-person customers handled by the bank, in particular, ensure that the customer due diligence requirements are adequately fulfilled (*Use of Technology*).

- Enhance controls over processing of account opening applications through online banking by -
  - setting out diligent measures for bank staff to verify documentary proof without viewing the originals; and
  - requiring additional verification process or presence at branch for customers identified with higher risk (e.g. customer who is a politically exposed person) or higher risk for manipulation (e.g. customers of suspicious background).

Use of Technology

Banks may consider -

- ☑ using technologies (e.g. cloud-based customer information management technology, machine learning) to facilitate timely review and ascertaining the authenticity of the identification documents submitted by customers.
- ☑ using technologies (e.g. data analytical techniques to conduct comprehensive search on customers, machine learning to match information regarding a particular customer) to enhance the effectiveness of customer due diligence process as well as to reduce human discretion in the process.
- ☑ using biometrics and other technologies (e.g. facial, fingerprint, liveness and/or geo-location recognition) to confirm that the person operating the online banking account is indeed the person who owns the bank account, minimising the risk of potential corruption/fraud (e.g. impersonation) practised by the customer with/without connivance of bank staff.

4.4.3 SAFEGUARDING OF CUSTOMERS' PERSONAL DATA

- Build in security safeguards to protect customer information, physically and electronically maintained, from tampering or leakage (Reference at ***Section 3.3.4*** of ***Chapter 3***).
- Restrict access to confidential customer information to authorised staff only on a need-to-know basis, and subject the access rights granted to regular review.
- Keep access logs for a prescribed period which is commensurate with the importance of computer systems, and review them regularly.

- Limit the use of shared accounts and ensure that individual staff members can be identified for their actions in the computer system.
- Issue regular reminder to bank staff on the importance of safeguarding sensitive information of customers and the consequences of unauthorised disclosure of confidential customer information (e.g. criminal liabilities).

Examples of Good Practices

- Strengthen the access control (e.g. access card, password, dual log-in with password and access card) for entry to office / computer systems where confidential information are accessible.
- Restrict photo taking / photocopying / printing of confidential information (e.g. adding watermark showing staff name/number printing the document, disabling the printing / "copy and paste" function); and prohibiting taking of confidential information out of bank office.
- Encourage staff to adopt a clean desk practice.
- Enhance control on (e.g. strong encryption) or restricting the downloading of customer data to portable storage media.
- Restrict the use of email in office (e.g. sending email to outsiders) where confidential data are accessible or devise mechanism to detect unauthorised disclosure of information through email (***Use of Technology***).

Use of Technology

Banks may consider -

- ☑ using technologies (e.g. block emails or prompt an alert when an email containing confidential information is sent to external parties, lock down computer when an unauthorised person tries to use the computer, or when someone tries to capture the screen with a camera) to detect unauthorised disclosure of confidential information and taking timely follow-up action to tackle "selling" of such information for bribe.

4.4.4 MANAGEMENT OF CUSTOMERS' BANK ACCOUNTS

- Step up control measures to protect customers that are considered vulnerable (e.g. the elderly) or subject to higher risk of abuse (e.g. those who opt out to receive statement or request hold mail services by bank staff) upon the bank's risk assessment.
- Devise control measures to protect inactive/dormant accounts from possible abuse (e.g. alert on unusual fund movements, strengthen verification process and escalated approval for fund movement or change of particulars, confirmation with customers, restrict account functions before further verification / due diligence process is completed), subject inactive/dormant accounts to regular and independent review to prevent unauthorised amendments of particulars (e.g. account with no apparent relationship sharing the same correspondence) or transactions.
- Educate customers on good practices in protecting their funds/accounts (e.g. not to pre-sign blank forms or provide identity documents for bank staff to keep, promptly update personal information) through different means (e.g. advisory messages on statement, website, or other communications).

Examples of Good Practices

- Maintain regular liaison with customers to detect/deter any suspicious approaches/ acts of the handling staff concerned.
- Prohibit staff from keeping copies of customers' identity documents or pre-signed instruction forms.

4.4.5 BANKING SERVICES THROUGH ONLINE BANKING

- Prohibit bank staff from operating customers' online banking accounts and obtaining account personal information (e.g. log-in name, password) of customers (*Use of Technology*).
- Require additional verification process or presence at branch if customers require enhanced online banking services (e.g. transfer of amount exceeding a prescribed limit, purchase of investment products) or for customers identified with higher risk (e.g. vulnerable customers).

- Implement security measures of mobile application for online banking (e.g. binding the application to one device only, requiring extra verification for logging in using another device / through another IP address).
- Notify customers through different channels (e.g. text message, email, letter) any high risk actions performed online.
- Educate customers to protect their device and personal sensitive information, including use of a strong password and two-step authentication, keep the account secure through regular log-ins and checking transactions, not to share account information with others including bank staff, etc., and suggest customers visiting the HKMA website on Personal Digital Keys, security tips, and educational video.

Use of Technology

Banks may consider -

- ☑ developing/deploying technologies/electronic tools to anaylse (e.g. the typing speed, finger position and finger pressure) to detect whether an unauthorised person is attempting to log/hack into a customer's account.

4.4.6 ANTI-MONEY LAUNDERING MEASURES

- Assign independent team/staff to monitor suspicious transactions (e.g. new accounts or previously inactive accounts having frequent large payments made to third parties, large number of transactions just under a specified threshold without apparent reason) (*Use of Technology*).
- Assign independent team/staff to conduct due diligence checks on existing customers as appropriate (e.g. if suspicious transactions in their accounts are detected).
- Put in place anti-money laundering measures in the system (e.g. setting a necessary threshold for fund transfer beyond or suspicious activity indicators of which the transaction will be subject to the stringent risk assessment checks, and regularly review their effectiveness) (*Use of Technology*).
- Ensure proper documentation and trail are maintained for each transaction as well as the work done on risk assessment and customer due diligence so that it is traceable.
- Require meeting with customers before establishing a business relationship and on a regular basis for customers potentially with higher risk of money laundering as part of the due diligence procedures.

Use of Technology

Banks may consider -

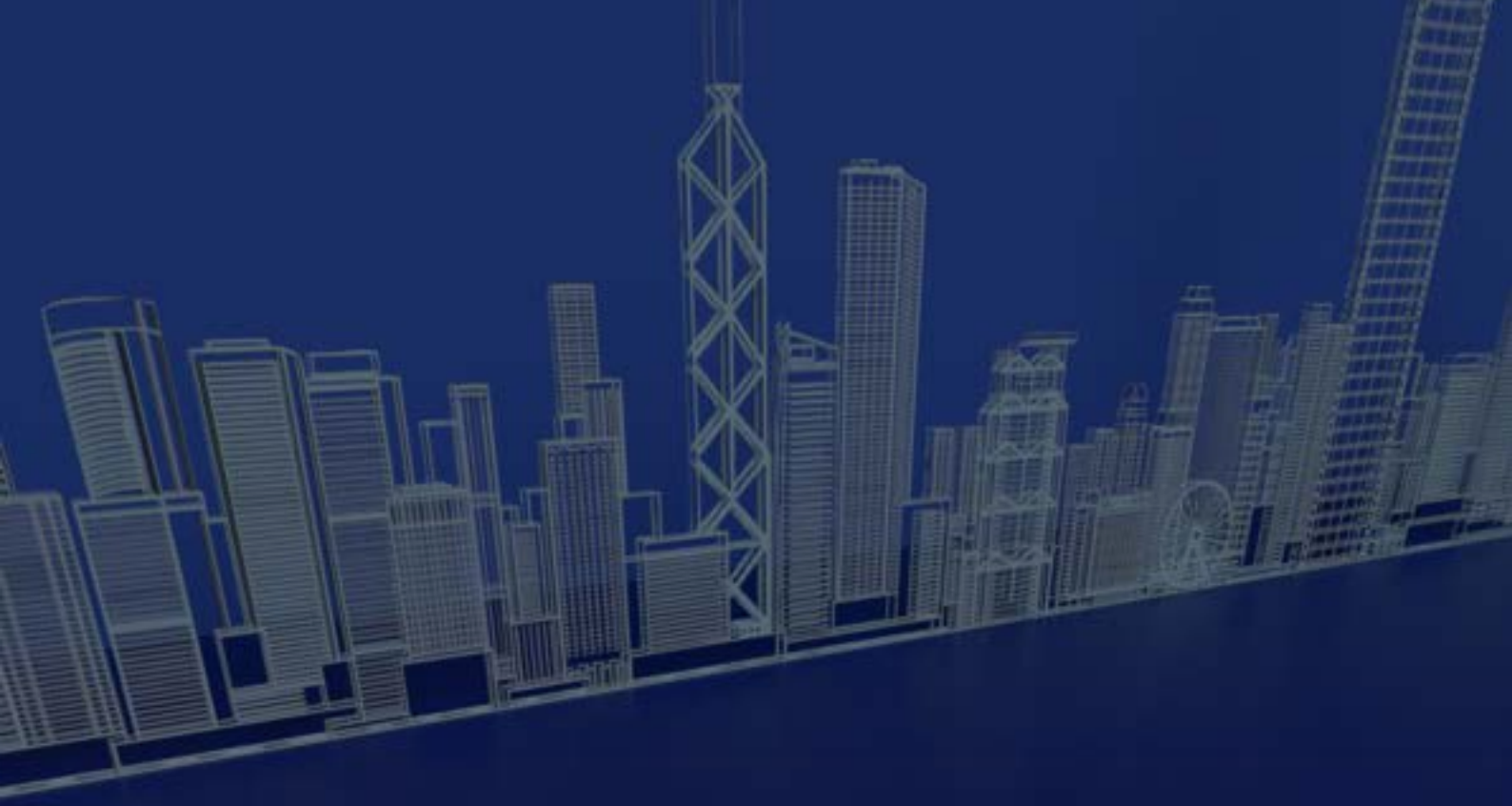
☑ using technologies (e.g. data analytics, machine learning) to analyse large volume of transactions, identify common patterns of suspicious transactions, and setting the benchmark for transactions requiring follow-up to facilitate bank staff in transaction monitoring process.

☑ using technologies (e.g. data analytics) to continuously gather, categorise, filter data regarding customers from open source and subscribed databases, and analyse in the context of financial crime risks to enhance the efficiency in on-going monitoring process.

4.4.7 STAFF TRAINING

- Provide regular training to bank staff to -
  - enhance their understanding on and compliance to the account opening process;
  - build up their capability to detect the use of fraudulent documents (e.g. forged identity documents, fake financial statements) or suspicious transactions;
  - handle confidential customer information (e.g. security measures, classification of information); and
  - familiarise with the requirements of the AMLO and other legislation regarding money laundering offences (e.g. OSCO), as well as guidelines issued by regulators[29], importance of compliance to the said requirements and possible consequence of non-compliance. Banks may consider arranging role-based (e.g. relationship managers, staff with control functions) / trade-based training to educate staff about the specific risks and responsibilities relevant to the duties of individual staff.

[29] *For example, comprehensive circulars and SPM guidelines on anti-money laundering & counter-financing of terrorism issued by the HKMA.*



5 CREDIT FACILITY AND LOAN SERVICES

5.1 INTRODUCTION
5.2 KEY PROCESSES
5.3 MAJOR CORRUPTION RISKS AND RED FLAGS
5.4 CORRUPTION PREVENTION SAFEGUARDS

5 CREDIT FACILITY AND LOAN SERVICES

5.1 INTRODUCTION

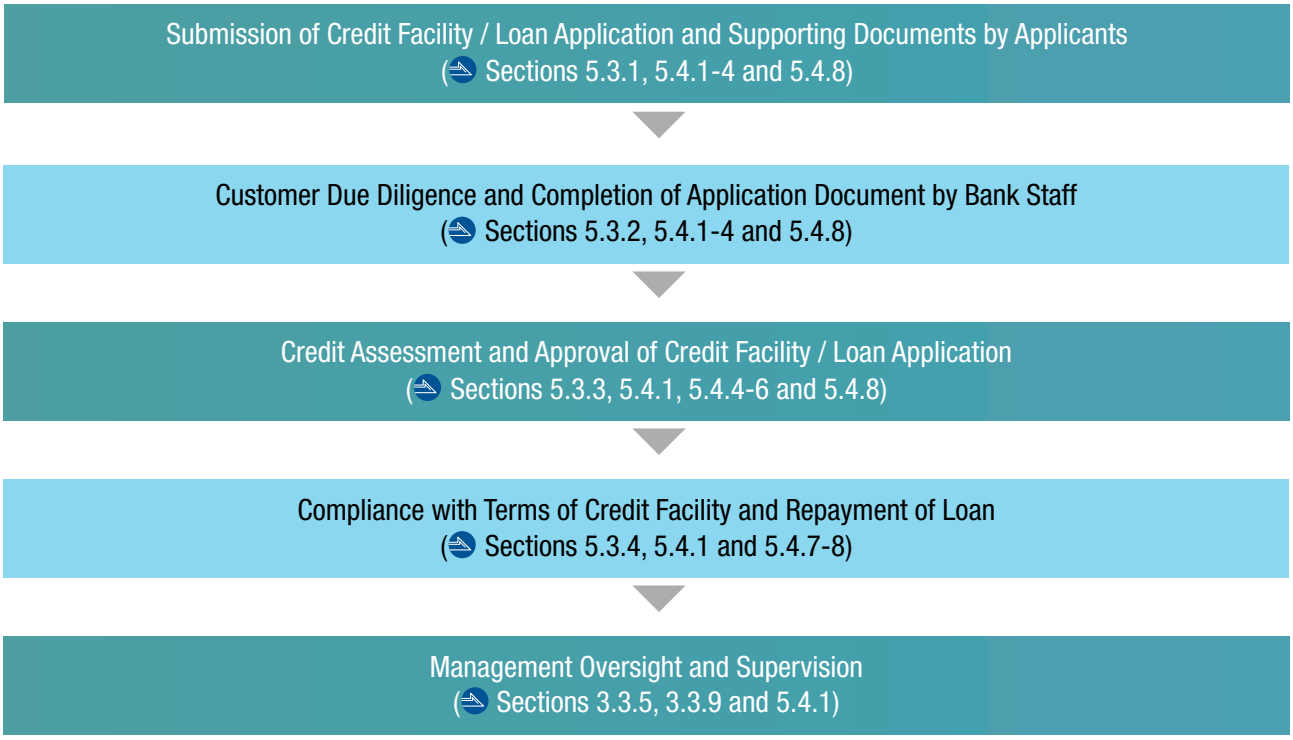
Credit facility and loan services are the core businesses in a bank's operations, which involve undertaking of loan services, customer due diligence, loan / credit facility assessment, approval, monitoring and repayment. However, due to keen competition among the industry, the incentives brought by the commission-based remuneration as well as the substantial sums of money involved (e.g. amount of credit facility / loan granted), unscrupulous bank staff might, upon soliciting/accepting advantages from customers, conspire with them to deliberately favour or provide assistance on the credit facility / loan applications so as to circumvent the necessary requirements and controls.

This Chapter highlights the major risks covering credit facility and loan services and provides the corresponding recommended measures in the related process, covering undertaking of loan business[30], handling of credit facility / loan applications, conduct of customer due diligence, credit appraisal and approval, monitoring of compliance with terms of credit facility and loan repayment, etc. Given the increasing trend to use technologies for internal control, streamlining and efficiency (Reference at ***Section 3.3.10*** of ***Chapter 3***), the corruption prevention safeguards as recommended in this Chapter also cover adoption of technologies where appropriate.

[30] *Banks may refer to Chapter 6 for corruption risks and safeguards in relation to sales process.*

5.2 KEY PROCESSES

The following flow chart illustrates the key processes in respect of granting of credit facility / loan in a bank –



5.3 MAJOR CORRUPTION RISKS AND RED FLAGS

MAJOR CORRUPTION RISKS

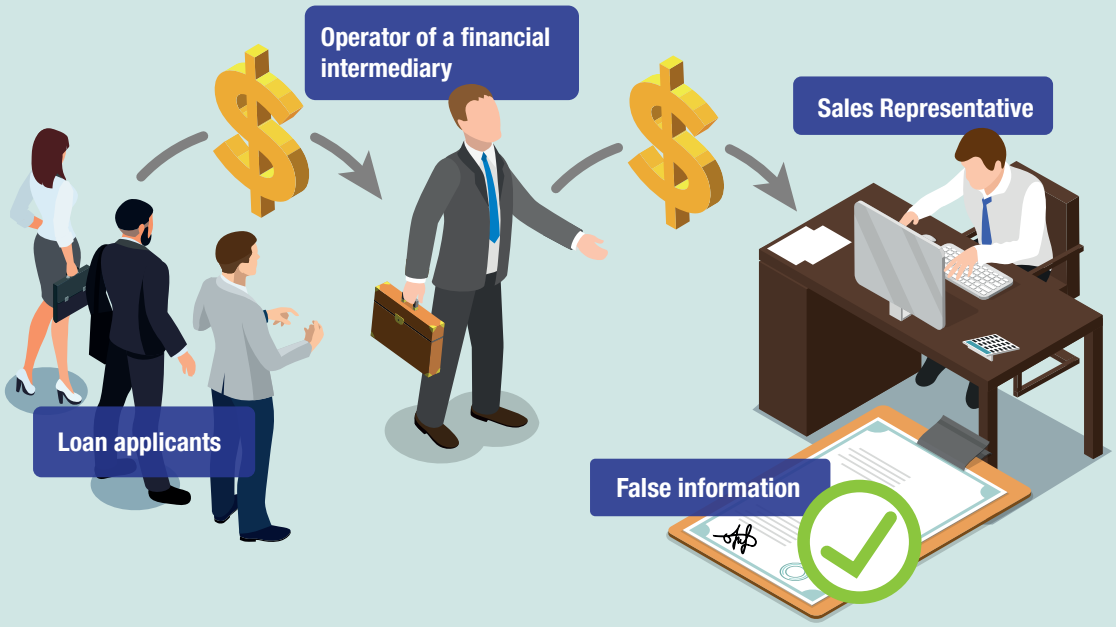
5.3.1 SUBMISSION OF LOAN APPLICATIONS BY APPLICANTS

- Colluded bank staff soliciting/accepting advantages from intermediaries for handling/favouring loan applicants referred by them, which is prohibited by the bank.
- Compromised bank staff soliciting/accepting advantages from applicants as a reward for conniving at false information/supporting documents provided by them.
- Colluded bank staff soliciting/accepting advantages from intermediaries as a reward for assisting their customers to apply for government-guaranteed financing scheme.

Case Study 1 – Conspiracy with an Intermediary for Deceiving Commissions

1 A sales representative of a bank (Bank A) who previously worked in a financial intermediary (FI) is responsible for sourcing potential loan applicants by operating street booths and distributing promotional items (e.g. flyers). He receives commission from Bank A on each successful loan application handled by him.

2 FI sources loan applicants from its own network and charges loan applicants a certain percentage of the loan amount as service fee for each successful application. The operator of FI offers advantages to the sales representative as a reward for his assistance in handling loan applications referred from FI.



3 As a measure to protect the interests of the bank and its customers, Bank A rejects personal loan applications referred from intermediaries and prohibits its sales representatives from handling such referral from intermediaries. Noting that Bank A has inadequate safeguards against detection of fraudulent practices (e.g. no supervisory/ independent checks on the source of business), the sales representative falsely indicates on the application forms that the personal loan applications referred from FI are sourced from the street booth, with an intent to deceive Bank A to accept the loan applications referred from FI. He also instructs the loan applicants to confirm on the application forms that they are not referred from an intermediary.

4 Having believed that the information provided on the application form is genuine, Bank A approves the loan applications and releases commissions to the sales representative for the successful loan applications. The sales representative notifies the loan application results to applicants as well as the operator of FI so that the latter can charge its customers service fee.

5 The sales representative of Bank A may contravene Sections 9(1) and 9(3) of the POBO, while the operator of FI may commit an offence under Section 9(2) of the POBO.

Analysis and Points to Note –

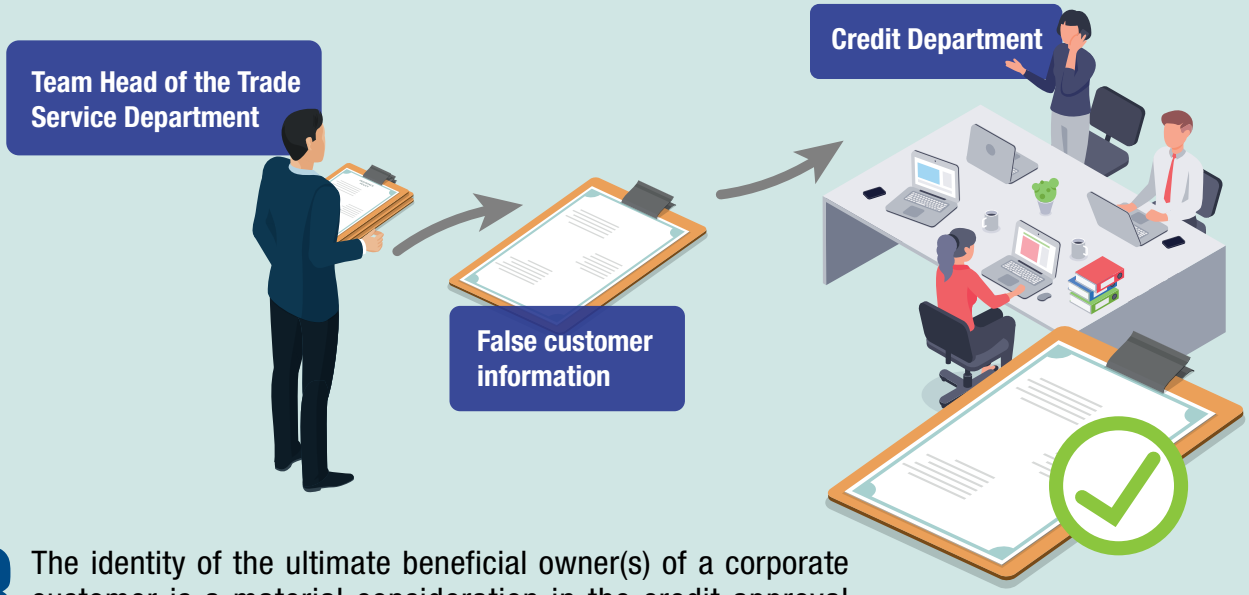
- Due to the lack of knowledge or insufficient market information, some desperate loan applicants wrongly believe that financial intermediaries could assist them to secure loan more easily so that they are willing to pay additional service charges to the intermediaries for loan application. Keen competition among banks to source loan applicants could exert pressure on and/or drive up commissions paid to sales staff, and unscrupulous bank staff may cross the line (e.g. handling loans referral from intermediary which is prohibited by the bank) to secure more business. These bank staff members may collude with intermediaries, to assist their customers in loan applications which is prohibited by the employing bank, and at the same time earning extra commissions by providing false information on the application forms to circumvent control of the bank.
- Such contravention of the POBO and commission of other related offences by the parties concerned will seriously injure customers' interests as they are required to pay additional service fees to the intermediary for the loan applications made to the bank. Such corrupt practices also have a negative impact on the integrity culture of the bank. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 5.4.1-2, 5.4.8*** and ***6.4.3***.

Case Study 2 – Conspiracy with Customer to Conceal Material Facts in Loan Application

1 A team head of the trade service department of a bank (Bank B) is responsible for promoting finance products (e.g. loans) to corporate customers. If a corporate customer decides to apply for business loans, the request would be referred to the credit department of Bank B for credit assessment and loan approval. The credit department mainly relies on the customer information provided by the trade service department, without further checking/verifying the information provided.

2 The team head of the trade service department accepts bribes from a friend who has bad credit history for assisting him in a business loan application. Knowing the credit

department's practices, the team head assists his friend by concealing the fact that his friend is the ultimate beneficial owner of a company, and providing false customer information for the credit department's follow-up actions.



3 The identity of the ultimate beneficial owner(s) of a corporate customer is a material consideration in the credit approval process. Having believed that the customer information provided by the team head is genuine, the credit department of Bank B grants a business loan to the company.

4 The team head and his friend may respectively contravene Sections 9(1) and 9(2) of the POBO.

Analysis and Points to Note –

- In order to get a loan from bank, ineligible applicant (e.g. applicant who goes bankrupt or has bad credit history) might collude with bank staff to provide false information or conceal certain material facts to deceive the banks in the credit assessment and approval process. When an applicant is willing to offer bribe for a favourable treatment in loan application and approval, it reflects the underlying financial problems of his business and the poor intergiry of that applicant. Therefore, the chance of defaulting repayment will be high. Sometimes, it may be desirable from the customer service angle to have the same bank staff member to provide customer service and act as the bank's contact point for important clients. However, if all verification/clarification of questionable or doubtful transactions are routed through the same bank staff member, it would undermine checks and balances, and create opportunities for manipulation by unscrupulous staff.

- Such contravention of the POBO and commission of other related offences by the parties concerned will lead to financial loss of the banks. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 5.4.1-2, 5.4.5*** and ***5.4.8***.

Case Study 3 – Acceptance of Bribe for Assistance in Application for Government-Guaranteed Financing Scheme

1 To ease the cash flow problems of enterprises in the challenging business environment, the Government has launched a financing guarantee scheme (the Scheme) with relatively easy terms for Small and Medium Enterprises[31] to apply for. The maximum loan amount for each eligible enterprise is the total amount of employee wages and rents for certain months or the specified maximum amount, whichever is the lower. Under the Scheme, the Government provides full guarantee coverage for the loans of eligible enterprises handled by the participating lenders.

2 Bank C is one of the participating lenders of the Scheme. To satisfy the eligibility of the Scheme, Bank C requires loan applicants to submit a number of supporting documents. For operational efficiency, a team is designated to handle such applications. Bank C allows its staff to exercise discretion by professional judgement (e.g. waiving the submission of original documents) when receiving applications, and does not require the handling staff to check against third party documents given credit history is not a key factor to approve the loan applications under the Scheme.

[31] *The SME Financing Guarantee Scheme was first launched in 2011 by HKMC and transferred to and carried on by HKMC Insurance Limited in 2018, aims at helping tide the enterprises over financing difficulties as a result of a possible credit crunch in midst of the uncertain global economic environment.*

3 An operator (the Operator) of a consultancy company, who is a former staff of Bank C, is familiar with Bank C's operations and the staff processing loan applications. The consultancy company provides one-stop services to assist enterprises to apply for loan under the Scheme, and claims that it could assist loan applicants to maximise/inflate the loan amount and charges them certain percentage of the loan amount as service fee for each successful application.

4 The Operator offers advantages to the handling bank officers as a reward for their assistance in handling the loan applications under the Scheme (e.g. by providing inside information on how Bank C handles the loan applications, turning a blind eye to the false supporting documents). Having believed that the applications and supporting documents provided are genuine, Bank C disburses a number of loans to the enterprises referred by the consultancy company.

5 The handling bank officers, and the Operator may respectively contravene Sections 9(1) and 9(2) of the POBO.

Analysis and Points to Note –

- It does occur that corrupt intermediary companies collude with enterprises and bank staff to take advantages of the government-guaranteed financing scheme. Some of the eligible enterprises may face genuine business difficulties, but they want to inflate the amount of loan they could obtain under the scheme (e.g. by providing forged payslips / MPF records to exaggerate headcounts of the enterprise), while some are only shell companies without any business activities. Corrupt intermediary companies may bribe bank staff for assistance (e.g. provide inside information on the bank's internal controls and process, circumvent control of the bank) to achieve the above purpose. Customers who collude with the intermediaries to perform any corrupt act (e.g. knowing and agreeing that part of the 'consultation fee' they pay is for to the purpose of "tea money" to the bank manager to facilitate the checking process) may also contravene the POBO and commit other related offences.

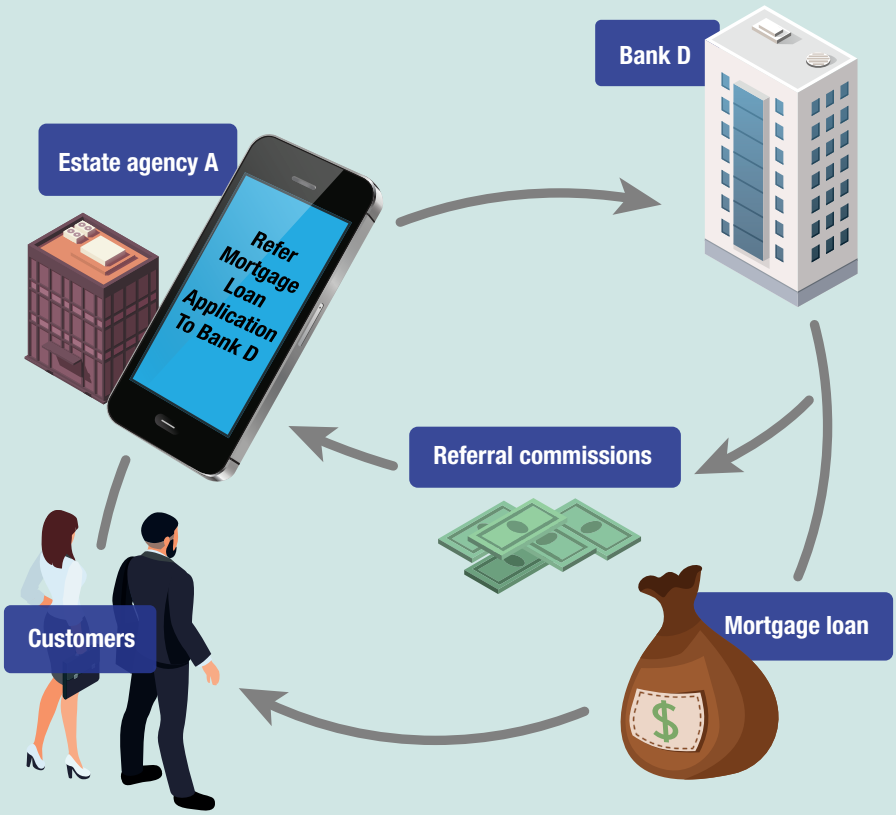
- Such contravention of the POBO and commission of other related offences by the parties concerned will seriously injure the borrowers' interests (e.g. paying additional service fees to the intermediary companies for the loan applications made to the bank). Banks' failure in detecting such malpractice may also adversely affect the banks' reputation and reflect the incapability of the bank to work as a participating lender for government schemes. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 5.4.1, 5.4.4-5*** and ***5.4.8***.

5.3.2 CUSTOMER DUE DILIGENCE AND COMPLETION OF APPLICATION DOCUMENTS

- Dishonest bank staff submitting loan application documents containing false information to deceive the banks for ineligible commissions (*Case Study 1* is also relevant).
- Unscrupulous bank staff who conduct site inspection or other due diligence duties soliciting/accepting advantages for making/giving a favourable recommendation/ report.

Case Study 4 – Using False Documents to Deceive Mortgage Referral Fees

1 To attract business, a bank (Bank D) runs a mortgage loan referral programme. Under the programme, referral fees in the amount of a certain percentage of the mortgage loans will be given to the designated estate agency which has successfully referred business to Bank D. One of the designated estate agencies (Agency A) operates a smart phone application for the public to refer potential mortgage loan applications to it and earn referral commissions in return.



2 Noting the programme arrangement as well as the smart phone application operated by Agency A, and knowing that Bank D does not have supervisory/independent checking on source of business, a branch manager of Bank D who is responsible for handling walk-in customers, uses the smart phone application to refer loan applications to Agency A to earn referral commissions. In fact, those applications are all from walk-in applicants.

3 On the other hand, with intent to deceive Bank D, the branch manager falsely states on the signed application forms that those walk-in mortgage loan applications handled by him were referred by Agency A, and submitted the signed application forms to Bank D only after the referral arrangement has been recognised by Agency A. Having believed that the information provided on the application forms is true and upon successful application, Bank D grants referral fees to Agency A. Referral commissions are then granted to the branch manager by Agency A afterwards.

4 The branch manager of Bank D may contravene Section 9(3) of the POBO.

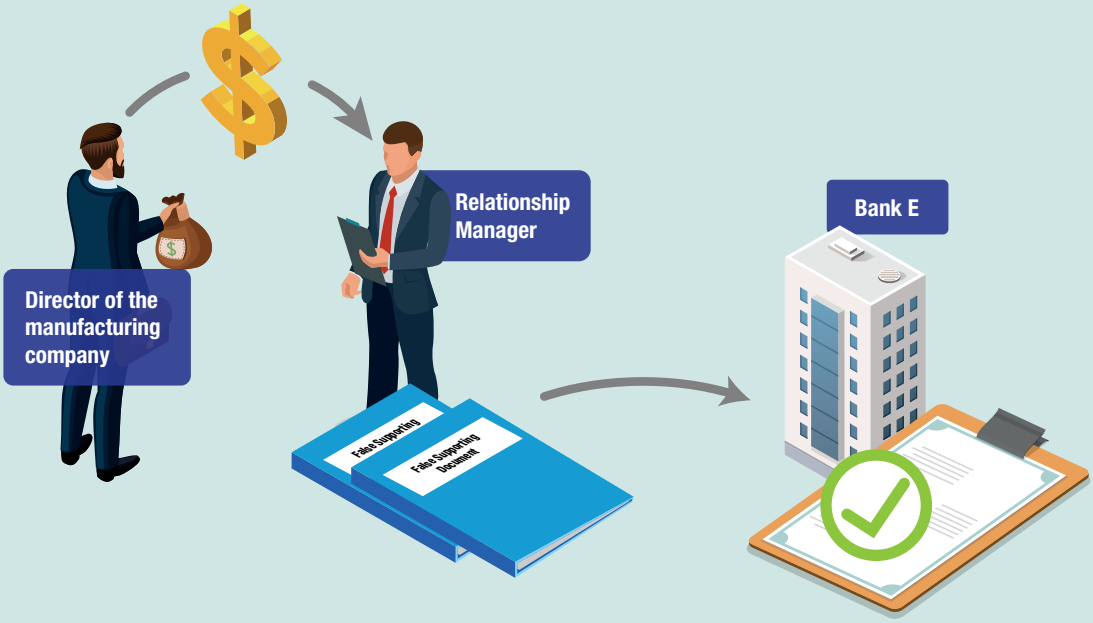
Analysis and Points to Note –

- Some dishonest bank staff might abuse their knowledge on banks' operations to manipulate the loan application process (e.g. input false information on the application form after it is signed by the customer and submit it to deceive banks for extra commissions).
- Such contravention of the POBO and commission of other related offences by the bank staff will cause financial loss to the banks and have a negative impact on the integrity culture of the bank. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 5.4.1-2*** and ***5.4.8***.

Case Study 5 – Acceptance of Advantages during Site Inspection outside Hong Kong

1 A relationship manager of a bank (Bank E) is responsible for handling credit facility applications received from small and medium enterprise customers under his client portfolios. A manufacturing company, a regular customer handled by the relationship manager, applies for credit facilities for its new production equipment outside Hong Kong. To facilitate credit assessment, Bank E assigns the relationship manager to visit the production plant of the manufacturing company outside Hong Kong alone for site inspection purpose.

2 During the site visit, the director of the manufacturing company keeps offering the relationship manager lavish entertainment and appreciates his good customer services over the years. The relationship manager finds the equipment old and substandard when conducting the inspection in the production plant. When they return to Hong Kong, the director offers an expensive watch to the relationship manager and requests the latter to turn a blind eye to the old equipment. The relationship manager accepts the advantages



and promises to prepare a favourable site inspection report for the manufacturing company. A site inspection report with favourable recommendation is produced and submitted to credit department together with other application and supporting documents for credit assessment and approval process afterwards. Basing on the relationship manager's assessments and recommendation, Bank E approves the credit facilities.

3 The relationship manager and the director of the manufacturing company may respectively commit an offence under Sections 9(1) and 9(2) of the POBO. The relationship manager may also commit an offence under Section 9(3) of the POBO.

Analysis and Points to Note –

- There are cases where unscrupulous customers offer advantages to bank staff for favourable assistance in credit facility application. The risks are unavoidably elevated if the customer meeting is held outside the bank branch/office, the site inspection is conducted outside Hong Kong, or the work is carried out by one single staff. These arrangements may expose the bank staff to significant risk of temptation as he may think only he and the customer know about the bribery arrangement. Besides, from customer relationship perspective, banks may not wish to regularly change relationship managers' postings or swap their client portfolios in order to maintain good relationship with customers. While the need for good customer service is understandable, the lack of periodic staff rotation increases the risk of manipulation by unscrupulous staff and may allow fraud or malpractice to continue for a prolonged period.
- Such contravention of the POBO and commission of other related offences by the parties concerned will cause financial loss to the bank (e.g. potential repayment default due to bad loans) and adversely affect the reputation of the bank. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 5.4.1, 5.4.3, 5.4.8*** and ***7.4.2.5***.

5.3.3 CREDIT ASSESSMENT AND APPROVAL OF LOAN APPLICATIONS

- Corrupt bank staff soliciting/accepting advantages in return for approving unqualified loans or credit facilities (Reference at ***Case Study 3***).
- Corrupt bank staff responsible for determining the terms (e.g. interest rate, repayment terms) of the credit facility / loan business soliciting/accepting advantages in return for offering better terms to the applicants.

5.3.4 COMPLIANCE WITH TERMS OF CREDIT FACILITY AND REPAYMENT OF LOAN

- Corrupt bank staff who have authority/discretion in endorsing minor exceptions in terms of credit facility or extension of loan repayment soliciting/accepting advantages from borrowers in return for favourable treatments (Reference at ***Case Study 1*** of ***Chapter 1***).

Red Flags

1. **Malpractices during Application Process**

   (a) **Exceptional increase of credit facility / loan applications volume** –

   - Unexpected increase in loan applications (either in volume or amount) by a particular bank staff member, which is exceptional or without apparent reasons in a short period of time.
   - Sudden drop in the number of walk-in customers applications received by bank coupled with corresponding increment of particular source of business (e.g. referred by an external estate agency) without justifiable reasons.

2. **Relationship with Customers**

   (a) **Frequent and lavish entertainment with customers** – Bank staff responsible for handling credit facility / loan applications (e.g. relationship manager) having too close relationship with the applicants, customers or external intermediaries (e.g. accepting frequent and/or lavish entertainment from the latter).

   (b) **Staff refusing others to handle customers under their charge** – Staff refusing other colleagues to handle his customers during his vacation leave, or using different reasons to delay or exempt from taking “block leave”.

3. **Submission of Suspicious Documents for Loan Application**

   (a) **Suspicious supporting documents** – Applicants' supporting documents (e.g. collateral valuation report) issued by a third party which is being identified as having a history of involvement in dubious/fraudulent activities, or which show that they involve in a business not commensurate with their known profile, structure, business strategy or historical pattern of trade activity without reasonable justification.

   (b) **Suspicious signs on supporting documents** – Suspicious signs (e.g. common mistakes/typos or similar features/contents of supporting documents submitted from different applicants or handled by the same bank staff, same account number or business address on the bank statements from two or more applicants) are noted on supporting documents.

   (c) **Inadequate documentation** – Bank staff failing to keep adequate documentation and records for the loan application process, or provide the completed documents/records for supervisory checks as required by the bank.

4. **Malpractices during Loan Repayment**

   (a) **Exceptionally high bad debt cases** – Exceptionally high bad debt cases handled by a particular staff member.

5.4 CORRUPTION PREVENTION SAFEGUARDS

5.4.1 GUIDELINES AND INSTRUCTIONS

- Lay down comprehensive policies and procedures for the processes in relation to the credit facility and loan services, including, amongst others, the following –
  - handling process of different types of customers in particular those who pose higher risk to banks upon the banks' risk assessment (e.g. intermediaries, customers with higher risk of money laundering) or those who are vulnerable;
  - requirements for information and supporting documents for credit facility and loan applications;

- referral of business by bank staff (e.g. referral fees, prohibiting bank staff from referring a customer to any other banks / financial institutions / organisations without the prior approval of the bank, consequence of the unauthorised referral);
- criteria and procedures for granting new credits, renewing existing credits, repayment extension and approving exceptions;
- protection of customers' personal data (e.g. lending details, credit assessment report); and
- requirement of maintenance of proper records for subsequent audits.

- Ensure that the above rules are transparent to the bank staff concerned (e.g. via company intranet, circulars, training).

5.4.2 SUBMISSION OF APPLICATION AND SUPPORTING DOCUMENTS

- Publicise the terms and conditions (e.g. eligibility, service fee, supporting documents required) for the credit facility / loan services and make it accessible to all types of applicants as far as practicable (e.g. in different language and suitable font size).
- Enhance control and monitoring measures at counters/bank staff's office (e.g. install CCTV to record the application process).
- Engage computer system or issue a standard checklist to guide bank staff on receiving supporting documents in order to reduce the likelihood of omissions.
- As far as practicable, automate loan application process (especially for those types of loan that are relatively standardised such as personal loan) to minimise human error or possible manipulation (***Use of Technology***).
- Prohibit bank staff from requesting or advising customers to sign on blank/ incomplete credit/loan application documents.
- Require loan applicants to acknowledge the terms and conditions on the application document before signing the application document; produce the original or certified true copy of the supporting documents for verification; declare on the application form whether they are referred by financial intermediaries and whether fees/commissions are paid to the intermediaries on the referral arrangement.

- Require frontline staff to conduct customer due diligence on the applicants' background, including but not limited to a thorough understanding of the applicants' organisation structure, the purpose of the credit facility / loan and its source of repayment, verify the authenticity of supporting documents and require additional endorsement by branch supervisors on a risk basis.

Use of Technology

Banks may consider –

- ☑ using online platform to submit real-time loan applications by customers so as to lessen the risk of false information added by the handling staff after the paper application forms signed by the applicants or the time of submission is electronically logged on the electronic application forms.
- ☑ using biometrics or other technologies (e.g. facial, fingerprint, liveness and/or geo-location recognition) to confirm the person who applies for loan is indeed the person who owns the identification documents as well as the bank account, which can minimise the risk of potential fraud (e.g. use of false identity documents, impersonation) practised by the customer with/without connivance of bank staff.

5.4.3 SITE INSPECTION AND WORK OUTSIDE HONG KONG

- As far as practicable, assign more than one staff member to conduct site inspections, especially if it is outside Hong Kong, and they should preferably be of different units (e.g. one being the frontline handling staff, the other a credit department staff) to avoid the situation of a subordinate being "unduly influenced" by his supervisor to act in collusion.
- Use standard format for the site inspection report covering various inspection items, require site inspections to be documented with photos of the sites and assets concerned, as far as possible (***Use of Technology***).
- On a risk basis, conduct surprise site inspection to verify information provided by customers.
- Conduct random independent audit/assurance review on higher risk cases (e.g. site visits done by a bank staff alone, selling process outside the branch).
- Although some business activities need to be conducted outside Hong Kong, as far as practicable, ensure that some important/key processes (e.g. submission/approval of credit proposal) are carried out in Hong Kong.

Use of Technology

Banks may consider –

☑ Using technologies to facilitate real-time and on-the-spot data capture/transfer for site inspection, thereby enhancing monitoring even outside the branch / Hong Kong. The relevant data/records (e.g. videos/photos taken during onsite inspection) should be made contemporaneously which help ensure the traceability of records and facilitate compliance check instantly. For effective implementation, consideration should be given to issuing mobile phones to staff and installed with cloud-based applications to facilitate real-time capture and instant transfer of information to cloud for storage.

5.4.4 SAFEGUARDS FOR GOVERNMENT-GUARANTEED FINANCING SCHEME

- Publicise the information relating to the Scheme's eligibility criteria, application procedures, assessment criteria, etc. in different languages.
- Include a warning note in the application form that any false declaration would lead to termination of the loan agreement, claw-back of any loans disbursed, report to law enforcement agencies and regulators, and the possibility of criminal charges.
- To avoid double benefit (i.e. applying for funding for the same operation/project under two funding schemes that is not allowed), devise controls to prevent/detect double application cases in the same bank and, as far as possible, across banks (e.g. by requiring loan applicants to declare in their applications whether they are applying for or have received any loan under the Scheme and report any change of information in respect of their applications).
- Exercise the same vigilance and independence when handling loan applications under the Scheme as that of other credit facilities / loans handled by the bank.
- Specify whether unsuccessful applicants are allowed to re-submit applications and if so, the conditions for re-submission.

5.4.5 CREDIT ASSESSMENT AND APPROVAL OF APPLICATION

- Lay down requirements for all new or renewal of existing credit facility / loan applications to undergo thorough credit assessments before approval, justification of any decisions violating credit risk policy/criteria for approval by designated authority.

- In addition to the information provided by customers and frontline staff, conduct reference check internally (e.g. credit history) and externally (e.g. engage external parties to conduct company search, consumer credit reference agency rating, Commercial Credit Reference Agency report, etc.) (***Use of Technology***). As far as practicable and on a risk basis, check with the issuing authority (e.g. audit firm, bank) on the authenticity of the supporting documents (e.g. audit report, bank statement).
- Avoid delegating staff member who directly deals with customers with any credit approval authority. If delegated, the assigned credit limit should not be significant and the approvals made by customer handling staff should be subject to independent reviews or audits.
- Require staff member who performs credit assessment and approval duties to be independent from other business unit. Allocate cases to them by rotation, with justifications properly documented for any out-of-turn cases.
- Ensure checks and balances to prevent undue reliance on the decisions of a single officer (e.g. loans approved by one staff member to be reviewed periodically by another staff member or by an independent reviewer on a risk basis, credit facilities / loans over a certain amount should be reviewed by the Chief Executive Officer / Credit Committee and reported to the Board on a regular basis).
- Document the deliberations and decisions made on controversial application cases (e.g. having weaknesses in the credit assessment, excess over internal limits), and require proper approval (e.g. require another approver to counter-sign) of such cases.
- For any suspected fraudulent application/supporting document, remind staff to report to appropriate authorities in the bank (e.g. compliance department) and refer to law enforcement agencies and/or regulators as appropriate.

Use of Technology

Banks may consider –

☑ using technologies and analytical techniques to assist credit assessment process (e.g. using machine learning technology to develop a credit model based on datasets adopted by the bank and automate the assessment process to determine the terms of the credit facility/loan, using artificial intelligence to identify patterns to predict risk of bankruptcy and generate insights to improve the credit model and assessment model).

5.4.6 NOTIFICATION OF RESULTS

- For successful application, send the result together with the terms and conditions for the credit/loan granted to the applicant directly to deter fabrication of credit facility / loan applications by using customer details without the latter's knowledge or leakage of information to unauthorised parties.
- For unsuccessful applications, notify the applicants in writing.

5.4.7 LOAN REPAYMENT AND APPROVAL OF EXTENSION

- Separate loan extension approval authority from staff who deal directly with customers.
- Exercise the same vigilance and independence in the approval of the loan extension as that of new credit facility / loan application, and with proper justification and documentation.
- Limit the number of loan extension, and assign the case to another bank staff for processing when the number of extension exceeds the number permitted.
- Monitor credit performance of loans through exception reports, and build in controls in the system to alert the management on exceptional/irregular cases as necessary (e.g. identify irregularities like repeated extensions of repayment due dates and the approving bank staff involved).

5.4.8 STAFF TRAINING

- Provide regular training to bank staff to
  - enhance their understanding on and compliance obligations to the loan application process;
  - build up their capability to detect the use of fraudulent documents (e.g. forged identity documents, fake financial statements);
  - reinforce the escalation process/channels when detecting irregularities or alleged frauds; and
  - strengthen their ability to valuate asset/collateral and assess credit.

6 SALES PROCESS AND WEALTH MANAGEMENT

6.1 INTRODUCTION
6.2 KEY PROCESSES
6.3 MAJOR CORRUPTION RISKS AND RED FLAGS
6.4 CORRUPTION PREVENTION SAFEGUARDS

6 SALES PROCESS AND WEALTH MANAGEMENT

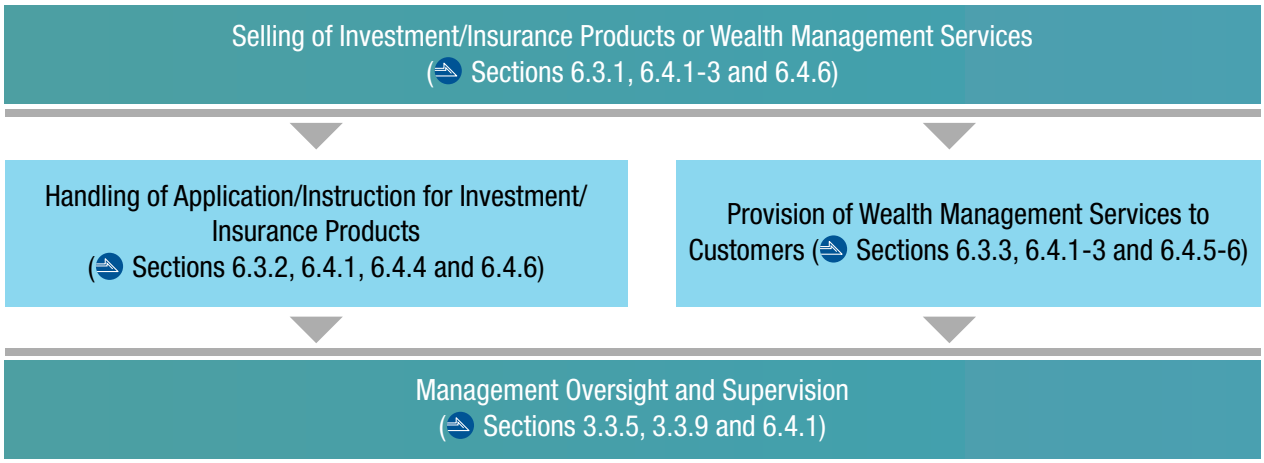
6.1 INTRODUCTION

Apart from deposit and loan services, banks also develop and distribute finance products (e.g. investment plans, structured products) or partner with other financial institutions / insurance companies and promote such products and wealth management services to their customers. As these activities may involve substantial sums of money and remuneration to bank staff based on the products sold, services provided, and/or target met, the processes are susceptible to risks of manipulation. The risks are further increased as some customers tend to rely on the bank staff in managing their fund, giving rise to opportunities for abuse by unscrupulous bank staff in particular given the long business relationship established. The adoption of appropriate corruption prevention measures could help safeguard the integrity of the above processes, avoid abuse of the remuneration system and protect the bank, its staff and customers.

This Chapter highlights the major risks and provides the corresponding recommended measures in the related process, covering selling of investment/insurance products and wealth management services and products, referral of business, handling of application/ instruction documents, provision of wealth management services and products, as well as remuneration structure. Given the increasing trend to use technologies for internal control, streamlining and efficiency (Reference at ***Section 3.3.10*** of ***Chapter 3***), the corruption prevention safeguards as recommended in this Chapter also cover adoption of technologies where appropriate.

6.2 KEY PROCESSES

The following flow chart illustrates the key procedures adopted by bank staff in sales of investment/insurance products and wealth management services and products for customers –



6.3 MAJOR CORRUPTION RISKS AND RED FLAGS

MAJOR CORRUPTION RISKS

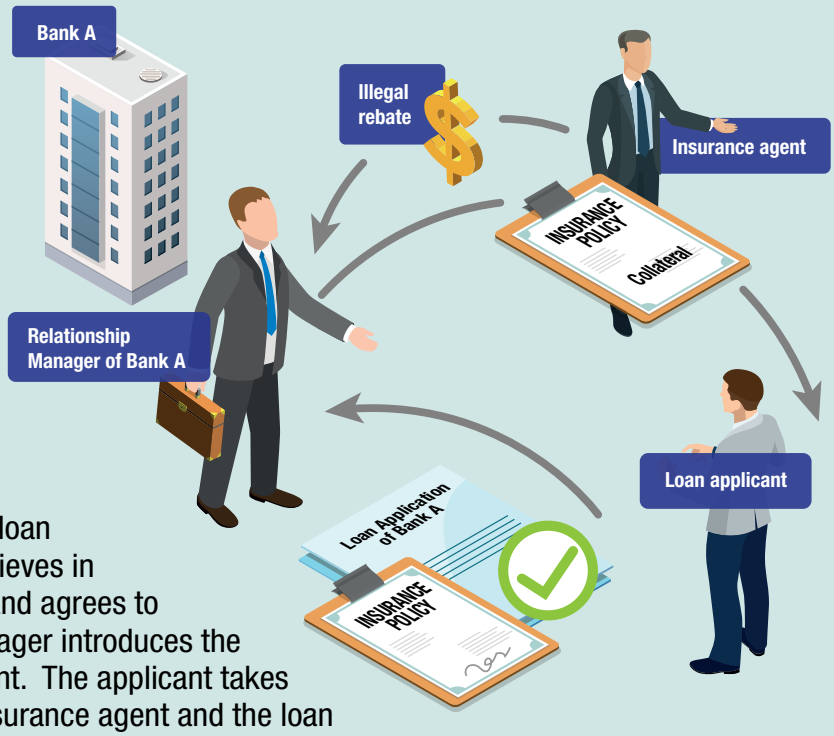
6.3.1 SELLING OF INVESTMENT/INSURANCE PRODUCTS[32] AND WEALTH MANAGEMENT SERVICES AND PRODUCTS / REFERRAL OF BUSINESS

- Colluded bank staff soliciting/accepting illegal rebates as a reward for promoting the investment/insurance products of and referring/diverting customers to other banks or financial institutions, which is prohibited by his employing bank.
- Colluded bank staff offering advantages (e.g. by sharing the sales commissions) to staff of other banks, intermediaries or financial institutions as a reward for referring customers to him for selling of investment/insurance products.
- Unscrupulous bank staff deceiving customers to take out insurance policies for personal gain (e.g. sharing of commission from an insurance agent).

[32] *Banks may refer to the "Corruption Prevention Guide for Insurance Companies" which provides corruption risks and the corresponding safeguards in core operations of insurance industry, including sales of insurance policies. The Guide is available at cpas.icac.hk/EN/Info/Lib_List?cate_id=3&id=2568.*

- Compromised bank staff using false risk assessment records of customers in order to sell investment products that do not match with the customers' risk tolerance level for securing commission.
- Dishonest staff abusing the sales process (e.g. splitting insurance policy of customers) for higher commission in particular for commission-based remuneration schemes that are too complicated, poorly designed and prone to abuse and fraud.
- Banks may engage intermediaries to assist/facilitate selling or wealth management activities (e.g. mortgages, corporate business finance). Intermediaries may also expose to the above risks of corruption committed by their staff when acting on the bank's behalf or providing services to the bank, or offering advantages to the bank's personnel to secure business, etc.

Case Study 1 – Conspiracy with Outsiders for Deceiving Customer into Taking Out Insurance Policy for Illegal Commissions



1 A relationship manager of a bank (Bank A) is responsible for handling loan applications. He agrees to promote insurance products of his friend who is an insurance agent for illegal rebate.

2 The relationship manager misleadingly informs a loan applicant of Bank A that the bank requires an insurance policy as a collateral for securing a loan for him. Due to insufficient knowledge on Bank A's loan criteria and policy, the applicant believes in the relationship manager's advice and agrees to the proposal. The relationship manager introduces the insurance agent to the loan applicant. The applicant takes out an insurance policy from the insurance agent and the loan is subsequently approved.

3 The insurance agent pays a proportion of his commissions from the insurance policy to the relationship manager as a reward for the latter's referral of customer.

4 The relationship manager and the insurance agent may respectively commit an offence under Sections 9(1) and 9(2) of the POBO.

Analysis and Points to Note –

- Some unscrupulous bank staff might, for their own personal gain (e.g. soliciting/accepting rebates from other financial institutions), promote the products of other financial institutions or even deceive customers into buying these products. Such risks are elevated if customers are not familiar with the banking practice in Hong Kong or from a vulnerable group (e.g. the elderly).
- Such contravention of the POBO and commission of other related offences by the parties concerned will adversely affect customers' interest as well as the reputation of the bank. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 6.4.1-3*** and ***6.4.6***.

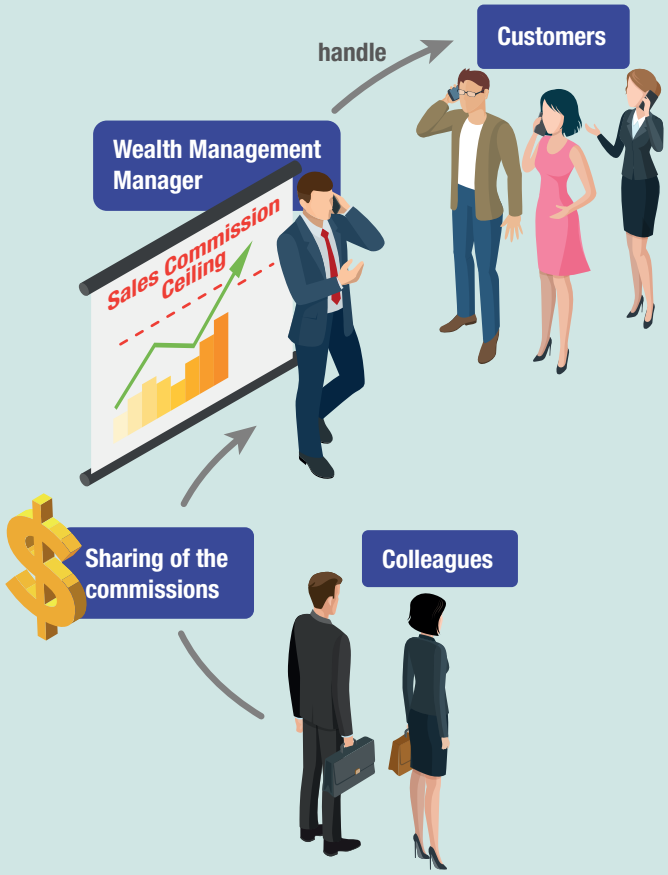
6.3.2 HANDLING OF PURCHASE FOR INVESTMENT/INSURANCE PRODUCTS

- Dishonest bank staff submitting investment/insurance products application/instruction documents containing false information to deceive the banks for personal gain (e.g. earning ineligible commissions, fabricating sales targets) or solicitation/acceptance of advantages from the parties involved (e.g. sharing of the extra commissions earned), by various fraudulent ways such as falsely representing on the application/instruction documents that another bank staff member who is not involved in the sales process is the handling officer of the applications/transactions so as to earn/share extra/overriding commission.

Case Study 2 – False Representation of Handling Staff on Application Forms to Deceive Commission

1 Wealth management managers of a bank (Bank B) earn sales commission for investment products promoted and sold by them. The sales commission is subject to a ceiling.

2 A wealth management manager of Bank B meets and promotes investment products to a number of customers who agree to buy the products. Upon his request, the customers sign on the application forms for the product, without being aware of the need to check the name of the handling staff.



3 As the manager has reached his sales commission ceiling and cannot earn any extra sales commissions, he names two of his colleagues, also wealth management managers who are not present during the whole sales process as the handling staff for the said transactions so that the latter can earn the commissions. He solicits advantages from the two colleagues by requesting sharing of the commissions by the latter. The colleagues agree to such arrangement so they can also meet their sales target.

4 Bank B does not have adequate safeguards (e.g. random post-sales confirmation calls to verify some essential information of the sales process) to deter/detect related malpractice. Knowing Bank B's practices, the wealth management manager conspires with his colleagues to submit the application forms for the investment products containing false information to Bank B. Having believed that the application forms are true and accurate, Bank B releases the commissions to the two colleagues who then give majority of the commissions they earn to the wealth management manager.

5 The wealth management manager and the two colleagues may respectively contravene Sections 9(1) and 9(2) of the POBO. They may also commit an offence under Section 9(3) of the POBO.

Analysis and Points to Note –

- Some dishonest bank staff might falsely represent on the selling documents that other bank staff who are not involved in any part of the sales process as the handling officers of the applications with a view to soliciting the commissions earned by the latter.
- Such contravention of the POBO and commission of other related offences by the bank staff concerned will cause financial loss (e.g. paying extra commission to the colluded staff) to the banks. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 6.4.1-4*** and ***6.4.6***.

6.3.3 WEALTH MANAGEMENT SERVICES AND PRODUCTS

- Unscrupulous bank staff soliciting/accepting advantages for giving priority for handling customer's transactions and providing privileged investment information.
- Customers from different cultures, who may regard offering monetary rewards to bank staff as a norm, offering advantages to bank staff as a reward for gain on investments managed by the latter.
- Dishonest bank staff performing unauthorised transactions for customer and concealing the transactions by furnishing false records (e.g. transaction records, monthly statement).
- Corrupt bank staff assisting customers to purchase investment products where illicit funds are laundered to legitimate investment returns, through making use of the characteristics of wealth management services which involve large amount of funds, complexity of products and services, and a culture of confidentiality and personalised services.

Case Study 3 – Soliciting Additional Commission from Customers

1 An associate director of an investment bank (Investment Bank C) asks one of his non-local customers to pay him 20% of the realised profits from investment as "handling and intelligence fees". As the customer believes that this is a normal trade practice in Hong Kong without knowing that the Investment Bank C prohibits its staff from soliciting and accepting advantages including commission in relation to their duty, he agrees to the proposal.

2 The associate director accords priority in providing latest investment advice to and execute investment transactions for the customer. As he manages to make a good profit, the customer pays the fees to him as agreed.

3 The associate director convinces the customer to entirely rely on him to manage his account and opt out of receiving advice slip. As the customer has trust in the associate director in managing his investment, he agrees to his proposal. The associate director then makes some transactions in the account which are not authorised by the customer, which finally causes loss to the customer.

4 The associate director may commit an offence under Section 9(1) of the POBO.

Analysis and Points to Note –

- Some dishonest bank staff might abuse their relationship with customers to solicit and accept illegal commission from them or even deceive customers into paying extra commission to them. Moreover, customers who are not familiar with the bank practices and anti-corruption laws in Hong Kong are prone to corrupt approach by bank staff. Some of them may even consider paying extra commission as a business practice and/or courtesy. It is also hard to detect procedurally corrupt offers made by satisfied customers.
- Section 19 of the POBO clearly states that it shall not be a defence to show that such advantage is customary in any profession, trade, vocation or calling. Such contravention of the POBO and commission of other related offences by the parties concerned will put the banks' reputation at stake, thereby affecting the customers' confidence in the bank. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.7, 3.3.9, 6.4.1-3*** and ***6.4.5-6***.

Red Flags

1. **Malpractices in Sales Activities**

   (a) **Exceptional increase in sales handled by individual staff / referred by intermediaries** – Unexpected increase in sales transactions by bank staff / intermediaries, which are exceptional or without apparent reasons in a short period of time.

2. **Malpractices in Wealth Management**

   (a) **Abnormal patterns in customers' portfolios** – Abnormal patterns identified in customers' transactions handled by the same bank staff member (e.g. purchasing of investment products with risk mismatching his profile, suspicious transaction amount and frequency).

6.4 CORRUPTION PREVENTION SAFEGUARDS

6.4.1 GUIDELINES AND INSTRUCTIONS

- Lay down comprehensive policies and procedures for sales activities and wealth management, including, amongst others, the following –
  - performance of risk assessment process (e.g. channels and audit trail, guidance on risk profiling, information to obtain);
  - handling of different types of customers in particular those who pose higher risk to banks upon the banks' risk assessment (e.g. customers with a lower risk tolerance on investment products, customers with a higher risk of money laundering) and the relevant review and escalation procedures;
  - performance of sales activities (e.g. explanation of terms, placement of order) and remuneration structure for handling/selling of different types of products/services (e.g. sales commission);

- referral of business by bank staff, including referral within the bank (e.g. referral mechanism and commission, documentation) and outside the bank (e.g. prohibiting bank staff from referring a customer to any other banks / financial institutions / organisations without the prior approval of the bank, consequence of unauthorised referral);
- acceptance of referral by intermediaries / middlemen, including types of business that referral from external parties are allowed, terms of such transactions (e.g. fixing of price, service fees), referral mechanism, commission and documentation;
- handling of application/instruction for investment/insurance products (e.g. completion and checking of forms), and provision of wealth management services (e.g. provision of investment advice) to customers; and
- requirement of maintenance of proper record for subsequent audits.

- Ensure that the above rules are transparent to the parties concerned (e.g. via company intranet, circulars, training).

6.4.2 REMUNERATION STRUCTURE AND INCENTIVE SYSTEM

- Where an incentive system is adopted to award those staff of good performance in particular the frontline staff, ensure that the design of the incentive system can induce ethical behaviour of staff and minimise any potential misconduct and mis-selling activities[33].
- Set reasonable sales targets for bank staff in a way that deters corruption, and ensure that the bank's commission policy does not create undue pressure on staff for engagement in corrupt or fraudulent activities.
- Review the sales targets and remuneration/commission policy periodically to verify that there are reasonable safeguards in place to prevent them from encouraging bribery.

[33] *Following the completion of the Focused Review on Incentive Systems of Front Offices in 20 Retail Banks, which aims for better alignment of incentive systems of frontline staff with customers' interests, the HKMA published the Review Report in May 2022 to share the identified industry-wide observations, incentive design principles and sound incentive practices to reinforce good customer and conduct outcomes. Banks may refer to the report in devising their incentive system. The report is available at: www.hkma.gov.hk/media/chi/doc/key-information/guidelines-and-circular/2022/20220525c1a1.pdf.*

6.4.3 SELLING OF INVESTMENT/INSURANCE PRODUCTS AND WEALTH MANAGEMENT SERVICES AND PRODUCTS / REFERRAL OF BUSINESS

- Enhance independence for assessing a customer's risk profile (e.g. conducting the assessment by bank staff other than the selling staff, developing an online platform for customers to complete risk assessment questionnaire, providing standard profiling questions) and performing ordinary banking services from sales activities, and require customers to acknowledge the risk assessment results (***Use of Technology***).

- Enhance control and monitoring measures to ensure that the sales activities are performed in accordance with the bank's policy. For instance, install CCTV / audio recording function to record the sales process, provide standard script and require bank staff to properly disclose and explain to customers the key features, risks and terms of products, require sales activities (including taking of orders) to be performed at a designated area of a branch/bank office or through designated channels, require additional approval for any investment products exceeding customer's risk profile, changing of risk profile, etc.

- When engaging intermediaries to assist/facilitate selling / wealth management activities, commit intermediaries and their staff to anti-corruption business practices (e.g. inform the intermediaries of the bank's anti-corruption policy, include suitable anti-corruption and probity requirements in the agreements with the intermediaries, prohibit illegal rebate, etc.) (Reference at ***Section 2.2*** of ***Chapter 2***).

- Engage staff independent of the sales process of the bank to handle and validate the transactions referred/arranged by intermediaries.

- Inform customers through different means the key features/risks of the services/ products (e.g. service fee, means that such fees are collected) and require customers to acknowledge the terms on the application/instruction documents.

Examples of Good Practices

- Designate at least two bank staff for the duty if resources allow and on a risk basis (e.g. sales activities conducted outside the bank office / branch), and require them to maintain sufficient record and step up monitoring over such cases.

- Develop an enquiry hotline which allows customers to communicate with the bank directly, or provide the contact of the immediate supervisor of the frontline staff to the customers for enquiry and follow-up actions.

6.4.4 HANDLING OF APPLICATION/INSTRUCTION FOR INVESTMENT/INSURANCE PRODUCTS

- Enhance the integrity and control in completion of application/instruction documents (e.g. validating the information thereon by branch manager or a central team) (***Use of Technology***).
- Establish a robust mechanism for processing application for investment/insurance products (including executing orders, confirmation and settlement) especially for those supplied by other financial institutions.

Use of Technology

Banks may consider –

- ☑ using technologies to enhance the process of risk assessment (e.g. online platform for completing a risk assessment questionnaire by customers, risk profiling, prompt alert and generate management report for any mismatching sales or changing of customer risk profile) and submission of purchase documents (e.g. by electronic means during the sales meeting with the customers/potential customers to lessen the risk of false representation of handling staff as the names of such are electronically logged on the electronic application documents) so as to minimise the risk of false representation by bank staff / customers.
- ☑ using technologies (e.g. natural language processing, voice analytics) to monitor the communications with customers to identify potential signs of stress, fraud/corrupt approach, etc.

6.4.5 PROVISION OF WEALTH MANAGEMENT SERVICES AND PRODUCTS

- Establish effective procedures for ascertaining the background of fund (e.g. source of wealth, source of fund, employment) and identifying customers and beneficial owners (e.g. politically exposed person).
- Provide an investment mandate including details of investments (e.g. product type, risk, allocation, fee structure) and the corresponding authorised actions (e.g. to buy or sell) and require endorsement of customers. When a transaction would result in deviation from the mandate, document the approval of customer to proceed with the transaction and the rationale behind.

- Provide investment-related information (e.g. market analysis, performance of investment products) through different channels (e.g. bank's website) to enhance transparency and lessen the reliance on bank staff to relay the information to customers.
- Define a customer contact protocol (e.g. circumstance where staff other than the relationship manager would contact customers to verify sensitive/doubtful transactions) and strike a balance between customer service and control (e.g. independent staff to verify transactions on a risk basis, arrange back-up staff to customers).

6.4.6 STAFF TRAINING

- Provide regular training to bank staff to –
  - enhance their understanding on compliance requirements / obligations to the sales process;
  - enhance their knowledge on bank products (e.g. features, fees, risks) in order to provide sufficient information to customers and minimise the risk of selling unsuitable products inadvertently and intentionally;
  - enhance their knowledge on risk assessment process; and
  - build up their capability to detect the use of fraudulent documents (e.g. forged identity documents).

7 PROCUREMENT AND STAFF ADMINISTRATION

7.1 INTRODUCTION
7.2 KEY PROCESSES
7.3 MAJOR CORRUPTION RISKS AND RED FLAGS
7.4 CORRUPTION PREVENTION SAFEGUARDS

7 PROCUREMENT AND STAFF ADMINISTRATION

7.1 INTRODUCTION

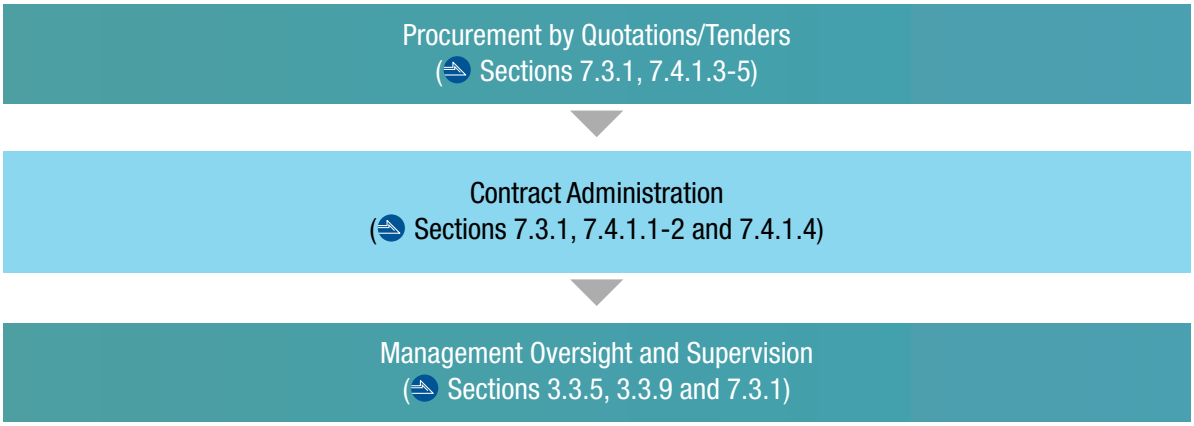
Past corruption cases show that procurement is an area most vulnerable to corrupt manipulation and malpractice due to the substantial business interests involved, and the power which individual staff may possess in determining where the money goes. On the other hand, staff administration activities including staff recruitment and supervision, performance appraisal, promotion and disciplinary actions, remuneration and reimbursement for claims, etc. are also prone to abuse and corruption if they are not properly managed. Sound staff administration policies and measures are essential in maintaining an effective and efficient work force and conducive to promoting a clean business culture in the bank (Reference at ***Section 2.2*** of ***Chapter 2***).

This Chapter highlights the major risks and provides corresponding recommended measures in the procurement and staff administration processes. Given the increasing trend to use technologies for internal control, streamlining and enhancing efficiency (Reference at ***Section 3.3.10*** of ***Chapter 3***), the corruption prevention safeguards as recommended in this Chapter also cover adoption of technologies where appropriate.

7.2 KEY PROCESSES

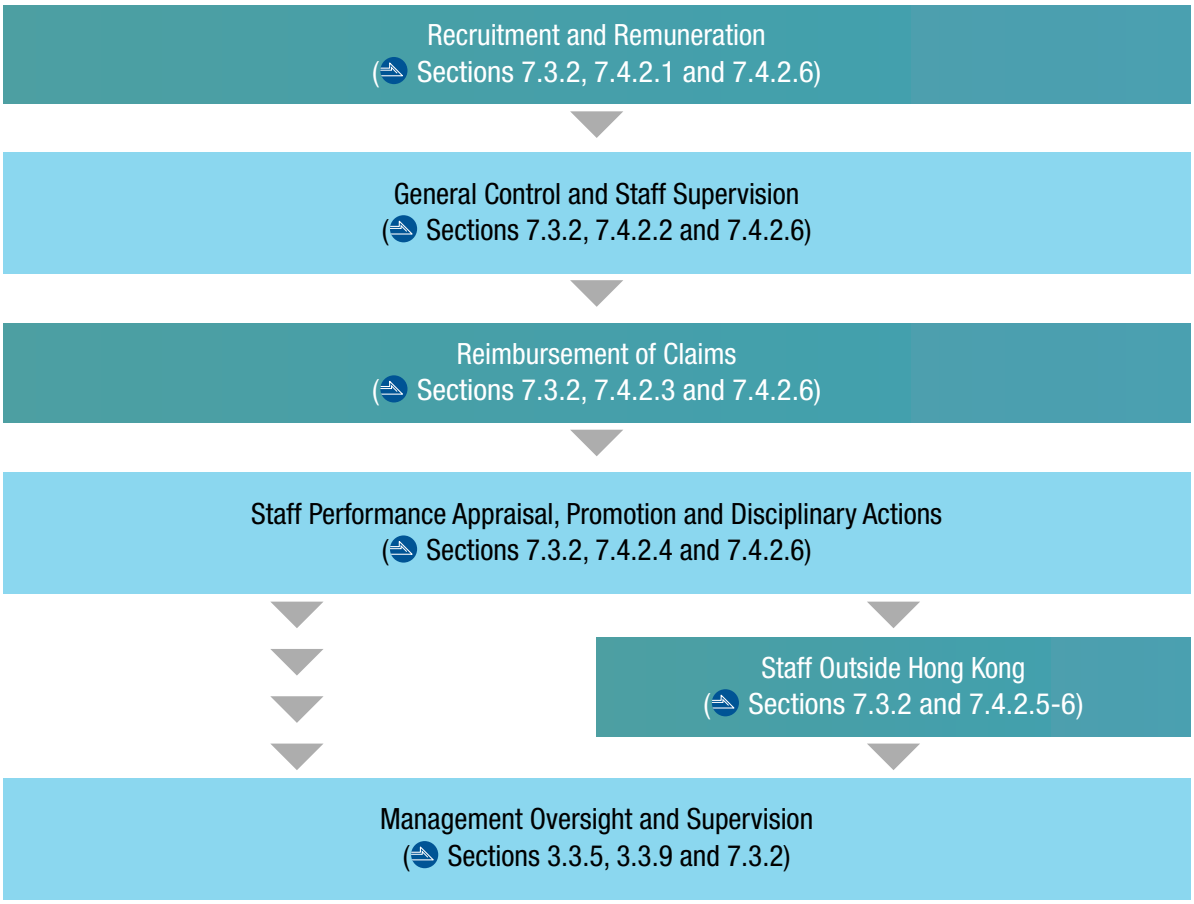
7.2.1 PROCUREMENT

The following flow chart illustrates the key procedures in procurement -



7.2.2 STAFF ADMINISTRATION

The following flow chart illustrates the key procedures in staff administration –



7.3 MAJOR CORRUPTION RISKS AND RED FLAGS

MAJOR CORRUPTION RISKS

7.3.1 PROCUREMENT

- Colluded bank staff soliciting/accepting advantages from suppliers / service providers for inappropriately including them (who may be unqualified) in the invitation to bid, divulging to them sensitive information (e.g. other bidders' quotations) or inside information (e.g. specific requirements/expectations not disclosed to other bidders), favouring them in quotation/tender evaluation, etc.
- Dishonest bank staff failing to declare their relationship with the suppliers / service providers (e.g. close relative, shareholding in the company) with a view to favouring them in the procurement process.
- Dishonest bank staff soliciting/accepting advantages from suppliers / service providers for placing excessive orders with them, inflating quantity provided or price, circumventing normal purchase procedures or approving authorities through splitting of orders, or colluding with them to purchase items for personal use in particular for banks where procurement is decentralised and determined by staff of individual office/branch.
- Unscrupulous bank staff colluding with suppliers / service provider to fabricate competitive quotations purported to be submitted by other bidders, or discard other bidders' quotations.
- Compromised bank staff soliciting/accepting advantages from suppliers / service providers for turning a blind eye to their poor performance or renewing the contract repeatedly without going through any competitive process.
- Given the increasing use of technology by banks, banks possibly procuring more goods (e.g. hardware, IT systems) and services (e.g. IT infrastructure maintenance) in this aspect, or procuring tailor-made goods/services (e.g. tailor-made Regtech solutions to suit the bank's operations) which may not have open market value for reference, and hence relying on bank staff who have technology/specialist knowledge to conduct and monitor the procurement process. Over reliance on individual staff in the procurement process and lack of open market value of the procured goods/services may make them more vulnerable to the above corruption risks.

- With the globalisation and technological advancement, it has become increasingly common to outsource banking functions/activities (e.g. back-office operations) to service providers within/outside Hong Kong. Besides, banks may engage service providers to facilitate their business operations (e.g. engage intermediaries/agents on mergers and acquisitions transactions, hire purchase agreements, corporate business finance). Given that the staff/agents who work on behalf of the service providers as well as the operations are not directly supervised and monitored by the bank, the relevant corruption risks may also increase. Any malpractices arising from these service providers may also damage the bank's reputation.

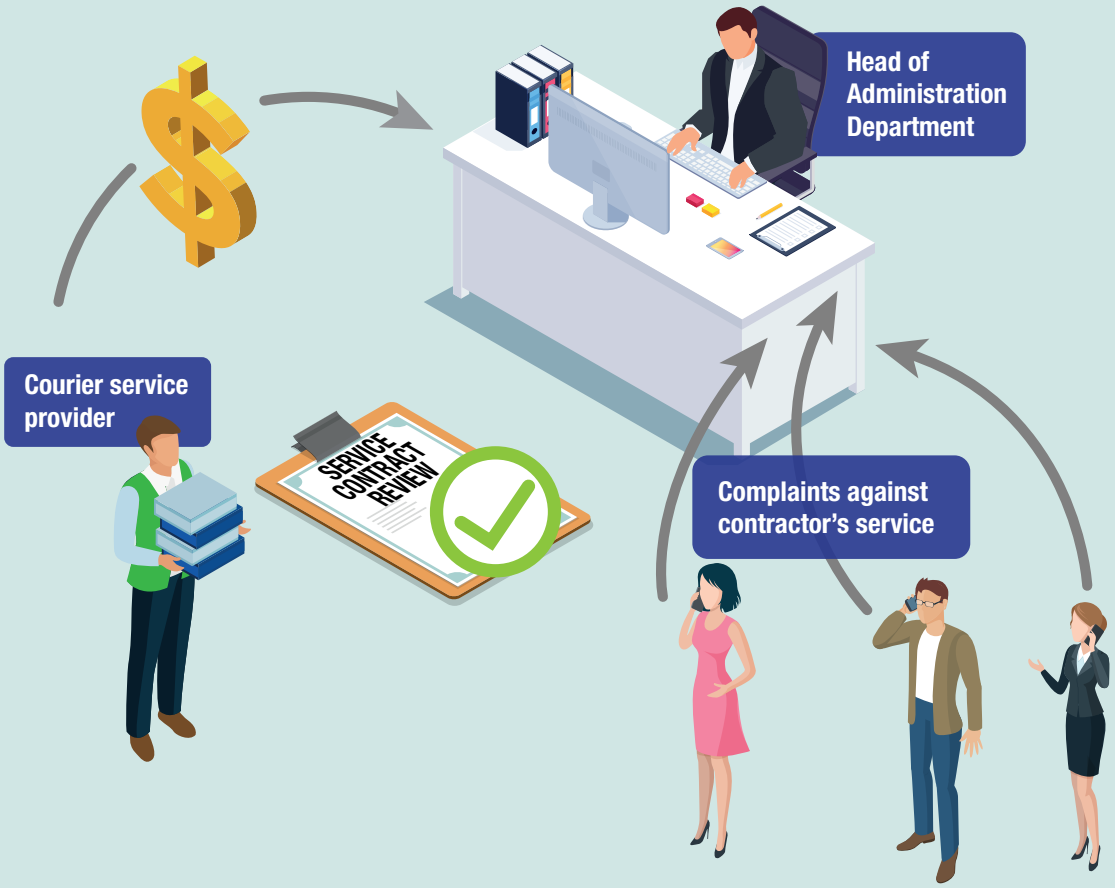
Case Study 1 – Acceptance of Advantages for Assistance in Service Contract Renewal

1 The head of administration department of a bank (Bank A) is responsible for engaging courier service provider. The incumbent service provider has been the sole service provider for Bank A for many years and the department head gets acquainted with its director.

2 During the term of service contract, the department head receives many complaints about the substandard service (e.g. late delivery) of the courier company. As Bank A neither has policies/procedures on handling of complaints against contractor nor a contractor performance evaluation mechanism, the department head connives at the substandard services of the company and takes no actions against the complaints.

3 When the contract is about to expire, the director of the courier company offers money to the department head and requests him to favour the company in renewing the service contract, to which the department head agrees. During the procurement exercise, the department head draws up biased service specifications to favour the incumbent service provider (e.g. requiring work experience in banking, not specifying time limit for delivery). He also tips off other bidders' price to the director.

4 The department head of Bank A and director of the courier company may respectively contravene Sections 9(1) and 9(2) of the POBO.



Analysis and Points to Note –

- Some dishonest bank staff might connive at substandard contractors by making no reports to the management of and taking no actions against under-performance by contractors for bribe. They might also favour a particular bidder during the procurement exercise for corrupt return. Bank staff must be cautious in handling relationship with suppliers and service providers as such close relationship may constitute an actual/potential conflict with the bank staff's monitoring role over them.

- Such contravention of the POBO and commission of other related offences by the parties concerned will result in the bank suffering from such poor performance provided and high service fees paid. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.9*** and ***7.4.1***.

Case Study 2 – Connivance of Substandard Renovations Outside Hong Kong

1 A bank (Bank B) plans to renovate its branch network outside Hong Kong and assigns a staff member to be the project manager to station there to oversee the renovation project. During the course of the project, a Hong Kong contractor responsible for the renovation keeps offering the project manager entertainment and free trips.

2 In examining the renovation of the first branch, the project manager finds the workmanship and materials sub-standard. The contractor "reminds" the project manager of the entertainment and free trips provided, and further remits money to the project manager's bank account in Hong Kong for recommending to the bank's head office in Hong Kong to continue to appoint him to renovate other branches. As its general practices, Bank B mainly relies on the project manager to oversee the renovation work outside Hong Kong without any supervisory/independent checks. Knowing Bank B's practices, the project manager accepts the advantage, conceals the fact of substandard work and makes favourable comments on the performance of contractor to Bank B, which accepts the comments and awards further contracts to the contractor without verification by his supervisor or an independent party.

3 The project manager and contractor may respectively contravene Sections 9(1) and 9(2) of the POBO.

Analysis and Points to Note –

- Procurement of goods and services is one of the most corruption-prone business processes in all trades/industries, in particular those involving specialist knowledge and/or specialised services (e.g. renovation works). Some unscrupulous contractors might offer advantages to the subject bank staff for securing a contract or conniving at its substandard performance. The risks are heightened if such work is conducted outside Hong Kong due to the perceived remoteness and absence of daily monitoring of the bank staff.
- Such contravention of the POBO and commission of other related offences by the parties concerned will result in the bank suffering from such poor performance provided and high service fees paid. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.5, 3.3.9*** and ***7.4.1***.

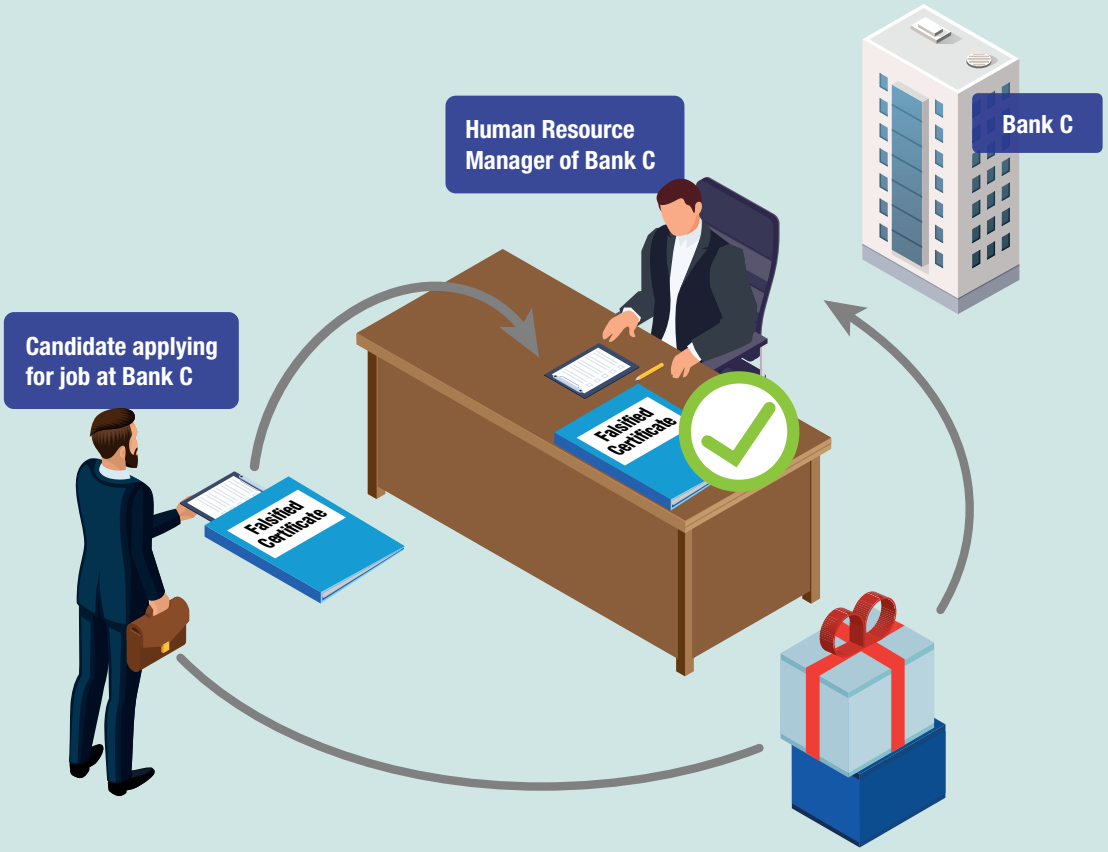
7.3.2 STAFF ADMINISTRATION

- Colluded bank staff soliciting/accepting bribe for concealing false academic / work experience proof submitted by candidates for a job.
- Unscrupulous bank staff referring job applicants to the bank for bribe (e.g. solicit referral fee from job applicants).
- Dishonest bank staff responsible for recruitment/promotion favouring a candidate during the recruitment/promotion process, or offering a favourable remuneration package upon receipt of bribe or without making proper declaration where necessary (e.g. close relationship with the candidate).
- Compromised supervisors soliciting/accepting advantages from subordinates in return for conniving at their substandard performance or favouring them in allocation of duties.
- Dishonest bank staff making false reimbursement claims (e.g. using bogus receipts) or reimbursement claims for private purpose (e.g. claiming reimbursement for dinner with personal friends purporting to be duty-related) (Reference at ***Case Study 2*** of ***Chapter 1***).
- Unscrupulous bank staff offering job vacancy including internship at bank as a bribe for seeking business opportunities.

Case Study 3 – Provision of False Academic Proof for Bank Employment

1 A candidate applies for the position of relationship manager in a bank (Bank C). He submitted his resume stating that he had attained a business degree from a university with a certificate issued by the university as supporting document. He however is not graduated from the university and the certificate is forged.

2 The human resource manager of Bank C is a friend of the candidate. The candidate offers a gift to the manager to conceal his background and accept the falsified certificate. As its general practices, Bank C relies on the human resource manager to check the originals of the applicants' academic certificates and sign to certify true copies of the documents, without verifying the authenticity of the academic certificates by an independent staff or with the document issuing institutions. Having believed that the candidate was a graduate of the university, Bank C hires the candidate as a relationship manager.



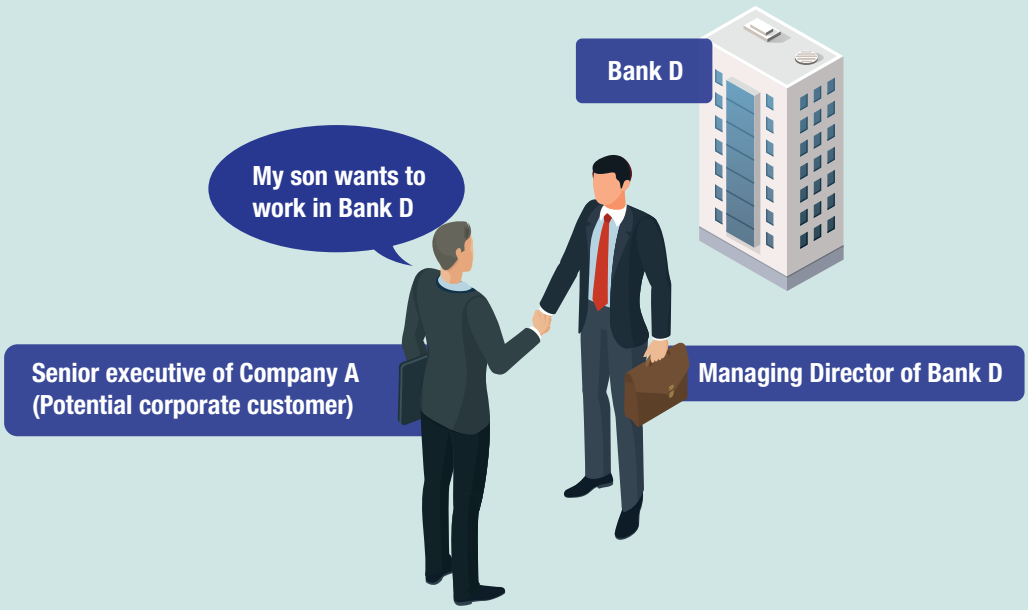
3 The human resource manager and the candidate may respectively contravene Sections 9(1) and 9(2) of the POBO. The human resource manager may also commit Section 9(3) of the POBO.

Analysis and Points to Note –

- Some devious candidates might submit falsified academic certificate / work experience proof to obtain a job at banks. They may resort to corrupt means for assistance by bank staff to conceal their malpractice.
- Such contravention of the POBO and commission of other related offences by the parties concerned will adversely affect the reputation of the bank, leading to recruitment of underqualified and unethical staff. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.5, 3.3.9, 7.4.2.1-2*** and ***7.4.2.6***.

Case Study 4 – Offer of Job Opportunity in Return for Business Opportunities to Boost up Sales Target

1 A managing director of a bank (Bank D) heads the sales department and is granted with the authority to recommend interns for Bank D. During a business event, a senior executive of a company (Company A) which is a potential corporate customer to Bank D, indicates to the managing director that his son is interested in working as an intern in Bank D.



2 To attract potential business from Company A, the managing director recommends to offer an internship to the senior executive's son and explicitly mentions business expectation to him in return. Although Bank D has policies in place over hiring of interns (e.g. clear guidelines on appointing interns including the requirement for the interns to meet the academic qualifications, requiring the staff to declare conflict of interest including business relationship with the interns / their close associates), it does not have adequate controls on verifying the compliance with the established requirements. Knowing Bank D's practice, the managing director arranges the human resource department to hire the senior executive's son as an intern who actually cannot meet the stipulated qualification requirements of Bank D, in return for subsequent investment by the senior executive, which enables the managing director to meet his sales target of the month.

3 The senior executive and the managing director of Bank D may respectively contravene Sections 9(1) and 9(2) of the POBO.

Analysis and Points to Note –

- Some dishonest bank staff might misuse their authority to offer job opportunities of the bank, in return for business opportunities which is considered as an advantage under the POBO (Reference at ***Section 1.2.1*** of ***Chapter 1***). While banks may put in place a mechanism for declaration of conflict of interest by staff, staff who fails to make proper and true declaration may risk himself committing an offence under the POBO or other possible offence.
- Such contravention of the POBO and commission of other related offences by the parties concerned will adversely affect the reputation of the bank. If controls are inadequate in the bank, this would create opportunities and temptation for exploitation by the dishonest parties concerned. In order to deter/detect such malpractices in the above process, banks are advised to adopt the recommended practices as provided in ***Sections 3.3.9***, ***7.4.2.1-2*** and ***7.4.2.6***.

Red Flags

1. **Malpractices in Procurement**

   (a) **Use of a particular brand/supplier** – Staff member insists on using a particular brand/supplier without objective justifications.

   (b) **Exceptions** – Staff member frequently uses exceptions or urgent purchases to bypass stipulated procedures and controls (e.g. frequent use of single quotation / direct purchase method).

   (c) **Suspicious signs on quotations** – Suspicious signs (e.g. supplier's name very similar to another more well-known one, vendor's contact information matches that of a bank staff or with no information except a mobile phone number, common mistakes/typos on quotations from two or more vendors) are noted on quotations or quotation invitation list.

2. **Malpractices in Staff Administration**

   (a) **Staff member refusing others to handle his work** – Staff member refuses to take vacation leave or refuses others to take up his work during his vacation leave or block leave.

   (b) **Abusing authority and deviating from normal procedures without justifications** – Staff member with the relevant authority hires a candidate without going through the established procedures and without justifications.

7.4 CORRUPTION PREVENTION SAFEGUARDS

7.4.1 PROCUREMENT

- The CPD of ICAC has separately developed a publication "Best Practice Checklist on Procurement". The relevant key processes on procurement of goods and services, covering sourcing suppliers, inviting quotations/tenders, awarding/managing contracts, receiving goods/services, etc, and the recommended practices / corruption prevention safeguards are included in the publication for organisations' adoption subject to their respective organisational structure, resource capability, operational need, and risk exposure. Banks can make reference to the publication which is available at the following webpage –

  cpas.icac.hk/EN/Info/Lib_List?cate_id=3&id=199

  The relevant corruption prevention safeguards which are not covered in the above publication and specific to the banking sector are highlighted in the following sections.

7.4.1.1 Handling of Personal Data and Confidential Information

- For procurement of goods/services involving access to personal data or confidential information of the bank (e.g. developing/maintaining technology infrastructures), banks should ensure that –
  - personal data and confidential information of the bank are disclosed to suppliers / service providers on a need-to-know basis for services undertaken by them;
  - the bank (including external and internal auditors or other agents appointed by the bank) has full access to relevant business records/documents for audit checks on the suppliers / service providers and their sub-contractor (if any);
  - the suppliers / service providers are required to submit report on security, control or other aspects regularly or upon request; and
  - the suppliers / service providers and their sub-contractors (if any) have put in place adequate security safeguards.

7.4.1.2 Performance Monitoring

- Conduct effective performance monitoring (e.g. set up key performance indicator matrix to monitor/measure the performance of suppliers / service providers) to ensure that poor performance is not connived at by compromised staff and that such supliers / service providers are not eligible for future bidding.

- Handle cases of unsatisfactory performance of suppliers / service providers in accordance with established policies and procedures (e.g. issue of warning, suspension from invitation to bid for a specified period, removal from suppliers list). (*Use of Technology*).

Use of Technology

Banks may consider -

☑ using technologies to enhance monitoring over vendors'/contractors' performance (e.g. data analytics to collect and analyse data from different users/sources to assess the performance on a continuous basis and facilitate retrieval of their track records, to provide a portfolio management view of vendors'/contractors' relationship with the bank, etc).

7.4.1.3 Procurement Outside Hong Kong

- Ensure some important processes (e.g. recommendation, approval) are carried out in Hong Kong although some business/transactions need to be conducted outside Hong Kong.
- Communicate to suppliers / service providers, in particular the non-local ones, the bank's anti-bribery and acceptance of advantages/entertainment policy, stance of zero-tolerance to corruption, and provide channel for feedback/enquiry.
- Enhance safeguards for procurement outside Hong Kong (e.g. conduct supervisory checks, require proof such as photos for inspection) to ensure that such procurement would not lead to an increase in risk or impair the ability of competent authorities to supervise the performance.

7.4.1.4 Staff Training

- Provide regular training to staff, in particular those from user departments, to enhance their understanding on and compliance to the procurement guidelines and procedures.

7.4.1.5 Engagement of Service Providers

- For outsourcing contractors and important service providers (e.g. services performed to comply with obligations as a regulated entity), conduct due diligence checks (e.g. corporate governance, financial strength, security and internal controls, capability, expertise and experience, required regulatory authorisations or registrations) on selected service provider before engagement to ensure their capability to execute the contract as pledged.

- Require suppliers / service providers to establish mechanisms and practices to ensure business integrity (e.g. code of conduct for staff members and its promotion) and compliance to regulatory requirements, if any.
- Review and monitor the security practices and control measures of the service providers regularly (e.g. audit, expert report on confidentiality, security adequacy and compliance) if necessary.

7.4.2 STAFF ADMINISTRATION

- The CPD of ICAC has separately developed a publication "Best Practice Checklist on Staff Administration". The relevant key processes on staff administration, covering staff recruitment, remuneration package, staff supervision and promotion, etc, and the recommended practices / corruption prevention safeguards are included in the publication for organisations' adoption subject to their respective organisational structure, resource capability, operational need, and risk exposure. Banks can make reference to the publication which is available at the following webpage –

  cpas.icac.hk/EN/Info/Lib_List?cate_id=3&id=220

  The relevant corruption prevention safeguards which are not covered in the above publication and specific to the banking sector are highlighted in the following sections.

7.4.2.1 Recruitment and Remuneration

- Assign independent staff or appoint an external agent to vet all applications against entry requirements, and verify applicants' qualifications against reliable documents/records and independent source of information (e.g. licence information from the SFC).
- Appoint a recruitment panel (comprising senior staff of the concerned department and human resource department), or subject to the level of staff recruited, arrange few rounds of interviews involving different departments.
- For selected applicant with appointment may give rise to conflict of interest with the bank (e.g. relative of potential business partner of the bank), require additional vetting by independent compliance team.
- Conduct reference checks with former and current employers of the selected candidates including integrity and conduct[34].

[34] *The HKMA has endorsed the Mandatory Reference Checking Scheme which requires authorized institutions to obtain conduct-related information of a prospective employee from his former and current authorized institution employers. Such information includes (i) breach of legal or regulatory requirements; (ii) incidents which cast doubt on an individual's honesty and integrity; (iii) misconduct reports filed with the HKMA; (iv) internal or external disciplinary actions arising from conduct matters; and (v) ongoing internal investigations.*

Referral of Candidates by Bank Staff

- Require a referrer/candidate to declare their relationship, including any relevant official dealings / business relationships.
- Exercise the same vigilance and independence when handling the job application from a referee of a bank staff member as that of other candidates recruited openly or from other source (e.g. recruitment agency).
- If practicable, avoid arranging a staff to work under the supervision of his referrer to avoid conflict of interest, or review the entitlement of referral commission by such referrers.

Remuneration

- Determine the scale and weighting for adjustment of salary. Reward staff for non-financial performance (e.g. diligence, honesty, ethics) to motivate probity behaviour and reinforce a clean business culture (e.g. probity behaviour has a weighting in salary adjustment) (Reference at ***Section 2.2*** of ***Chapter 2***).
- Lay down the criteria and authorities for the consideration and approval of remuneration packages (including allowance, fringe benefits and other benefits) to be offered to different ranks of staff, taking into account the latter's qualifications, work experience, expertise, etc.

7.4.2.2 General Controls and Staff Supervision

- Establish a fair and transparent mechanism for the allocation of duties and customers.
- Stay alert to undesirable behaviours and misconduct, sudden change of staff member's lifestyle (i.e. to a luxury one) or financial condition (e.g. in debt, suspicious transaction in bank account) as well as close relationship (e.g. financial dealing) between bank staff and customer / third party having business dealing with the staff (e.g. contractor), and initiate enquiries if necessary; or conduct regular due diligence checks on staff members in particular those with sensitive duties (e.g. credit approval) (***Use of Technology***).
- Subject to legislative/regulatory exception, require staff to timely report to the bank of any investigation, including the progress and results, by any law enforcement agencies / regulators against the staff (e.g. HKMA, SFC) for matter in relation to business of the bank and nature of his duty (e.g. investigation in relation to his former employment). The bank should take appropriate follow-ups or measures to prevent the staff from breaching the rule or regulation, and getting access to sensitive information.

Use of Technology

Banks may consider –

- ☑ using technologies (e.g. machine reading, artificial intelligence) to detect undesirable behaviour and monitor misconduct more efficiently and effectively (e.g. different communication tools to uncover suspicious communication / relationships of bank staff) and to conduct surveillance across different channels.
- ☑ computerising and automating the staff administration process to facilitate efficient and prudent management, compliance with the established policies/procedures by the staff in recruitment, declaration and management of conflict of interest, performance appraisal, documentation of the staff engaged throughout the process and their actions taken to enhance accountability, keeping dossier of exceptional engagement cases for general reference, etc.

7.4.2.3 Reimbursement of Claims

- Require staff to claim reimbursement by using a prescribed voucher to provide necessary information (e.g. name of customer met) and attach the original invoices or receipts duly certified by a supervisor.
- Set a ceiling for various kinds of entertainment reimbursement (e.g. meal expense per head), and if exceeded, require additional scrutiny by supervisor.
- Evaluate the reasonableness of reimbursement submitted by staff (e.g. check against sales turnover, number of customers handled by the staff, customer meeting records).

7.4.2.4 Staff Performance Appraisal, Promotion and Disciplinary Action

- Devise an appraisal form covering the core competencies, which covers both financial and non-financial performance, for each rank or post to be assessed. Require appraisal reports to be completed by the immediate supervisor and counter-signed by a more senior staff member.
- Assess all eligible candidates based on pre-determined and objective criteria for promotion, with reference to their appraisal reports for a specified period of time by an assessment panel.

- Maintain proper records of disciplinary actions taken to uphold accountability in the process, ensure consistency of decision and for audit / reference check purpose.
- Make available a channel for aggrieved staff to seek review of the decision on promotion / disciplinary action taken against them.

7.4.2.5 Staff Outside Hong Kong

- Given the rise of globalisation and cross-boundary business, banks may assign local staff to work outside Hong Kong (e.g. performing site inspection for credit assessment at overseas factory). The risks of impropriety are heightened due to the perceived remoteness and absence of daily monitoring of the bank staff. On the other hand, banks may also designate staff of its banking group worldwide to undertake duties for Hong Kong branch in their local office (e.g. attestation service for opening Hong Kong bank account). Such staff may not be familiar with the legislative and regulatory requirements in Hong Kong. To ensure compliance of these requirements and integrity of the relevant work process, banks should –
  - ensure that the staff understand the policies, procedures and requirements of the work process through various means (e.g. training, circulation of guidelines);
  - publicise the details of function/responsibility to perform Hong Kong-related services undertaken by non-local branches/offices;
  - on a risk basis, tighten up the monitoring and supervision on the work process (e.g. regular checks conducted by Hong Kong staff); and
  - other controls stipulated in this Guide on relevant functions are also applicable.

7.4.2.6 Staff Training

- Provide regular training to bank staff to –
  - enhance their understanding on and compliance to the procedures and guidelines of staff administration process; and
  - sharpen supervisors' management and oversight skills (e.g. staying alert to red flags in operations/staff behaviour, supervisory accountability, assessing performance of subordinates).

8 ICAC SERVICE AND ASSISTANCE

8.1 INTRODUCTION
8.2 CORRUPTION PREVENTION ADVISORY SERVICES
8.3 EDUCATION SERVICES
8.4 REPORTING CORRUPTION

8 ICAC SERVICE AND ASSISTANCE

8.1 INTRODUCTION

The ICAC stands ready to help banks establish, strengthen and continually improve their anti-corruption controls/programmes that cater for their operational needs. The channels for reporting cases of suspected corruption are also provided in the below paragraphs.

8.2 CORRUPTION PREVENTION ADVISORY SERVICES

- The CPAS of the CPD, ICAC which has compiled this Guide is a specialised unit that focuses on providing the following **free** professional corruption prevention advice and services to private organisations and business companies –
  - providing **confidential** and **tailor-made** advice on anti-corruption management systems including the adoption of the recommended measures in the Guide; and corruption prevention measures for specific business operations (See ***Qs & As*** below) on request;
  - offering assistance in drawing up a Code of Conduct for the directors and staff (Reference at ***Section 2.3*** of ***Chapter 2***) and other probity guidelines (e.g. corporate policy/guidelines on reporting corruption and anti-corruption commitment across territories) that will help them comply with anti-corruption requirements as well as raise the company's integrity standard;
  - organising corruption prevention training for banks to raise their directors'/staff's awareness of corruption risks and corruption prevention measures specific to their business operations; and
  - answering any enquiries about this Guide.
- For further information, please contact the CPAS through the following channels –

Phone:	2526 6363
Fax:	2522 0505
E-mail:	*cpas@cpd.icac.org.hk*
Website:	*cpas.icac.hk*

Q10. In what areas can the CPAS render advice for a bank?

A The service will cover a bank's anti-corruption management system, including its anti-corruption policy, ethical standard and anti-corruption guidance for all bank personnel (e.g. through a Code of Conduct for directors and staff), identification and assessment of corruption risk, anti-corruption controls, training and communication; and specific systems and procedures such as bank account opening process, sales process, approval for credit facilities and general operational areas (e.g. procurement, staff administration, inventory management, contract management).

Q11. Will the CPAS disclose our service request and other information (e.g. our policies, procedures, risks, concerns, incidents) to others / the public?

A No. Our services are provided in strict confidence to protect clients' information unless individual clients are willing to share their experience of using the services of the CPAS so as to assist in promoting the services. Your bank has full discretion to decide on the information to be given to us.

8.3 EDUCATION SERVICES

- The Hong Kong Business Ethics Development Centre (HKBEDC) of the ICAC's Community Relations Department strives to promote business and professional ethics in Hong Kong on a long-term basis. Its services for the banking industry include –
  - offering anti-corruption and ethics training to banks and financial institutions to promote ethical corporate culture and good governance;
  - organising seminars, workshops and Continuing Professional Development courses with industry bodies and on the *BEDC Channel* (*hkbedc.icac.hk/en/services/bedc_channel*) to enhance business and professional ethics of banking practitioners;
  - producing training materials on anti-corruption laws and integrity management for the industry; and
  - maintaining a *Banking and Finance* thematic webpage (*hkbedc.icac.hk/en/sector_industry/banking_and_finance*) on the HKBEDC website (*hkbedc.icac.hk*) to provide an online repository of education resources and training materials for use by financial and banking practitioners.

- The HKBEDC also maintains a Corruption Prevention Network for Banks (Banking Network) to foster co-operation and exchange of information among bank managers on integrity promotion and corruption prevention. Members of the Banking Network will receive the latest anti-corruption news, updates on ICAC cases, e-newsletters, as well as information on new education resources, training activities and members' exclusive events. Bank managers from training, human resources, legal & compliance departments are welcome to *join the Banking Network* (*hkbedc.icac.hk/enewsletter/bank-bulletin/*).

- For further details, please contact the HKBEDC or visit its website –

Phone:	2826 3288
Fax:	2519 7762
E-mail:	*hkbedc@crd.icac.org.hk*
Website:	*hkbedc.icac.hk*

8.4 REPORTING CORRUPTION

- Reporting corruption in person is more direct and allows the ICAC to get more details of the corruption complaint. Complainant's identity and content of complaint are handled in strict confidence.

- Full evidence is not required when lodging a complaint. One may report if he has reasonable doubt. Complainants only need to state the known facts of the suspected case and the ICAC will follow up according to the information provided.

- Any person encountering corruption should make a report to the ICAC through any of the following channels –

Phone:	25 266 366 (24-hour service)
Mail:	G.P.O. Box 1000, Hong Kong
In person:	ICAC Report Centre (24-hour service) G/F, 303 Java Road, North Point, Hong Kong ICAC Regional Offices[35] (opening hours: 9:00 a.m. - 7:00 p.m. Monday to Friday; closed on Saturdays, Sundays and public holidays)

[35] *Contact information of the ICAC Regional Offices is available at www.icac.org.hk/en/crd/struct/ro/index.html.*

APPENDICES

Sample Code of Conduct *(for Reference Only)*[36]

(Name of Bank)

Ethical Commitment

1. The *(name of bank)* (hereafter referred to as the Bank) regards honesty, integrity and fair play as our core values that must be upheld by all directors and staff[37] of the Bank at all times. This Code sets out the basic standard of conduct expected of all directors and staff, and the Bank's policy on acceptance of advantage and handling of conflict of interest when dealing with the Bank's business.

Prevention of Bribery

2. The Bank prohibits all forms of bribery and corruption. All directors and staff are prohibited from soliciting, accepting or offering any bribe in conducting the Bank's business or affairs, whether in Hong Kong or elsewhere. In conducting all business or affairs of the Bank, they must comply with the Prevention of Bribery Ordinance (POBO) of Hong Kong and must not:

   (a) solicit or accept any advantage from others as a reward for or inducement to doing any act or showing favour in relation to the Bank's business or affairs, or offer any advantage to an agent of another as a reward for or inducement to doing any act or showing favour in relation to his principal's business or affairs;

   (b) offer any advantage to any public servant (including government / public body employee) as a reward for or inducement to his performing any act in his official capacity or his showing any favour or providing any assistance in business dealing with the government department / public body; or

   (c) offer any advantage to any staff of a government department or public body while they are having business dealing with the latter.

   (The relevant provisions of the POBO are at ***Annex 1***.)

[36] *Internal Remarks for Banks: In devising its code of conduct, the Bank may wish to make adaptations of this Code to suit its core values and operational needs while adopting the principles of the recommended guidelines.*

[37] *"Staff" cover full-time, part-time and temporary staff, except where specified.*

Acceptance of Advantage

3. It is the Bank's policy that directors and staff should not solicit or accept any advantage for themselves or others, from any person, company or organisation having business dealings with the Bank or any subordinate, except that they may accept (but not solicit) the following when offered on a voluntary basis:

   (a) advertising or promotional gifts or souvenirs of a nominal value;

   (b) gifts given on festive or special occasions, subject to a maximum limit of $_____ [38] in value; and/or

   (c) discounts or other special offers given by any person or company to them as customers, on terms and conditions equally applicable to other customers in general.

4. Gifts or souvenirs described in paragraph 3(a) that are presented to directors and staff in official functions are deemed as offers to the Bank. The directors and staff concerned should report the acceptance to the Bank and seek direction as to how to handle the gifts or souvenirs from *(the approving authority)* [39] using Form A (***Annex 2***). If a director or staff member wishes to accept any advantage not covered in paragraph 3, he should also seek permission from (the approving authority) using Form A.

5. However, a director or staff member should decline an offer of advantage if the acceptance could affect his objectivity in conducting the Bank's business or induce him to act against the interest of the Bank, or the acceptance will likely lead to perception or allegation of impropriety.

6. If a director or staff member has to act on behalf of a client in the course of carrying out the Bank's business, he should also comply with any additional restrictions on acceptance of advantage that may be set by the client (e.g. directors and staff members performing any duties under a government or public body contract will normally be prohibited from accepting advantages in relation to that contract).

7. *[Internal Remarks for Banks: The Bank may remind its directors and staff on the Bank policy for referral of customers to any other banks or financial institutions. In particular, directors and staff should be prohibited from soliciting or accepting advantages (e.g. referral fee) for referring a customer to any other banks or financial institutions without the prior approval of the Bank as this might constitute an offence under the POBO (para. 2). Even the referral might not involve an advantage, they should be made aware that such referrals without proper declaration to the Bank and prior approval of the Bank as required might also constitute a conflict of interest or misuse of their official position (paras. 11&15).]*

[38] *Internal Remarks for Banks: The Bank can set the appropriate maximum limit of the value of the gifts allowable to be accepted after taking into account its operational needs. Yet, a modest amount should be set as the maximum limit to prevent directors and staff from falling prey to corruption.*

[39] *Internal Remarks for Banks: Please specify the post of the approving authority in the Code and the Form. The Bank can designate the appropriate approving authority after taking into account its operational needs and organisation structure.*

Offer of Advantage

8. Directors and staff are prohibited from offering advantages to any director, staff member or agent of another bank or organisation, for the purpose of influencing such person in any dealing, or any public official, whether directly or indirectly through a third party, when conducting the Bank's business. Even when an offer of advantage carries no intention of improper influence, it should be ascertained that the intended recipient is permitted by his employer/principal to accept it under the relevant circumstance before the advantage is offered.

Entertainment

9. As defined in Section 2 of the POBO, "entertainment" refers to food or drink provided for immediate consumption on the occasion, and any other entertainment provided at the same time. Although entertainment is an acceptable form of business and social activity, a director or staff member should avoid accepting lavish or frequent entertainment from persons with whom the Bank has business dealing (e.g. suppliers) or from his subordinates to avoid placing himself in a position of obligation.

Records, Accounts and Other Documents

10. Directors and staff should ensure that all records, receipts, accounts or other documents they submit to the Bank give a true representation of the facts, events or business transactions as shown in the documents. Intentional use of documents containing false information to deceive or mislead the Bank, regardless of whether there is any gain or advantage involved, may constitute an offence under the POBO.

Conflict of Interest

11. Directors and staff should avoid any conflict of interest situation (i.e. situation where their private interest conflicts with the interest of the Bank) or the perception of such conflict. When an actual or a potential conflict of interest arises, the director or staff member should make a declaration to (the approving authority) through the reporting channel using Form B (***Annex 3***).

    *[Internal Remarks for Bank: The Bank may wish to include some common examples of conflict of interest as appropriate (Reference at **Appendix 2**).]*

Granting Credit

12. Directors and staff must not grant credit to himself, his relatives or companies in which he or his relatives has a personal interest. Directors and staff must make a declaration to (*the approving authority*) in accordance with paragraph 11 if they come across any application that is submitted by such individual/company. (*The approving authority*) should consider such notification and manage potential/actual conflict of interest identified.

Personal Investments

13. Directors and staff must not deal in the shares or other securities of any listed companies when possessing privileged or price-sensitive information that is not generally known to other investors and to the public. Directors and staff must not disclose such information to any third party.

14. Directors and staff must notify (*the approving authority*) immediately in writing of the details of any dealings in which they may have been inadvertently concerned in the shares or other securities of any listed companies of which they possess privileged or price-sensitive information. (*The approving authority*) should consider such notification and manage potential/actual conflict of interest identified or take action as appropriate.

Safeguard of Bank Assets / Information and Customer Funds

15. Directors and staff must not misuse their official position in the Bank to pursue their own private interests, which include both financial and personal interests and those of their family members, relatives or close personal friends.

16. Directors and staff in charge of or having access to any bank assets, including funds, property, information, and intellectual property, should use them solely for the purpose of conducting the Bank's business. Unauthorised use, such as misuse for personal interest, is strictly prohibited. Directors and staff having access to customer funds must also make sure they are handled in a trustworthy and honest manner.

17. Directors and staff should not disclose any classified information of the Bank (e.g. information about the customers, business partners) without authorisation or misuse any bank information. In particular, unauthorised sale of information or disclose of information that might be of use to other business operators or companies in competition with the Bank's business is strictly prohibited. Those who have access to or are in control of such information, including information in the Bank's computer system, should protect the information from unauthorised disclosure or misuse.

Outside Employment/Work

18. If a director or staff member wishes to take up employment/work outside the Bank, he must seek the prior written approval of *(the approving authority)*. *(The approving authority)* should consider whether the outside employment/work would give rise to a conflict of interest with the staff member's duties in the Bank or the interest of the Bank.

Relationship with Suppliers/Contractors, Other Business Partners and Customers

Business Practices of Suppliers/Contractors

19. Directors and managerial staff responsible for managing suppliers/contractors should be aware of their business practices to ensure that proper and prudent methods are adopted to deliver the Bank's services.

Loans

20. Directors and staff should not borrow or receive credit from third parties on a favoured basis or on terms other than at arm's length. Directors and staff should not accept any loan from, or through the assistance of, any individual or organisation having business dealings or seeking business opportunities with the Bank.

    [Internal Remarks for Banks: The above are not exhaustive. The Bank may wish to include other guidelines on the conduct required of directors and staff in their dealings with suppliers, contractors, customers, and other business partners as appropriate.]

Policy on Reporting of Suspected Corruption and other Criminal Offences

21. The Bank maintains a policy to handle reports of misconduct and criminal offences including corruption. A director or staff member should himself/herself or through the Bank (the appropriate channels including the names of the handling officer(s) and office(s)) report instances of crime or suspected crime discovered in the course of his/her work, including attempt to bribe himself/herself, to (the appropriate authority) of the Bank or law enforcement agencies / industry regulators at the first practicable opportunity. Upon making or receipt of such reports, the reporting and handling staff as appropriate should avoid making any enquiries or taking any action that may hinder or jeopardise subsequent investigation by the law enforcement authority concerned. All directors and staff members who make, receive or have knowledge of such reports should treat the reports in the strictest confidence.

    [Internal Remarks for Banks: the Corruption Prevention Department can offer assistance in compiling a corporate policy on reporting of corruption upon request.]

Compliance with Laws of Hong Kong and in Other Jurisdictions

22. Directors or staff must comply with all local laws and regulations when conducting the Bank's business, and also those in other jurisdictions when conducting business there or where applicable.

    [Internal Remarks for Banks: The Corruption Prevention Department can assist in providing broad principles/guidelines when the Bank compiles its corporate policy on anti-corruption commitment across territories.]

Compliance with Professional Standards and Regulatory Requirements

23. [Internal Remarks for Banks: There are a number of professional standards and regulatory requirements in relation to the conduct of bank business (e.g. Supervisory Policy Manual and other circulars issued by the Hong Kong Monetary Authority, Code of Banking Practice, Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission) issued by the Government, relevant regulators and industry associations. To ensure professionalism and proper conduct, the Bank may wish to remind directors and staff to observe the above standards and requirements, as appropriate, when discharging their duties.]

Compliance with the Code

24. It is the responsibility of every director and staff member of the Bank to understand and comply with this Code, whether performing his/her duties of the Bank in or outside Hong Kong. Managers and supervisors should also ensure that the staff under their supervision understand well and comply with this Code.

25. Any director or staff member in breach of this Code will be subject to disciplinary action, including termination of appointment. Any enquiries about this Code or reports of possible breaches of this Code should be made to *(post of a designated senior staff member)*.

_____

(Name of Bank)

Date :

Extracts of the Prevention of Bribery Ordinance (Cap. 201)

Section 9 – Corrupt transactions with agents

(1) Any agent who, without lawful authority or reasonable excuse, solicits or accepts any advantage as an inducement to or reward for or otherwise on account of his –

(a) doing or forbearing to do, or having done or forborne to do, any act in relation to his principal's affairs or business; or

(b) showing or forbearing to show, or having shown or forborne to show, favour or disfavour to any person in relation to his principal's affairs or business,

shall be guilty of an offence.

(2) Any person, who, without lawful authority or reasonable excuse, offers any advantage to any agent as an inducement to or reward for or otherwise on account of the agent's –

(a) doing or forbearing to do, or having done or forborne to do, any act in relation to his principal's affairs or business; or

(b) showing or forbearing to show, or having shown or forborne to show, favour or disfavour to any person in relation to his principal's affairs or business,

shall be guilty of an offence.

(3) Any agent who, with intent to deceive his principal, uses any receipt, account or other document –

(a) in respect of which the principal is interested; and

(b) which contains any statement which is false or erroneous or defective in any material particular; and

(c) which to his knowledge is intended to mislead the principal,

shall be guilty of an offence.

(4) If an agent solicits or accepts an advantage with the permission of his principal, being permission which complies with subsection (5), neither he nor the person who offered the advantage shall be guilty of an offence under subsection (1) or (2).

(5) For the purposes of subsection (4) permission shall –

(a) be given before the advantage is offered, solicited or accepted; or

(b) in any case where an advantage has been offered or accepted without prior permission, be applied for and given as soon as reasonably possible after such offer or acceptance,

and for such permission to be effective for the purposes of subsection (4), the principal shall, before giving such permission, have regard to the circumstances in which it is sought.

Section 4 – Bribery

(1) Any person who, whether in Hong Kong or elsewhere, without lawful authority or reasonable excuse, offers any advantage to a public servant as an inducement to or reward for or otherwise on account of that public servant's –

(a) performing or abstaining from performing, or having performed or abstained from performing, any act in his capacity as a public servant;

(b) expediting, delaying, hindering or preventing, or having expedited, delayed, hindered or prevented, the performance of an act, whether by that public servant or by any other public servant in his or that other public servant's capacity as a public servant; or

Extracts of the Prevention of Bribery Ordinance (Cap. 201)

(c) assisting, favouring, hindering or delaying, or having assisted, favoured, hindered or delayed, any person in the transaction of any business with a public body,

shall be guilty of an offence.

(3) If a public servant other than a prescribed officer solicits or accepts an advantage with the permission of the public body of which he is an employee being permission which complies with subsection (4), neither he nor the person who offered the advantage shall be guilty of an offence under this section.

Section 8 – Bribery of public servants by persons having dealings with public bodies

(1) Any person who, without lawful authority or reasonable excuse, while having dealings of any kind with the Government through any department, office or establishment of the Government, offers any advantage to any prescribed officer employed in that department, office or establishment of the Government, shall be guilty of an offence.

(2) Any person who, without lawful authority or reasonable excuse, while having dealings of any kind with any other public body, offers any advantage to any public servant employed by that public body, shall be guilty of an offence.

Section 2 – Interpretation

"**Advantage**" means –

(a) any gift, loan, fee, reward or commission consisting of money or of any valuable security or of other property or interest in property of any description;

(b) any office, employment or contract;

(c) any payment, release, discharge or liquidation of any loan, obligation or other liability, whether in whole or in part;

(d) any other service, or favour (other than entertainment), including protection from any penalty or disability incurred or apprehended or from any action or proceedings of a disciplinary, civil or criminal nature, whether or not already instituted;

(e) the exercise or forbearance from the exercise of any right or any power or duty; and

(f) any offer, undertaking or promise, whether conditional or unconditional, of any advantage within the meaning of any of the preceding paragraphs (a), (b), (c), (d) and (e),

but does not include an election donation within the meaning of the Elections (Corrupt and Illegal Conduct) Ordinance (Cap. 554), particulars of which are included in an election return in accordance with that Ordinance.

"**Entertainment**" means the provision of food or drink, for consumption on the occasion when it is provided, and of any other entertainment connected with, or provided at the same time as, such provisions.

Section 19 – Custom not to be a defence

In any proceedings for an offence under this Ordinance, it shall not be a defence to show that any such advantage as is mentioned in this Ordinance is customary in any profession, trade, vocation or calling.

For Reference Only

(Bank Name)

REPORT ON GIFTS/ADVANTAGES RECEIVED

Part A – To be completed by Receiving Staff

To: *(Approving Authority)*

Description of Offeror :

Name & Title : _____

Company : _____

Relationship (Business / Personal) : _____

Occasion on which the Gift/Advantage was / is to be received : _____

Description & (assessed) value of the Gift/Advantage: _____

Suggested Method of Disposal :	**Remark**
☐ Retain by the Receiving Staff	_____
☐ Retain for Display / as a Souvenir in the Office	_____
☐ Share among the Office	_____
☐ Reserve as Lucky Draw Prize at Staff Function	_____
☐ Donate to a Charitable Organisation	_____
☐ Return to Offeror	_____
☐ Others (please specify) :	_____

_____

(Name of Receiving Staff)
(Title / Department)

(Date)

Part B – To be completed by Approving Authority

To: *(Name of Receiving Staff)*

The recommended method of disposal is ***approved / not approved***. *The gift/ advantage concerned should be disposed of by way of : _____

_____

(Name of Approving Authority)
(Title / Department)

(Date)
**Delete as appropriate*

For Reference Only

(Bank Name)

DECLARATION OF CONFLICT OF INTEREST

Part A – Declaration *(To be completed by the Declarer)*

To: *(Approving Authority)*

☐ I have no conflict of interest, whether actual or potential, in discharging my official duties in relation to [*insert the name of the project / exercise requiring positive declaration by the Bank*], and undertake to declare any such conflict immediately when I become aware of it.#

(# For use only when there is a requirement for positive declaration)

☐ I would like to report the following actual/potential* conflict of interest situation arising during the discharge of my official duties:

Person(s)/organisation(s) with whom/which I have official dealings and/or private interest
My relationship with the person(s)/organisation(s) (e.g. relative)
My contact with the person(s)/organisation(s) (Please state the frequency of contact and the usual occasions of contact, etc.)
Relationship of the person(s)/organisation(s) with the Bank (e.g. supplier)
Brief description of my duties which involved the person(s)/organisation(s) (e.g. handling of tender exercise)
File reference, if any, of the mentioned duties

(Name of the Declarer)

(Date) *(Title)*

Part B – Approval *(To be completed by Approving Authority)*

To: *(Declarer)*

Part B(i) – In respect of the declaration in Part A of this form, it has been decided that:

☐ The declaration as described in Part A is noted. You are allowed to continue handling the work as described in Part A, provided that there is no change in the information declared above.

☐ You are restricted in the work as described in Part A (e.g. prohibit from handling the specific part/duty that you have conflict, withdraw from discussion on a specific issue/case).

Details : _____

_____

☐ You may continue to handle the work as described in Part A, but an independent person would be recruited to participate in, oversee or review part or all of the decision-making process (e.g. task another staff with the required expertise to provide objective assessment on the matter).

Details : _____

_____

☐ You are relieved of your duty as described in Part A, which will be taken up by another person (e.g. staff, expert) through redeployment.

Details : _____

_____

☐ You should relinquish the personal/private interest (e.g. cease to be a member of a club/association, divest the investments until the conflict situation described in Part A no longer exists).

Details : _____

_____

☐ Others (please specify) (e.g. you should not contact the person(s)/organisation(s) concerned until the conflict situation described in Part A no longer exists).

Details : _____

_____

Part B(ii) – The justification(s) for the measure(s) as described in Part B(i) above is/are:

(Factors of consideration including the materiality of the conflict, link between the conflict and the matter in question, and any possible negative public perception over the conflict/incident.)

_____

_____

_____

_____

In all cases, please be reminded that you should not disclose any privileged/internal information of the subject matter to the person(s)/organisation(s) concerned and should further report if there are changes in circumstances necessitating reporting.

_____

(Name of the Approving Authority)

(Date) *(Title)*

Part C – Keeping of Records *(To be completed by the Declarer)*

To : (Designated office/staff for keeping the completed declaration form)

Via: (Approving Authority)

I noted the decision in Part B. The completed form is for your retention please.

_____

(Name of the Declarer)

(Date) *(Title)*

**Delete as appropriate*

** Potential conflict of interest refers to situation that may be developed into an actual conflict in the future.*

Examples of Conflict of Interest

Some common examples of conflict of interest are described below but they are by no means exhaustive –

- A staff member involved in the approving applications for bank accounts (e.g. conducting due diligence check) is a family member, a relative or a close personal friend of the applicant concerned.

- A staff member involved in the account opening process operates / has financial interest in an intermediary which assists its customers in applying bank accounts.

- A staff member involved in approving the loan applications from a corporate customer is closely related to / a relative of a director or has financial interest in the corporate customer.

- One of the candidates under consideration in a recruitment or promotion exercise is a family member, a relative or a close personal friend of the director involved in the exercise.

- A procurement staff involved in the selection of a service provider for the bank (e.g. selection of service provider for maintaining computer systems) is closely related to / a relative of a director or has beneficial interest in, a potential service provider / supplier.

- A director has financial interest in a company which tender is under consideration by the Board.

- A bank staff is a committee member of a professional institute in his private capacity. He seeks sponsorship from a bank's contractor whom he is responsible for monitoring, for organising an educational event of the professional institute.

- A bank staff has a directorship or employment in a debt collection agency which is one of the service providers of the bank.

- A staff member involved in the performance monitoring of service providers frequently accepts lavish entertainment from one of the service providers which he is responsible for monitoring.

- A staff leaks privileged information relating to the bank's operations to favour his friends or relatives who have official dealings with the bank.

Mitigating Measures for Managing Declared Conflict of Interest

(a) **Record** – Where the risk in a conflict of interest situation is indirect, remote or insignificant, and the occurrence of such a situation is infrequent, it may be sufficient to take note of the conflict only.

(b) **Restrict** – Where a conflict is not likely to arise frequently and the staff can be effectively separated from the part of activity or process in which the conflict arises, it may be suitable to restrict the staff's involvement in the task in which he has a conflict (e.g. withdrawing from discussion on a specific issue, abstaining from voting on the decisions) and access to the related information.

(c) **Recruit** – Where it is impractical to restrict a staff member's involvement, an independent staff member/expert may be recruited to participate in, oversee, or review part or all of the decision-making process if appropriate (e.g. engaging expert in the selection of highly specialised items).

(d) **Redeploy** – Where it is inappropriate to allow the staff who has declared a conflict of interest to handle a specific matter, it may be suitable to relieve of the staff's duty which may then be taken up by another staff through redeployment. For serious conflict of interest cases with a high likelihood of relapse, it may be suitable to post out the staff to avoid negative public perception.

(e) **Relinquish** – Where a staff member's commitment to the public duty outweighs his attachment to his private interest, and adopting other mitigating measures is not appropriate or possible, he may be asked to relinquish his personal or private interests (e.g. divesting the investments, ceasing to be a member of a club/association).

Ethics-Plus Decision Making Model

We make numerous decisions every day. Some decisions are tough calls when involving ethical dilemmas. The Hong Kong Business Ethics Development Centre (HKBEDC) of the ICAC developed the ethics plus Decision Making Model, to guide business practitioners to go through an array of important variables and reach a justified decision in a structured and systematic flow.

The Model

The Model consists of a six-step ETHICS thinking process and a four-factor PLUS standards to guide business practitioners to a righteous decision:

The ETHICS Process – Six major steps thinking process

E - Establish the relevant facts and identify the ethical issues at stake

T - Take stock of all the stakeholders involved

H - Have an objective assessment of each stakeholder's position

I - Identify viable alternatives and their effects on the stakeholders

C - Compare and evaluate each alternative with the Plus Standards

S - Select the best course of action

The Plus Standards – Four key factors to consider in the decision making

P - Professional / trade-related / company code of conduct

- Any violations to professional, industry specific or company code of conduct?

L - Legal requirements

- Is it against the law?

U - Uncompromising self-values

- Does it correspond with my self-values, such as loyalty and fairness?

S - Sunshine test

- Can I disclose my decision to others openly and honestly without misgivings?

Case Study

Terence is a bank relationship manager. His daughter is applying to a prestigious private school which is highly competitive in admission. Recently his boss hints Terence that if he can further boost his sales performance, he will be recommended for promotion.

Vincent is Terence's best friend who owns a business consulting firm. Several overseas clients of Vincent are high-net-worth investors who are interested in purchasing wealth investment products from banks in Hong Kong. However, these clients encounter difficulties in opening accounts in other banks as they cannot attend in person for an assessment of their financial sources, which is a prevailing requirement for banks.

Vincent tells Terence that his firm has been running short of working capital lately and these clients will pay his firm a lucrative sum of consulting fee if Vincent can help them open accounts in his bank. Desperate to solve his firm's financial problem, Vincent seeks Terence's assistance to open accounts for these clients by giving false representation to his bank that he has met with these clients in Hong Kong when the applications are made. Terence adds that these are good credit clients and are ready to buy high value wealth products with cash. Furthermore, Vincent offers to help Terence's daughter secure a place in the private school as Vincent's wife is an admission panel member of the school for which Terence applies.

The ETHICS Process

E - Establish the relevant facts and identify the ethical issues at stake

- Terence is facing a dilemma of whether to help Vincent's clients to open bank accounts or reject Vincent's request.

T - Take stock of all the stakeholders involved

- Major stakeholders include Terence and his family, Terence's bank, Vincent and Vincent's clients.

H - Have an objective assessment of each stakeholder's position

- **Terence and his family:**
  - Terence has served in the current position for several years and longed for a promotion.
  - Terence should perform customer due diligence according to the bank's policies and guidelines on account opening.
  - Terence and his wife are eager to secure a place for their daughter at the private school.
  - Terence is personally obliged to help his best friend through the tough times.

- **Terence's bank:**
  - Terence's bank strives to obtain more business, in particular by targeting high-net-worth investors.
  - Banks are subject to stringent rules and regulations. Non-compliance to customer due diligence will lead to disciplinary action, pecuniary penalty or even reputational harm to the bank.
- **Vincent:**
  - Vincent's company suffers from financial difficulties. It will generate lucrative income if Vincent is able to help his clients to open bank account successfully. Vincent may also get more business referrals from these clients.
- **Vincent's clients:**
  - The clients are ready to invest but without a local bank account. Failing to open accounts at other banks, they have high hope for Terence's bank.

I - Identify viable alternatives and their effects on the stakeholders

- Terence may come up with the following alternatives:

  <u>Accepting Vincent's request</u>

  1 Help Vincent's clients open accounts in his bank for buying wealth products and accept Vincent's offer of securing a school place for his daughter.

  2 Assist Vincent's clients in the account opening applications but decline Vincent's offer of the school place.

  Accepting Vincent's request to assist his clients in account opening can help Vincent through the financial hardship, facilitate Terence's promotion, boost the bank's business performance and fulfill the clients' need of investment.

  However, Terence, Vincent and his clients as well as Terence's bank may risk breaching relevant laws, rules and regulations. They may face disciplinary sanctions or legal consequences for failing to perform customer due diligence or committing bribery offences.

  <u>Rejecting Vincent's request</u>

  3 Decline Vincent's offer but strive to help Vincent get over his firm's financial problems through other legitimate means.

  4 Simply reject Vincent's request and decline his offer.

  Turning down Vincent will ensure all parties concerned adhere to relevant laws, rules and guidelines and avoid any legal implications.

  However, it may sacrifice Terence's promotion and his daughter's chance to study in the private school. It may also jeopardise Terence's friendship with Vincent and let the clients down.

Other alternatives

5 Other possible alternatives, which may include consultation with relevant law enforcement agencies if required.

C - Compare and evaluate each alternative with the Plus Standards

Professional / trade-related /company code of conduct

Terence fails to comply with Hong Kong Monetary Authority (HKMA) Supervisory Policy Manual and his bank's code of conduct for accepting Vincent's offer of a school place and misleading the bank in approving the account opening applications. Both HKMA's Supervisory Policy Manual and banks' code of conduct require banking practitioners and staff members not to involve in conflict of interest and whistle blow on suspected illegal activities such as fraud, deception and corruption.

Legal requirements

Both Terence and Vincent will breach Section 9 of the Prevention of Bribery Ordinance (POBO) if Terence accepts the favourable treatment by Vincent's wife for offering a school place to his daughter in return for assisting Vincent's clients to open accounts in his bank. In this case, the favour for Terence's daughter is an advantage from Vincent in exchange for Terence's abuse of power. Because of the deal, Terence may also violate Section 124 of the Banking Ordinance which prohibits receipt of any gift, commission, service or thing of value, etc. by staff for his own personal benefit or advantage or for that of his relatives.

In processing these clients' account opening applications, if Terence submits false or bogus documents to deceive the bank for approving the applications, Terence will infringe Section 9(3) of POBO. Besides, Terence may also be caught by Section 123 of the Banking Ordinance which makes it unlawful for bank staff to deceive their bank by false documents.

If Terence recommends or approves these clients' applications and handles their investment on bank wealth products, he may breach the Organized and Serious Crimes Ordinance or the Drug Trafficking (Recovery of Proceeds) Ordinance as well as the Anti-Money Laundering and Counter-Terrorist Financing Ordinance for not carrying out customer due diligence and reporting possible money laundering activities.

Uncompromising self-values

Terence should evaluate the alternatives against his personal values such as honesty, integrity, responsibility to the bank, professional competence and the interest of the banking sector as a whole. No alternative should compromise his personal values and beliefs.

Sunshine test

Lastly, Terence has to assess whether he can disclose his decision and openly discuss it without any reservations nor misgivings. If it cannot pass the sunshine test, it may not be an appropriate choice.

S - Select the best course of action – Terence's choice

Terence is facing a tough choice among career advancement, work responsibilities, professional duties, friendship, family and personal values. He should select the best option that is in compliance with the laws and regulations, professional requirements and aligns with his own personal values. He should also be prepared to answer any queries or provide justifications for his decision when being challenged.

Along these principles, the best option for Terence is to:

- decline Vincent's offer because it is against the laws, regulatory requirements, professional conduct and his personal values. The offer also fails the sunshine test;
- assist Vincent in applying bank loans via proper bank procedures and channels;
- map out new strategies to attract high-net-worth clients and establish long term relationships with existing clients; and
- spend more time with his daughter to prepare her for the school admission interviews.

Conclusion

The ethics plus Decision Making Model provides a framework for decision makers to exercise moral rationality and consider the consequences of each possible solution to the dilemma through different angles. By doing so, the decision maker will be able to reach a balanced and well-justified solution.

For more information about ethical decision making and other ethical dilemmas at work, please visit the dedicated *Ethical Decision Making* section (hkbedc.icac.hk/edm/en) at HKBEDC's website.

Addendum

Corruption Prevention Services for the Private Sector

Please note that with effect from 10 September 2026, the Corruption Prevention Advisory Service (CPAS) and the Hong Kong Business Ethics Development Centre (HKBEDC) of the Independent Commission Against Corruption (ICAC) have been restructured as the Private Sector Integrity Centre (PSIC).

Accordingly, any references to the CPAS and HKBEDC in this publication are to be read as referring to the PSIC from that date onwards.

As a one-stop service and knowledge hub, PSIC continues to provide free, confidential, and tailor-made corruption prevention and integrity services to private-sector organisations and individuals.

For enquires or services, please contact PSIC through the following channels:

- Hotline: 2526 6363
- Email: psic@cpd.icac.org.hk
- E-form: eform.cefs.gov.hk/form/ica004/en/
- Website: psic.icac.org.hk

Disclaimer

(In the event of any inconsistency or conflict between the following disclaimer and the disclaimer contained in other part of the publication, the following disclaimer shall prevail to the extent of the inconsistency or conflict.)

Descriptions and explanations of the legal and regulatory requirements under the Prevention of Bribery Ordinance (Chapter 201 of the Laws of Hong Kong) and any other ordinances, subsidiary legislation, orders, rules, regulations and case law (collectively, "Laws and Regulations") in this publication are intended to be general and abbreviated for ease of understanding. Users of this publication are advised to refer to the original text of the Laws and Regulations if considered necessary. Case scenarios are used in this publication to illustrate the legal and regulatory requirements and corruption risks. These case scenarios should be taken as hypothetical and not referring to any particular real case or any particular organisation or person. Moreover, the advice and recommendations given in this publication are by no means prescriptive or exhaustive, and are not intended to substitute any legal, regulatory or contractual requirements. Users should refer to the relevant instructions, codes and guidelines issued by the relevant authorities, and adopt the appropriate measures that best suit their operational needs and risk exposure.

The descriptions and explanations of the Laws and Regulations, case scenarios, advice and recommendations given in this publication are for general reference purposes only. The ICAC makes no warranties, express or implied, as to the accuracy, completeness, suitability and applicability of the aforesaid descriptions, explanations, case scenarios, advice and recommendations. The ICAC shall not have or accept any liability, obligation or responsibility whatsoever for any loss or damage incurred directly or indirectly by any person acting or refraining from acting in reliance upon the descriptions, explanations, case scenarios, advice, recommendations or any other information provided in this publication. Users of this publication are strongly advised to seek professional legal or other appropriate advice in relation to the information contained in this publication if considered necessary.

Private Sector Integrity Centre
Independent Commission Against Corruption
10 September 2026

廉政公署 ICAC

PSIC 私營機構誠信建設中心 Private Sector Integrity Centre